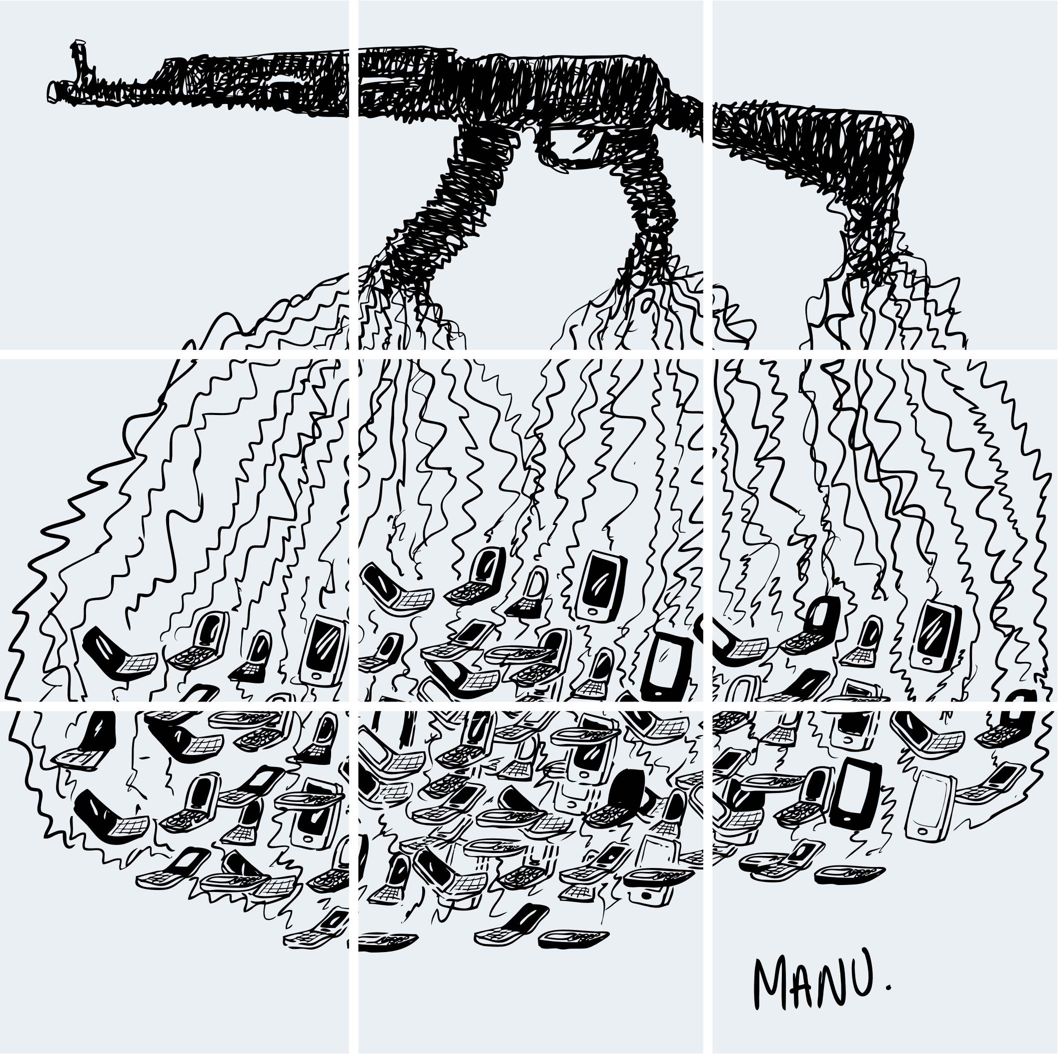
APRIL 2013

New Technology and the Prevention of Violence and Conflict

EDITED BY **FRANCESCO MANCINI**



UN
DP
Empowered lives.
Resilient nations.

USAID
FROM THE AMERICAN PEOPLE

IPI
INTERNATIONAL
PEACE
INSTITUTE

Cover Image: "Can Big Data From Cell Phones Prevent Conflict?"
© E. Letouzé.

Disclaimer: The views expressed in this paper represent those of the authors and not necessarily those of IPI. IPI welcomes consideration of a wide range of perspectives in the pursuit of a well-informed debate on critical policies and issues in international affairs.

IPI Publications
Adam Lupel, *Editor and Senior Fellow*
Marie O'Reilly, *Associate Editor*
Thong Nguyen, *Editorial Assistant*

Suggested Citation
Francesco Mancini, ed., "New Technology and the Prevention of Violence and Conflict," New York: International Peace Institute, April 2013.

www.ipinst.org

ABOUT THE EDITOR

FRANCESCO MANCINI is the Senior Director of Research at the International Peace Institute.

ACKNOWLEDGEMENTS

IPI owes a debt of thanks to all of its donors, whose support makes publications like this one possible. In particular, IPI would like to thank the United Nations Development Programme (UNDP) and the United States Agency for International Development (USAID) for their support and partnership on this project. Particular gratitude for guidance during the project goes to Anne Kahl, Chetan Kumar, Ozonnia Ojiello, and Jelena Raketic at UNDP's Bureau for Crisis Prevention and Recovery; to Joseph Hewitt, Neil Levine, and Rachel Locke at USAID's Office of Conflict Management and Mitigation; and to Alberto Cutillo and Taimi Strehlow at IPI. In addition, IPI, USAID, and UNDP would like to thank the members of the expert reference group and the anonymous reviewers of the case studies for their insights.

CONTENTS

Executive Summary

There are now 6 billion cell phone subscriptions in the world, and one third of the world's population is online.[1] These numbers are growing rapidly, particularly in the developing world, and they demonstrate an unparalleled level of global interconnectivity. They also point to the unprecedented amount of data that we are generating while using new information and communication technologies (ICTs): in 2012 alone, humans generated more data than over the course of their entire history.[2]

This report explores the ways in which ICTs and the data they generate can assist international actors, governments, and civil society organizations to more effectively prevent violence and conflict. It examines the contributions that cell phones, social media, crowdsourcing, crisis mapping, blogging, and big data analytics can make to short-term efforts to forestall crises and to long-term initiatives to address the root causes of violence. Five case studies assess the use of such tools in a variety of regions (Africa, Asia, Latin America) experiencing different types of violence (criminal violence, election-related violence, armed conflict, short-term crisis) in different political contexts (restrictive and collaborative governments).

The cases demonstrate clearly that employing new technologies for conflict prevention can produce very different results depending on the context in which they are applied and whether or not those using the technology take that context into account. This is particularly true in light of the dramatic changes underway in the landscapes of violence and conflict on a global level. As such, instead of focusing on supply-driven technical fixes, those undertaking prevention initiatives should let the context inform what kind of technology is needed and what kind of approach will work best.

With this in mind, lessons and insights from across the cases point to seven promising steps for strengthening prevention efforts that involve new technologies.

1. **Even if you crowdsource your hammer, not every problem is a nail.**

   New technologies have the potential to make huge contributions to violence- and conflict-prevention efforts, but they are not a panacea for holistic solutions. International organizations and governments should examine all the tools at their disposal for preventing conflict, and civil society organizations should not be blinkered by their particular thematic focus.

2. **Consider the context.**

   The cases show that socioeconomic, cultural, and demographic factors will all influence whether technology can have a positive impact, which technology would be appropriate, and how technologies could or should be combined. International organizations and governments should make needs assessments and feasibility studies that address these factors standard practice. Civil society organizations should also include such needs assessments or conflict and peace assessments in their proposals when seeking funding from donors.

3. **Do no harm.**

   Failure to consider the possible knock-on effects of applying a specific technology can lead to fatal outcomes in violent settings. Spoilers also leverage new technologies to incite violence, promote conflict, and perpetrate crimes. As such, a conflict-sensitive approach remains vital from conception to completion of any initiative involving new technologies. As part of project design and implementation, every actor should identify possible spoilers, conduct a cost-benefit analysis that incorporates levels of risk, develop mechanisms to mitigate risks, and create contingency plans.

[1] International Telecommunication Union (ITU), "ITU World Telecommunication/ICT Indicators Database, 2012," available at www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf ; United Nations, "The Millennium Development Goals Report 2012," New York, 2012, p. 63.

[2] The rate of data production now more than doubles every year, meaning that every year we produce more data than all previous years combined.

4. **Integrate local input throughout, and don't reinvent the wheel.**

   Examples abound where an absence of local input meant there was a lack of buy-in from the affected communities, project financing was unsustainable, the credibility of the information collected was questionable, or there was duplication of work. Once a project is underway, continual consultation with and involvement of the affected community is vital. In general, the application of new technological tools to prevention efforts at the local level works best when integrated into existing civil society initiatives.

5. **Use technology to help information flow horizontally more than vertically.**

   Horizontal citizen-to-citizen ICT initiatives can help to connect more "warners" and "responders" more quickly and closer to the crisis. They can also contribute to communities' resilience in the long term. International organizations should consider supporting spontaneous micro-initiatives in this area, provide funding to develop local capacity, improve connectivity between different initiatives, and help the sharing of best practices. Civil society organizations should identify and reward skilled individuals and groups in local communities who can adopt new technologies for preventing violence and conflict.

6. **Establish consensus regarding ownership, use, and sharing of information.**

   New technologies make it possible for international organizations and government agencies to acquire more information and more granular information to inform prevention efforts. International organizations, governments, and civil society actors should establish consensus around questions of privacy, access, and use of digital data in any given initiative. This will make prevention efforts more legitimate in the eyes of the affected communities, and ultimately more effective.

7. **Foster partnerships for better results.**

   There are indications that prevention initiatives that drew on the complementary strengths of international donors, governments, the private sector, and civil society proved more effective. International organizations and governments are well placed to foster such partnerships and should invest in doing so for more promising results.

Given the frequent paralysis at national and international levels when it comes to preventing conflict, the empowerment of individuals to participate in conflict-prevention initiatives in their own communities and societies may be one of the most significant innovations created by advances in technology. This is particularly true when it comes to bridging the persistent gulf between warning and response. Much more research is needed to assess how ICT can be used to generate action at the local level, as well as to inform or warn.

In the long run, however, the most effective approach to using new technologies for conflict prevention may well be the one needed in prevention more broadly: one that successfully balances both grassroots, decentralized efforts and the more rationalized and coordinated activities of governments and international organizations.

Introduction

Francesco Mancini

Forty years ago, on April 3, 1973, Martin Cooper made the first cell phone call in history. The general manager at Motorola called his rival at AT&T with a nine-inch and 28-ounce phone. Since then, cell phones have become facts of life. In only four decades, the total number of mobile phone subscriptions has reached almost 6 billion, corresponding to a global penetration rate of 86 percent.[1] Even more extraordinary is the speed of expansion in the developing world, where mobile subscriptions have dwarfed fixed lines. In 2011, 75 percent of worldwide subscriptions were in the developing regions, up from 59 percent in 2006. Cell phone penetration in sub-Saharan Africa now exceeds 50 percent, compared to a fixed telephone penetration of only 1 percent of the population.[2] By the end of 2011, there were 105 countries with more cell phone subscriptions than inhabitants, including African countries such as Botswana, Gabon, Namibia, the Seychelles, and South Africa.[3]

The global number of Internet users also continues to grow rapidly. By the end of 2011, more than one third of the world's population was online. And developing countries accounted for 63 percent of all users, with more rapid growth than developed countries. Major regional differences remain, however. While Internet penetration levels in the developing regions rose to 26 percent by the end of 2011, they remained below 15 percent in sub-Saharan Africa.[4]

Despite these low penetration levels in some areas, the diffusion of cell phones and the Internet have brought dramatic cultural, social, economic, and political changes in societies around the world. For example, much has been said about the role of social media in the eruption of the so-called Arab Spring, but factors such as the massive increase in the number of mobile devices with cameras and the greater accessibility of the Internet, with its ability to reach millions of people worldwide, have been just as important. Indeed, the penetration of smartphones in developing countries is on the rise. While China overtook the United States as the largest smartphone market in 2011, experts estimate that smartphone penetration in sub-Saharan Africa may reach 40 percent within five years.[5]

This global interconnectivity is also producing an unprecedented volume of data. With 12 million text messages (SMS) sent per minute and 2 billion YouTube pages viewed per day, the amount and variety of data produced is a phenomenon of historical significance.[6] More data was generated in the year 2012 than in all of human history combined.[7]

It is with these trends in mind—the increasingly rapid global interconnectivity, the increasing access to mobile devices globally, and the generation of an unprecedented quantity of data—that the International Peace Institute (IPI), with the support and partnership of the United Nations Development Programme's Bureau for Crisis Prevention and Recovery and the United States Agency for International Development's Office of

[1] International Telecommunication Union (ITU), "ITU World Telecommunication/ICT Indicators Database, 2012," available at www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf .

[2] United Nations, "The Millennium Development Goals Report 2012," New York, 2012, p. 63, available at www.un.org/millenniumgoals/pdf/MDG%20Report%202012.pdf#page=64 .

[3] ITU, "ITU World Telecommunication/ICT Indicators Database, 2012."

[4] United Nations, "The Millennium Development Goals Report 2012," New York, 2012, p. 64.

[5] Linda Sui, "China Overtakes United States as World's Largest Smartphone Market in Q3 2011," *Strategy Analytics*, November 2011, available at www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=6871 ; Jon Evans, "In Five Years, Most Africans Will Have Smartphones," Techcrunch, http://techcrunch.com/2012/06/09/feature-phones-are-not-the-future/#comment-box .

[6] ITU, "The World in 2010: ICT Facts and Figures," available at www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf .

[7] The rate of data production now more than doubles every year, meaning that every year we are producing more data than all previous years combined. See Marie O'Reilly, "Robert Kirkpatrick, Director of UN Global Pulse, on the Value of Big Data," *Global Observatory*, November 5, 2012, available at www.theglobalobservatory.org/interviews/377-robert-kirkpatrick-director-of-un-global-pulse-on-the-value-of-big-data.html ; Gil Press, "A Very Short History of Big Data," *What's the Big Data?*, June 6, 2012, available at http://whatsthebigdata.com/2012/06/06/a-very-short-history-of-big-data/ .

Conflict Management and Mitigation, launched a project to investigate the potential role of new information and communication technologies in conflict prevention.

PROJECT RATIONALE

Today, we know more about the causes, dimensions, and indicators of violent conflict than perhaps at any other time in history. Even where there is disagreement over drivers and effects in specific contexts, there is generally a degree of normative coherence on the causes and consequences of violent conflict. Yet, there continue to be stunted efforts to put this knowledge to use in the service of preventing violence before it breaks out. While some progress has been made over the past decade on preventing violent conflict, the international community has done more to improve its collective ability to bring violence to an end than it has to prevent its outbreak. In reality, political decision-making processes are still rarely influenced by existing conflict-prevention and early-warning systems—generating the so-called "warning-response gap."[8]

In addition, whereas funds tend to be generally available for responding to conflict, there tend not to be many funding options for prevention activities, even where violence is well predicted or occurs in repeated cycles.[9] More than ten years ago, in 1997, the Carnegie Commission estimated that preventing the Rwandan genocide would not only have saved thousands of lives, it also would have cost just one-third of the $2 billion spent on international relief and reconstruction.[10] These kinds of statistics have contributed to a widespread belief that there is both moral and fiscal value in prevention. Yet the reality is that prevention will continue to face insufficient investment. For donors, this is generally a problem of not being able to demonstrate results for prevention activities, as they would for crisis response or investments in development. At the national level, governments in affected countries may not be aware of the scale of the challenge, particularly if their engagement with the population is constrained, if they are complicit in one side of the dispute, or if they have insufficient capacity to address the problem.

New solutions are also needed to overcome the increasingly questioned dichotomy between operational prevention (short-term efforts to forestall an incipient or escalating crisis) and structural prevention (measures for addressing root causes of violence).[11] Contemporary preventive action has shown that success in short-term engagements addressing acute crises typically requires sustained and long-term efforts to address the root causes of violence. In recent years, the concept of systemic prevention was coined as the third component of a comprehensive prevention agenda.[12]

Can innovative technology provide new tools to overcome these limitations of conflict prevention? How can new technology contribute to the existing early-warning toolbox and help decrease the occurrence of violent conflict more effectively?

SCOPE AND METHODOLOGY

Against this backdrop, the core question that has been guiding the researchers of this project is: how can new information and communication technologies (ICTs) aid international actors, governments, and civil society organizations to strengthen their voice and action in order to more effectively prevent violent conflict? In this report, the term "new technology" is used to connote communication, information gathering, information sharing, and information analysis that take place via cell phones and over the Internet (e.g., social media, information mapping, GIS mapping), and that can be utilized in the service of conflict prevention. Here, conflict prevention refers to those activities that have as their primary purpose the avoidance of—or reduction in—political violence; the resolution or peaceful management of political

[8] Susanna Campbell and Patrick Meier, "Deciding to Prevent Violent Conflict: Early Warning and Decision-Making at the United Nations," paper presented for the 48th Annual Convention of the International Studies Association (ISA), Chicago, 2007.

[9] Since 2003 every recorded outbreak of civil war has occurred in a country with a history of civil conflict, see World Bank, *World Development Report 2011: Conflict, Security, and Development* (Washington, DC, 2011), p. 58.

[10] Carnegie Commission on Preventing Deadly Conflict, "Preventing Deadly Conflict: Final Report," New York: Carnegie Corporation of New York, 1997.

[11] These two distinct modes of conflict prevention were introduced by the Carnegie Commission on Preventing Deadly Conflict in the report "Preventing Deadly Conflict."

[12] See United Nations Secretary-General, *Progress Report on the Prevention of Armed Conflict*, UN Doc. A/60/891, July 18, 2006.

disputes that can lead to violent conflict; and the de-escalation of tensions within society.[13]

Each researcher was guided by a set of questions, which were general enough to allow for capturing the specificity of each case, but could also guarantee the uniformity of investigation. More specifically, each case study explored (1) the density and quality of ICTs utilized; (2) triggering events for the conflict or violence as appropriate, and the role of ICTs; (3) the role of civil society, national governments, donors, and regional and international organizations, if any; (4) government capacity and legitimacy, and its interactions with the community; (5) patterns of information flow and their relevance for the quality of early warning, credibility of alerts, and number of people reached; (6) whether and how ICT improved and/or worsened the situation; and (7) whether and how ICT facilitated, informed, or expedited the response to the conflict situation.

The project benefited from the inputs and insights of a small group of experts from academia, think tanks, the private sector, and the field (see annex). The experts gathered at the beginning of the project to provide feedback on the methodology for the project and the selection of case studies. The selection of the cases sought to ensure that a variety of prevention experiences were analyzed, including

1. cases from different regions of the world (Africa, Asia, Latin America);
2. cases with different types of violence (criminal violence, election-related violence, armed conflict, short-term crises);
3. cases in different political contexts (restrictive and collaborative governments); and
4. cases with different technological tools (big data, cell phones, crowdsourcing, crisis mapping, blogging, social media, etc.)

The combination of these criteria produced the five cases that follow this introduction. Given the relative newness of some of these technological advances, cases assessed experiences in the last five years and addressed both positive and negative results. They were written by independent experts, and high priority was given to the inclusion of those from universities, research organizations, and think tanks from the regions and countries where the analyzed conflicts or crises occurred. All experts worked using the same terms of reference and method of structured, focused comparison to ensure the comparability of their findings. Each study is a product of both desk and field research. With a view to facilitating the practical application of these findings, the report's conclusion captures cross-cutting lessons and recommendations for international organizations, governments, and civil society organizations.

[13] This typically includes early warning and assessment, preventive diplomacy, crisis management, conflict resolution, peacemaking, peacekeeping, peacebuilding, and all activities aimed at strengthening international, regional, and national systems and capacities in these fields. For a more detailed presentation of the concept of conflict prevention, see the "conflict prevention" section on pages 5 and 6 of this report.

Big Data for Conflict Prevention: New Oil and Old Fires[1]

Emmanuel Letouzé, Patrick Meier, and Patrick Vinck[2]

> The ability to manipulate big data, visualize dynamics, and recognize patterns and signatures for conflict creates new opportunities for humanitarian and development assistance in the most complex and dangerous environments.
>
> *David Kilcullen and Alexa Courtney*[3]

> The theory of technology as amplifier explains how the same technology can appear to have both positive and negative impacts, because technology is merely a magnifier of underlying human and institutional intent and capacity, which can themselves be positive or negative.
>
> *Kentaro Toyama*[4]

> The hope that technology will reduce the violence of war is a venerable one… Richard Gatling hoped his new fast-firing gun would serve to reduce the bloodshed of war, while Alfred Nobel believed the explosives he invented would make war unthinkable.
>
> *Peter W. Singer*[5]

This paper discusses how Big Data could help reveal key insights into the drivers, triggers, and early signs of large-scale violence in order to support and improve conflict-prevention initiatives. In general, big data refers to the exponential increase in the volume and speed of information being created every day in our digital, hyperconnected world.[6]

As a field of practice in the making, what we term here "Big Data for conflict prevention" is best characterized by its potential rather than by its track record. Certainly, in recent years technological innovation has become an important part of conflict prevention in a number of areas, including early warning and response. Sophisticated data mining techniques have also long been used for intelligence and defense purposes.[7] But, as we show, neither is—nor should be—synonymous with Big Data for conflict prevention.

The fundamental questions of what defines Big Data for conflict prevention, and what potential it has are still largely to be answered. Perhaps as importantly, there is a need to structure these questions around conceptual considerations and frameworks to guide and inform future debates on these complex and sensitive issues. Such is the

[1] The authors thank Francesco Mancini (IPI) for his guidance during the course of this paper's development, as well as Robert Kirkpatrick (UN Global Pulse), Melanie Greenberg (Alliance for Peacebuilding), Helena Puig Larrauri (independent consultant), Sanjana Hattotuwa (ICT4Peace), Lea Shanley and Alyson Lyons (Wilson Center), Jay Ulfelder (independent consultant), and Mark Whitlock (Columbia University) for their suggestions and comments. We also thank Sarah L. Cramer for excellent research assistance.

[2] Emmanuel Letouzé is a Non-Resident Adviser at the International Peace Institute, former Senior Development Economist at UN Global Pulse, PhD candidate at UC Berkeley. As the lead author of this report he may be contacted at eletouze@berkeley.edu . Patrick Meier is Director of Social Innovation at Qatar Foundation's Computing Research Institute (QCRI), former Co-Director of the Harvard Humanitarian Initiative's Program on Crisis Mapping & Early Warning, and former Director of Crisis Mapping at Ushahidi. Patrick Vinck is Director of the Program for Vulnerable Populations, Harvard Humanitarian Initiative; Visiting Scientist, Harvard School of Public Health, Research Scientist, Brigham and Women's Hospital, Adjunct Assistant Professor, Payson Center for International Development, Tulane University.

[3] David Kilcullen and Alexa Courtney, "Big Data, Small Wars, Local Insights: Designing for Development with Conflict-affected Communities," *McKinsey on Society*, available at http://voices.mckinseyonsociety.com/big-data-small-wars-local-insights-designing-for-development-with-conflict-affected-communities/ .

[4] Kentaro Toyama, "Technology as Amplifier in International Development," proceedings from iConference 2011, New York, 2011, p. 78.

[5] Peter W. Singer, "Military Robots and the Laws of War," *The New Atlantis*, No. 25 (Winter 2009): 40, available at www.thenewatlantis.com/publications/military-robots-and-the-laws-of-war .

[6] See below for a further discussion on the definition of the term. See also, Crysta Anderson, "What is Big Data, and Why Does it Matter?," *Smarter Computing Blog*, January 1, 2013, available at www.smartercomputingblog.com/big-data/what-is-big-data-and-why-does-it-matter/ .

[7] Rupesinghe, Kumar, *The Quest for a Disaster Early Warning System: Giving a Voice to the Vulnerable* (Oslo: Peace Research Institute, Oslo, 1998), available at http://iRevolution.net/2011/08/01/quest-for-disaster-early-warning .

double objective of this paper.

Before getting into the substance and details, let us start by contrasting two diametrically opposed and highly simplistic perspectives on the relevance of Big Data for conflict prevention as a way to sketch some of the terms of the larger debate.

One perspective would point to the potential of the present data revolution and posit that Big Data is not just relevant but perhaps even especially adapted to conflict prevention. It can provide a real-time, 360-degree view of complex, risky, and traditionally data-poor settings to policymakers sitting in some remote (i.e., safe) location—as a twenty-first century incarnation of generals standing on top of a hill overlooking the battlefield—thereby saving lives and resources.[8] Recent examples and current shifts do give credit to the notion that "the ability to manipulate big data, visualize dynamics, and recognize patterns and signatures for conflict creates new opportunities for humanitarian and development assistance in the most complex and dangerous environments."[9]

The other perspective, in contrast, would hold that relying primarily on biased-and-messy-data analysis by number crunchers who may have never set foot in the field to inform sensitive policy and programmatic decisions in conflict-prone or -affected contexts would indeed be like pouring hot oil on burning ashes.[10] In other words, the concern is that rushing to apply Big Data in such volatile and dangerous environments without fully understanding and addressing the associated risks and challenges—the non-representativeness of the data, the difficulty in separating "the signal from the noise," the larger challenge of modeling human behavior, even the risk of misuse of such tools by oppressive regimes—may well end up spurring rather than preventing the spread of conflict.

Both perspectives are of course largely wrong yet partly right, and the truth probably falls, as often, somewhere between the two.[11] Another truth is that the discussion—of Big Data in general, especially applied to the realm of policy broadly speaking—too often stays at a superficial level. It is high time we started unpacking what sits beneath the surface.

Against this background, this paper asks five key questions, which could serve to frame future discussions:

1. What do we mean by "Big Data for conflict prevention"?
2. What are current applications of related techniques in related fields?
3. How could Big Data be leveraged for conflict prevention, in theory?
4. Which associated challenges and risks are likely to arise?
5. What principles and institutions may help?

What Do We Mean by Big Data for Conflict Prevention?

"Big Data for conflict prevention" refers to the potential use of Big Data to support conflict-prevention efforts undertaken by a wide range of potential actors among communities, nongovernmental and community-based organizations, governments, international organizations, etc. As such, it falls at the intersection of a field that has a long tradition—conflict prevention—and a new and fast-growing practice—Big Data, especially applied to development objectives, referred to as Big Data for development. Before identifying and analyzing possible points of connection (and frictions) between both, it is useful to start by quickly defining and describing them separately.

CONFLICT PREVENTION

A commonly used definition of conflict prevention is Michael Lund's, who defines it as "[a]ny structural or intercessory means to keep intrastate or interstate tension and disputes from escalating into significant violence and use of armed forces, to strengthen the capabilities of potential parties to violent conflict for resolving such disputes peacefully, and to progressively reduce the underlying problems that produce these issues and

[8] cf. Casey Barrs, "Conflict Early Warning: For Who?" *The Journal of Humanitarian Assistance*, February 2006.

[9] Kilcullen and Courtney, "Big Data, Small Wars, Local Insights."

[10] See Barnett P. Rubin, *Blood on the Doorstep: The Politics of Preventive Action* (New York: The Century Foundation and the Council on Foreign Relations, 2002).

[11] Jennifer Leaning and Patrick Meier, "The Untapped Potential of Information Communication Technology for Conflict Early Warning and Crisis Mapping," Working Paper Series, Harvard Humanitarian Initiative (HHI), 2009; Patrick Meier, "Upgrading the Role of Information Communication Technology (ICT) for Tactical Early Warning/Response." Paper prepared for the 49th Annual Convention of the International Studies Association (ISA) in San Francisco, 2008.

disputes."[12] In other words, conflict prevention refers to a variety of activities aimed at anticipating and averting the outbreak of conflict, or attempting to limit its scale and spread.

In practical terms, conflict prevention includes early warning, crisis management, conflict resolution, peacemaking, peacekeeping, and peacebuilding activity, and all activities and expenditures aimed at strengthening international and regional systems and capacities in these fields.[13] Although the field has undergone important changes in recent years, it continues to be viewed through the two main complementary lenses of structural prevention and operational (or direct) prevention (other perspectives distinguish short- and long-term prevention[14]).

Structural prevention is comprised of medium to long-term development projects that address what are believed to be structural drivers of conflict (e.g., poverty, horizontal inequality, elite capture of the state or economy at the expense of the people, etc). Conflict-sensitive programming and conflict risk assessments form part of the toolkit of structural prevention, which typically draws on macro-economic and macro-political structural indicators. These, however, are at times questionable vis-à-vis data quality—assuming they are even available in the first place.

Operational prevention on the other hand is discussed in terms of conflict early warning and response systems (as well as preventive diplomacy). Operational conflict prevention addresses "proximate," more immediate, triggers of conflict. Indicators for conflict early-warning systems are usually developed based on risk assessments undertaken as part of structural prevention efforts. Initial early-warning systems have been criticized and often failed in large part because they were too hierarchical and top-down, lacked an early response mechanism, produced (late) and non-actionable general recommendations, etc.[15]

As a result, there has been an important shift in recent years toward what is referred to as Third and Fourth Generation early warning and response,[16] which are more bottom-up and decentralized—also referred to as tactical early warning and response (see table 1).

A gloomier but key take-away message from this has been what is commonly referred to as the

Table 1: Four Generations of Early Warning and Response

Generation	Location	Objective	Technology
1st Generation Since 1990's	Headquarters	Conflict detection	• Expensive, proprietary technology
2nd Generation Since 2000	Headquarters with stronger links to networks in the field	Conflict detection with limited response (mainly recommendations)	• GIS and satellites • Internet (email & websites)
3rd Generation Since 2003	Conflict areas with local networks included in the system	Conflict detection with stronger links to response mechanisms; monitors often serve as "first responders"	• Proprietary software with structured reporting & coding protocols • Mobile phones • GIS and open-source satellite imaging
4th Generation Since 2008	Conflict areas with less centralized organizational frameworks	Decentralized two-way information service for collection and dissemination	• Free and/or open source technologies, especially mobile phones

Source: OECD, "Preventing Violence, War and State Collapse: The future of Conflict Early Warning and Response," Paris, 2009; Patrick Meier, "Fourth-Generation Early Warning Systems," March 6, 2009, blog entry available at: http://bit.ly/jzpV8c.

[12] Michael Lund, "Preventing Violent Interstate Conflicts: Learning Lessons from Experience," in *Searching for Peace in Europe and Eurasia: An Overview of Conflict Prevention and Peacebuilding Activities*, edited by Paul van Tongeren, Hans von de Veen, and Juliette Verhoeven, (Boulder, CO: Lynne Rienner, 2002).

[13] See www.eplo.org/definitions.html .

[14] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0211:FIN:EN:PDF .

[15] Patrick Meier, "New Strategies for Effective Early Response: Insights from Complexity Science." Paper prepared for the 48th Annual Convention of the International Studies Association (ISA) in Chicago, 2007, available at http://iRevolution.files.wordpress.com/2011/07/meier-early-response-isa2007-feb23-final.pdf .

[16] Patrick Meier, "Fourth Generation Early Warning Systems," Conflict Early Warning and Early Response Blog, March 6, 2009, available at https://earlywarning.wordpress.com/2009/03/06/fourth-generation-early-warning-systems .

warning-response gap.[17] For the most part, the gap reflects the simple fact that most existing decision-making structures are not geared—and some are totally unconnected—to existing conflict early-warning systems. If the connection exists, other factors—such as the lack of political will—hinder responses.[18] The result has typically been an absence of any link between the formal early warning analysis and executive decision-making processes. In general, and despite great efforts and improvements over the years, it must be acknowledged that conflict early warning and response systems have had a fairly poor track record.[19] To be sure, "we cannot say today that we are in a position to prevent another Rwandan genocide. Conflict early warning faces similar challenges to those it did fifteen years ago."[20] And so, despite the fact that "billions of dollars have been invested in developing sophisticated data banks and early warnings, we have to note that even the most expensive systems have shown a striking inability to forecast political events," not to mention early response.[21] This observation was made twenty-five years ago. The contemporary academic and policy literature on conflict early warning and response advocates for a more people-centered approach. The UN defines the purpose of people-centered systems as empowering at-risk communities to get out of harm's way and/or mitigating the impact of a crisis on their livelihoods.[22] In addition, the literature calls for a greater focus on the causes of peace in order to identify and support opportunities for prevention.[23]

To this end, it remains to be seen whether and how Big Data may

1. have any impact on the structural factors that have made most conflict early warning and response systems designed for failure;
2. empower local communities and thus render them more resilient;
3. shed light on the dynamic causes of peace.[24]

As will be discussed below, these shifts and their underlying considerations create opportunities, challenges, and reference points for developing Big Data for conflict prevention.

BIG DATA AND "BIG DATA FOR DEVELOPMENT"

Although most of the discussions around Big Data have been happening in the realm of business, the application of Big Data to development problems—referred to as "Big Data for development"—has received increasing attention. By now are aware that 90 percent or so of all data ever produced were produced in the past two years alone.[25] No matter how data is defined,[26] the recent and current growth in the amount and variety of new kinds of data is a phenomenon of historical nature and significance that has led many prominent observers to dub it the "Industrial Revolution of Data."[27]

There are critics that downplay the novelty and impact of Big Data as hype, but we believe the best approach is to examine how these massive streams of complex real-time data can be best leveraged for the common good. Some assume that Big Data is only relevant to the study of highly developed countries. We argue that there is mounting evidence that Big Data is relevant to developing countries and to development. And we argue that it

[17] Susanna Campbell and Patrick Meier, "Deciding to Prevent Violent Conflict: Early Warning and Decision-Making at the United Nations." Paper prepared for the 48th Annual Convention of the International Studies Association (ISA) in Chicago, 2007.

[18] See Rubin, "Blood on the Doorstep."

[19] Meier, "New Strategies for Effective Early Response."

[20] David Nyheim, "Can Violence, War and State Collapse Be Prevented? The Future of Operational Conflict Early and Response Systems," OECD Publishing, 2008, available at https://earlywarning.wordpress.com/2008/07/02/nyheim-oecd .

[21] Kumar, *The Quest for a Disaster Early Warning System*.

[22] United Nations Office for Disaster Risk Reduction, "Global Survey of Early Warning Systems: An Assessment of Capacities, Gaps and Opportunities Toward Building a Comprehensive Global Early Warning System for all Natural Hazards," March 2006, available at www.unisdr.org/we/inform/publications/3612 .

[23] Patrick Meier, "Crowdsourcing for Peace Mapping," *iRevolution*, November 21, 2009, available at http://iRevolution.net/2009/11/21/peace-mapping .

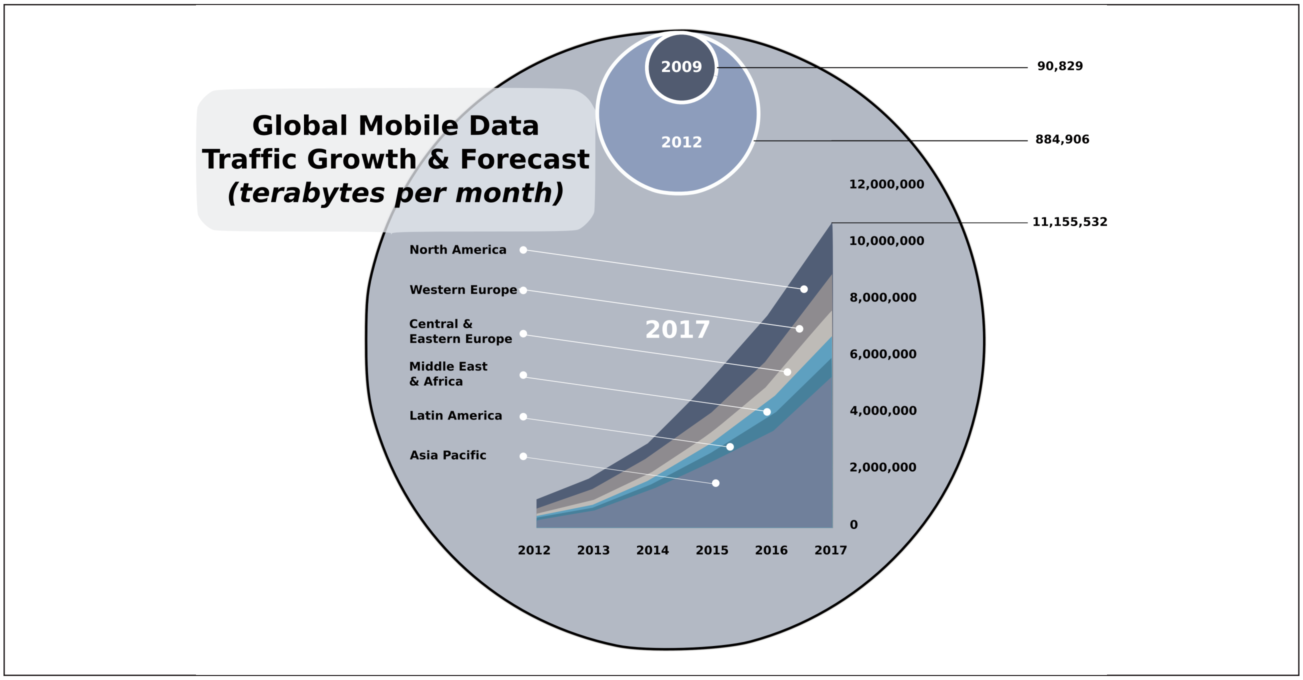
[24] Patrick Meier, "How to Create Resilience Through Big Data," *iRevolution*, January 11, 2013, available at http://iRevolution.net/2013/01/11/disaster-resilience-2-0 .

[25] See for example Nic Smith, "Big Data, Mobility and Predictive Analysis . . . What Are the Possibilities?," Analytics from SAP, November 27, 2012, available at http://blogs.sap.com/analytics/2012/11/27/big-data-mobility-and-predictive-analysis-what-are-the-possibilities/ and Zach Urbina, "Understanding Big Data & The Growing Need for Robust HIT Analytics," Healthcare IT Connect, August 29, 2012, available at www.healthcareitconnect.com/infographic-understanding-big-data-the-need-for-robust-hit-analytics/ .

[26] See "Has 90% of the World's Data Been Created in the Last Two Years?" Skeptics, August 10, 2012, available at http://skeptics.stackexchange.com/questions/10418/has-90-of-the-worlds-data-been-created-in-the-last-two-years .

[27] Referenced by Nathan Eagle in a video interview for UN Global Pulse, July 2011. Though, the term seems to have been originally coined by Joe Hellerstein, a computer scientist at the University of California, Berkeley. See "Data, Data Everywhere," *The Economist*, February 25, 2010, available at www.economist.com/node/15557443 .

Figure 1: The Exponential Growth in Cell-Phone Data



Source: Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017," February 2013; "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2009-2014," February 2010.

will increasingly be so, given the projected growth in certain kinds of data, especially those produced by increased cell-phone use (figure 1), which will drive Internet penetration around the world. But what exactly is "Big Data for development"?

To the best of our knowledge, the expression itself first appeared in the title of UN Global Pulse's White Paper in 2012 , written by one of the present paper's co-authors[28] and has since been used by other authors, whether or not referring to the exact same concept.[29]

A few points are worth clarifying. First, it is important to clearly distinguish when we (collectively) talk about Big Data as a field of practice and big data as data (the distinction and notation are ours). As a field of practice, what we term Big Data refers to what is otherwise called Big Data Analytics, i.e., methodologies leveraging advanced computing techniques such as machine-learning, as well as the actors and institutions using them to gain insights for decision-making purposes. The "value" of Big Data whether applied to development, business, or any other field, thus depends on the whole ecosystem around the (big) data.

As a field of practice, Big Data for development can also be—and has been—described through the main objectives it may serve. The Global Pulse white paper cites three applications, using a taxonomy that will provide a reference for thinking more deeply and concretely about Big Data for conflict prevention here and beyond:

1. **Early Warning**, i.e., the "early detection of anomalies in how populations use digital devices and services can enable faster response in times of crisis."
2. **Real-Time Awareness**, i.e., how "Big Data can paint a fine-grained and current representation of reality which can inform the design and

[28] "Big Data for Development: Challenges and Opportunities," UN Global Pulse, May 2012, available at www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf .

[29] Including https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2205810_code1827058.pdf?abstractid=2205145&mirid=1, Alice Newton, "Big Data for Development: Beyond Transparency," World Bank, July 23, 2012, available at http://blogs.worldbank.org/psd/big-data-for-development-beyond-transparency and, using "and" instead of "for": Wolfgang Fengler, "Big Data and Development: 'The Second Half of the Chess Board,'" World Bank, February 6, 2013, available at http://blogs.worldbank.org/africacan/big-data-and-development-the-second-half-of-the-chess-board, as well as before May 2012, World Economic Forum Briefing, "Big Data, Big Impact: New Possibilities for International Development," World Economic Forum Briefing, 2012, available at http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf, and Sanjana Hattotuwa, "A Brief Exploration of Open and Big Data: From Investigative Journalism to Humanitarian Aid and Peacebuilding," March 2012, available at https://ict4peace.files.wordpress.com/2012/03/a-brief-exploration-of-open-and-big-data-from-investigative-journalism-to-humanitarian-aid-and-peacebuilding.pdf .

targeting of programs and policies."

3. **Real-Time Feedback**, i.e., "the ability to monitor a population in real time makes it possible to understand where policies and programs are failing and make the necessary adjustments."[30]

As *data*, big data in general and big data for development in particular are significantly harder to define or even circumscribe.[31] This is probably the reason why big data (as a concept) has been more commonly described according to the key features and/or categorized according to different taxonomies of big data. The "3 Vs" of velocity, volume, and variety are probably the most common way the main features of big data have been presented in the literature and the mainstream press.[32] Other "Vs" are also regularly added, among them value, variability, verification, virality, and even viscosity.[33]

Deeper thinking around the definition and nature of big data has actually happened in the broad field of social science research and policy, some of which building on the 3 Vs, others moving away from it.[34] In the latter category, Alex Sandy Pentland, for instance, differentiates social media data on the one hand and cell-phone data (known as call detail records, or CDRs) or credit card transaction data on the other hand. He refers to the latter as "the little data breadcrumbs that you leave behind you as you move around in the world" as opposed to Facebook entries for instance, which can be "edited according to the standards of the day."[35] The Global Pulse white paper also proposed two taxonomies according to which Big Data for development could be apprehended. One is based on five key features[36] of Big Data for development. Another taxonomy described four kinds of digital source, namely "data exhaust," "online information," "physical sensors," and "citizen reporting or crowd-sourced data."[37] However, the present paper does not consider the fourth category of citizen reporting or crowdsourced data as big data for development (or conflict prevention). The main reason is that these data streams, although central to fourth generation early-warning systems, are typically not very large and are actively generated for analytical purposes.[38] Certainly, the distinction does and will increasingly get blurry when Twitter is used precisely for purposefully sharing real-time information in crisis contexts. But restricting our attention to these other kinds of largely passively-generated data (and those resulting from the active collection of observed data by satellites) seems both more consistent and useful.[39] This does not mean, however, that we draw a strict line. Indeed, much of what follows also applies to large volumes of crowd-

[30] UN Global Pulse, "Big Data for Development," p. 39

[31] See "Elusive Big Data: The Thing, and not the Thing," *The Economist*, February 18, 2013, available at www.economist.com/blogs/graphicdetail/2013/02/elusive-big-data .

[32] Diya Soubra, "The 3 Vs that Define Big Data," Data Science Central, July 5, 2012, available at www.datasciencecentral.com/forum/topics/the-3vs-that-define-big-data .

[33] See notably Alex Popescu "Big Data: Volume, Velocity, Variability, Variety,"myNoSQL, June 9, 2011, available at http://nosql.mypopescu.com/post/6361838342/bigdata-volume-velocity-variability-variety, R. Wang, "Monday's Musings: Beyond the Three V's of Big Data—Viscosity and Virality," *Softwareinsider*, February 27, 2012, available at http://blog.softwareinsider.org/2012/02/27/mondays-musings-beyond-the-three-vs-of-big-data-viscosity-and-virality/, and Dave Beulke "Big Data Impacts Data Management: The 5 Vs of Big Data," *Dave Beulke Blog*, November 1, 2011, available at http://davebeulke.com/big-data-impacts-data-management-the-five-vs-of-big-data/ .

[34] "The Ethnographer's Complete Guide to Big Data," Ethnography Matters, June 11, 2012, available at http://ethnographymatters.net/2012/06/11/the-ethnographers-complete-guide-to-big-data-part-ii-answers/ .

[35] "Reinventing Society in the Wake of Big Data,"A Conversation with Alex (Sandy) Pentland, *Edge*, August 30, 2012, available at: www.edge.org/conversation/reinventing-society-in-the-wake-of-big-data .

[36] "Digitally generated—i.e. the data are created digitally (as opposed to being digitised manually), and can be stored using a series of ones and zeros, and thus can be manipulated by computers; (2) Passively produced—a by product of our daily lives or interaction with digital services; (3) Automatically collected—i.e. there is a system in place that extracts and stores the relevant data as it is generated; (4) Geographically or temporally trackable—e.g. mobile phone location data or call duration time; (5) Continuously analysed—i.e., information is relevant to human well-being and development and can be analysed in real-time;" UN Global Pulse, "Big Data for Development," p. 15.

[37] "Data Exhaust—passively collected transactional data from people's use of digital services like mobile phones, purchases, web searches, etc., and/or operational metrics and other real-time data collected by UN agencies, NGOs and other aid organizations to monitor their projects and programs (e.g.,, stock levels, school attendance); these digital services create networked sensors of human behavior; (2) Online Information – web content such as news media and social media interactions (e.g., blogs, Twitter), news articles obituaries, e-commerce, job postings; this approach considers web usage and content as a sensor of human intent, sentiments, perceptions, and want; (3) Physical Sensors – satellite or infrared imagery of changing landscapes, traffic patterns, light emissions, urban development and topographic changes, etc; this approach focuses on remote sensing of changes in human activity;(4) Citizen Reporting or Crowd-sourced Data – Information actively produced or submitted by citizens through mobile phone-based surveys, hotlines, user generated maps, etc; While not passively produced, this is a key information source for verification and feedback," UN Global Pulse, "Big Data for Development," p. 16.

[38] The active versus passive dichotomy with respect to crowdsourced data has been discussed a great deal in the geography literature. The distinction made is whether people are actively providing information about themselves for a specific purpose, or are at least aware of the data collection and don't object, or whether they are unaware of and may object to being observed/tracked and have their information collected and used for purposes other than they originally intended. We are grateful to Lea Shanley for pointing this out.

[39] See a fuller discussion further below.

sourced data. Likewise, others have emphasized the value of "long data,"[40] while it is clear that a large part of the existing stock of analog data sources—such as books—will eventually be digitalized and lend themselves to data mining techniques. But are these big data? The answer is, as far as we are concerned, no. These are part of "all data"—just as price indices or weather data are. So, what is big data for development, and what is not? Three points stand out.

First, we define "big data for development" as the *traces of human actions picked up by digital devices*, or as the digital translation (understood in its literal sense) of human actions. By "actions" we mean, for instance, moving places, making a purchase or a phone call, researching a word online, publishing a blog post, sending a tweet, or updating a Facebook status (the true intent of which may not be known). The essential features of these digital traces are that they are left as actions unfolding in real-time,[41] and allow connecting numerous smaller heterogeneous, unstructured and structured data streams.[42] This general definition does not mean that one should not clearly distinguish "hard" structured data such as CDRs and Facebook posts, but in all cases Big Data for development is about what people do[43] and what we think these actions may mean in terms of their experiences, feelings, incentives, intentions, etc., which requires translating back the data into humanly graspable and hopefully actionable information.

Second, what exactly qualifies as 'big data for X' is dependent on X. The kind of big data used in Big Data for development or its sub-field of conflict prevention does not fully overlap with big data mined by private corporations, and, in contrast, other kinds of big data for development may not actually be very big or very high frequency. But they are sufficiently different from the kind of data traditionally used for development purposes to be called big data. And they may, over time, display some of the most common features of big data—such as microfinance data for example.[44] What qualifies as big data *for conflict prevention* will also depend in great part on how conflict prevention is defined and the context in which Big Data for conflict is deployed. This, in itself, requires human input—as will be discussed further below. In addition, what is "big" also depends on the tools at hand—bearing in mind that the problem is not so much information overload as filter failure.[45]

Third, big data do not exist in a vacuum but are part of a larger universe of data with loose boundaries. Rainfall or temperature data, or price data, are certainly big, high frequency, low granularity data. And they do have important bearing on human lives and ecosystems, and, as such, are integral parts of attempts at modeling and understanding these ecosystems. But, for definitional coherence, we choose to call these *contextual* (big) data not big data for development simply because they are not digital traces of human actions, even if and when human actions impact their patterns and trends—as in the case of prices or even rainfalls or temperatures. To be clear, they are not entirely exogenous to human actions—prices much less so than climate data—but they are not the direct digital expression of human actions. One can certainly see the qualitative difference here, which has bearing on how much policy can affect their underlying determinants. There is also a quantitative difference in how big either type can become: the growth, actual and potential, of big data for development as we define it is in all likelihood, significantly greater than that of these contextual big data, thus leading, in conjunction with their qualitative difference, to greater opportunities and challenges to affect human ecosystems. But the distinctive and defining feature of big data for development purposes is that these data are fundamentally different from the survey data that development experts and social scientists have

[40] See Samuel Arbesman, "Stop Hyping Big Data and Start Paying Attention to 'Long Data,'" *Wired Magazine*, January 29, 2013, available at www.wired.com/opinion/2013/01/forget-big-data-think-long-data/ .

[41] However, it must be noted that "for the purposes of global development, "real-time" does not always mean occurring immediately. Rather, "real-time" can be understood as information which is produced and made available in a relatively short and relevant period of time, and information which is made available within a timeframe that allows action to be taken in response i.e. creating a feedback loop, " UN Global Pulse, "Big Data for Development," p. 15.

[42] The last point was highlighted by Lea Shanley.

[43] See "Big Data is About People and Behavior," Enterra Insights, February 25, 2013, available at http://enterpriseresilienceblog.typepad.com/enterprise_resilience_man/2013/02/big-data-is-about-people-and-behavior.html .

[44] Thomas Goetz, "Harnessing the Power of Feedback Loops," *Wired Magazine*, June 19, 2011, available at www.wired.com/magazine/2011/06/ff_feedbackloop/all/1 .

[45] See Clay Shirky. More information available at www.shirky.com/ .

collected and relied on for decades.[46]

To summarize, for the purposes of this paper, big data for development (and conflict prevention) will be one of three types:

1. "digital breadcrumbs," following Sandy Pentland—which may include physical sensors (of electric usage for instance);
2. open web data (social media, blogs, online news, etc.), most of which is unstructured; and
3. remote sensing data using satellite imagery.[47]

Against this background, we now turn to cases where Big Data or roughly similar techniques have been and are being used for roughly similar purposes.

What Are the Current Uses of Related Techniques in Related Fields?

To date, a number of pilot and experimental projects have been implemented that can loosely be grouped under the umbrella of "Big Data for conflict prevention." But the majority may not qualify as such—either because they leverage technology rather than Big Data (analytics) specifically, or because they focus on counterterrorism or crime prevention rather than conflict prevention. This double distinction is important. First, the application of Big Data to conflict prevention problems remains in its infancy, and we need to delineate clearly the boundaries of the field of practice to identify its specific potential, obstacles, and requirements. Second, conflict prevention is based on a set of principles and practices meant to serve well-defined objectives, which can be at odds with those of counterterrorism or crime prevention, such that the application of Big Data to the principles and objectives of conflict prevention, may also yield specific challenges and requirements.

Most of these projects remain to be rigorously evaluated to draw lessons for Big Data for conflict prevention. As is often noted, Big Data does lend itself to over-promises and under-delivery, and while much needs to be done to unlock its potential, unrealistic expectations and misconceptions run against its objectives. So what can we learn about the realistic potential of Big Data from roughly similar techniques in roughly similar fields?

COUNTERTERRORISM, INTELLIGENCE, AND LAW-ENFORCEMENT

Counterterrorism, intelligence, and law-enforcement have intensive data requirements to feed the respective needs for detection, surveillance, evidence, and reporting. The characteristics of big data lend themselves well to these applications, allowing for real-time analysis of billions of records and alerts to improve situational awareness, among other things.

As Jeffrey Seifert notes:

> Data mining has become one of the key features of many homeland security initiatives. Often used as a means for detecting fraud, assessing risk, and product retailing, data mining involves the use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. In the context of homeland security, data mining can be a potential means to identify terrorist activities, such as money transfers and communications, and to identify and track individual terrorists themselves, such as through travel and immigration records.[48]

By 2011 the US Central Intelligence Agency (CIA) reportedly sifted through 5 million tweets a day.[49] More recently, various sources reported that the CIA had admitted to the "full monitoring of Facebook, Twitter, and other social networks."[50] The expectations are that Big Data will identify links between events and sequences or paths leading to national security threats, ultimately leading to forecasting future activities and events. While the ability to do so remains out-of-reach—and may remain so because of the complex nature of the

[46] John Cleland, "Demographic Data Collection in Less Developed Countries 1946-1996," Population Studies 50, No. 3 (November 1996): 433-450.

[47] Note that these correspond quite exactly to Global Pulse's 1st three categories.

[48] Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview," Congressional Research Service Report for Congress, January 28, 2007.

[49] See Kimberly Dozier, "CIA Following Twitter, Facebook," *Associated Press*, November 4, 2011, available at http://news.yahoo.com/ap-exclusive-cia-following-twitter-facebook-081055316.html .

[50] See RC Christian, "CIA Admits Full Monitoring of Facebook and Other Social Networks," Coup Media Group, January 29, 2013, available at http://coupmedia.org/intelligence-leaks/cia-admits-full-monitoring-of-facebook-and-other-social-networks-2901 .

systems examined—there are a number of practical applications that already use Big Data analytics. The US National Security Agency (NSA) is also reportedly building a "heavily fortified $2 billion center" in Utah, "a project of immense secrecy" meant "to intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks," that will provide further support to the notion that "the NSA has become the largest, most covert, and potentially most intrusive intelligence agency ever."[51]

Other US government initiatives are, on paper, less secretive. Programs like the Intelligence Advanced Research Projects Activity (IARPA)'s Open Source Initiative seek to "develop methods for continuous, automated analysis of publicly available data in order to anticipate and/or detect societal disruptions, such as political crises… disease outbreaks, economic instability, resource shortages, and responses to natural disasters."[52] Similarly, the Defense Advanced Research Projects Agency (DARPA) seeks to develop Big Data analytics and usability solutions for warfighters among other applications. DARPA also uses automated language translation technology for rapid translation of foreign languages to search materials for emerging threats and automated data search and pattern recognition applications, for example. Another initiative at DARPA is the XDATA program that seeks to develop scalable algorithms for processing imperfect, semistructured data and to create a usable visual human-computer interface to facilitate interaction and reasoning. DARPA is also involved in early warning through its Integrated Early Warning System (ICEWS).[53]

Big Data is also used for police work and public safety purposes. The New York City Police Department (NYPD) collaborates with Microsoft to aggregate and analyze existing public safety data streams in real time for investigators and analysts.[54] With a focus on high-risks sites, the result of this collaboration, the Domain Awareness System, pulls data from a network of 3,000 closed circuit cameras along with license-plate readers, 911 calls, past crime reports, and radiation detectors to identify threats. Although the trend started in the 1990's when police forces started to systematically gather and analyze data from high-crime areas, the advent and adoption of Big Data analytics, by allowing the search for patterns and correlations in vast quantities of high frequency data, are leading to the development of a radically new form of "predictive policing"[55] (or "predictive analytics"[56]) to "predict,"[57] "sense,"[58] "stop,"[59] or "fight"[60] crime "before it happens" (and as well as to inform decisions about resource allocation).[61] Such programs are already used in US cities beyond New York, like Los Angeles, Las Vegas, Seattle, Santa Cruz, Memphis, and Rochester, as well cities in the United Kingdom.

In an impressive example of the potential of predictive policing to date, biologists are using similar techniques and adapting a mechanism developed to study hunting patterns of wild animals

[51] All quotes are from James Bamford, "The NSA is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired Magazine*, March 15, 2012, available at www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/ .

[52] IARPA, "Open Source Indicators (OSI) Program," available at www.iarpa.gov/Programs/ia/OSI/osi.html .

[53] See Patrick Meier, "DARPA's Crisis Early Warning and Decision Support System," *Conflict Early Warning and Early Response*, March 20, 2010, available at https://earlywarning.wordpress.com/2010/03/20/early-warning-decision-support ; and Noah Shachtman, "Pentagon's Prediction Software Didn't Spot Egypt Unrest," *Wired Magazine*, February 11, 2011, available at www.wired.com/dangerroom/2011/02/pentagon-predict-egypt-unrest/ .

[54] "Mayor Bloomberg, Police Commissioner Kelly and Microsoft Unveil New, State-of-the-Art Law Enforcement Technology that Aggregates and Analyzes Existing Public Safety Data in Real Time to Provide a Comprehensive View of Potential Threats and Criminal Activity," New York City Press Release, August 8, 2012, available at www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2012b%2Fpr291-12.html&cc=unused1978&rc=1194&ndi=1 .

[55] See Charlie Beck, "Predictive Policing: What Can We Learn from Wal-Mart and Amazon about Fighting Crime in a Recession?" *The Police Chief*, November 2009, available at www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1942&issue_id=112009 .

[56] "Police Using 'Predictive Analytics' to Prevent Crimes Before They Happen," *Agence France-Presse*, July 29, 2012, available at www.rawstory.com/rs/2012/07/29/police-using-predictive-analytics-to-prevents-crimes-before-they-happen/ .

[57] Christopher Beam, "Time Cops: Can Police Really Predict Crime Before It Happens?," Slate, January 24, 2011, available at www.slate.com/articles/news_and_politics/crime/2011/01/time_cops.html .

[58] Frank Main, "Police Sensing Crime Before It Happens," *Chicago Sun-Times*, September 24, 2012, available at www.suntimes.com/3295264-417/intelligence-crime-police-weis-department.html .

[59] Ronald Bailey, "Stopping Crime Before It Starts," *Reason*, July 10, 2012, available at http://reason.com/archives/2012/07/10/predictive-policing-criminals-crime .

[60] See "Memphis PD: Using Analytics to Fight Crime Before It Happens," *IBM Smarter Planet Leadership Series*, available at www.ibm.com/smarterplanet/us/en/leadership/memphispd/ .

[61] See "Memphis PD."

to model and map street gang patterns in Los Angeles with impressive predictive power.[62] In a very practical way encountered by hundreds of millions of airline passengers, Big Data analytics are also central to airline passenger prescreening programs.

Another example is the integration of modern aerial reconnaissance; infrared sensors; color/monochrome daylight TV cameras; image-intensified TV cameras; laser designators and laser illuminators to create full-motion, real-time videos with viewing options combining multiple layers of information that can be used, for example, to send imagery to soldiers on the ground and track enemy movements, as in the case of the US Air Force's Gorgon Stare airborne surveillance program.[63]

In light of these innovations and the perceived potential of Big Data, the US Office of the Director of National Intelligence is sponsoring research projects involving fourteen universities in the United States, Europe, and Israel with the goal of using advanced analytics to predict significant societal events.[64]

The Obama Administration's commitment to pursuing Big Data for national security is also reflected in the approximately $250 million allocated for Big Data projects at the Department of Defense, including $60 million for research. The stated objectives are to improve situational awareness of warfighters and analysts, to provide increased support to operations, and more generally to harness and utilize massive data in new ways and bring together sensing, perception, and decision support to make truly autonomous systems that can maneuver and make decisions on their own.

COMMUNITY-LED USES: ACADEMIA, ACTIVISTS, CIVIL SOCIETY ORGANIZATIONS, CITIZENS

Another growing application of Big Data in a field roughly related to conflict prevention is the emerging applications to map and analyze unstructured data generated by politically active Internet use by academics, activists, civil society organizations, and even general citizens.[65] For example, in reference to Iran's post-election crisis beginning in 2009, it is possible to detect web-based usage of terms that reflect a general shift from awareness/advocacy toward organization/mobilization, and eventually action/reaction within the population.[66]

Further, data visualization of the Iranian blogosphere identified a dramatic increase in religiously oriented users. Text mining has also been used to shed light on shifting priorities and mounting concerns; for example a retrospective study of tweets and the Arab Spring found that in 2010 socio-economic terms ("income," "housing," "minimum wage") largely prevailed while in 2011, 88 percent were related to "revolution," "corruption," "freedom," etc. Understanding what matters to people and how their priorities and grievances change in qualitative and quantitative terms may help policy design.

Another application is mapping group composition and interaction using social network analysis (SNA). For example, by visualizing connections between Tea Partiers and Occupy Wall Street followers, analysts could tell that the Tea Partiers were a more tight-knit and insular group, whereas Occupiers had more connections and greater potential to scale up and expand.[67]

Bringing this kind of insight to active gangs, for instance, and correlating it with other kinds of data could certainly be useful.

Another kind of civilian-led application is trying to model and predict social upheavals and revolutions. One avenue has involved structured data mining by gathering and correlating them with past events. For example, mathematicians and computer

[62] Laura M. Smith, et al., "Adaptation of an Ecological Territorial Model to Street Gang Spatial Patterns in Los Angeles," submitted to *AIMS' Journals*, available at www.math.ucla.edu/%7Ebertozzi/papers/lauraDCDS12.pdf , cited in Bailey, "Stopping Crime Before It Starts."

[63] Ellen Nakashima and Craig Whitlock, "With Air Force's Gorgon Drone 'We Can See Everything,'" *The Washington Pos*t, January 2, 2011, available at www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html .

[64] Bernhard Warner, "What the Intelligence Community is Doing With Big Data," *Bloomberg Businessweek*, February 5, 2013, available at www.businessweek.com/articles/2013-02-05/what-the-intelligence-community-is-doing-with-big-data .

[65] These groups are in contrast to the intelligence community. Concretely this means that data and a range of tools, such as web data mining, that would traditionally be within the realm and privilege of the intelligence community are increasingly available to civilian.

[66] Luke Allnutt, "Pictures at a Revolution," *Foreign Policy Magazine*, April 11, 2012, available at www.foreignpolicy.com/articles/2012/04/09/pictures_at_a_revolution .

[67] According to *New Scientist* San Francisco Bureau Chief Peter Aldhous, "One key pattern to watch will be the number of disconnected Twitter users at the bottom right of each diagram. These can be viewed as the potential for growth for each movement, Smith suggests. Right now, that looks large for Occupy, and not so impressive for the Tea Party." Source: Peter Aldhous, "Occupy vs Tea Party: What Their Twitter Networks Reveal," *New Scientist*, November 17, 2011, available at www.newscientist.com/blogs/onepercent/2011/11/occupy-vs-tea-party-what-their.html .

scientists have developed a model that tracks food prices and makes predictions about the risk that a food riot may burst out.[68] In the case of the Arab Spring, these researchers say "they submitted their analysis warning of the risks of social unrest to the US government on Dec. 13, 2010. Four days later, Tunisian fruit and vegetable vendor Mohamed Bouazizi set himself on fire – an event widely seen as the catalyst for the Arab Spring."[69]

Other scholars have conducted similar exercises using global news media and conducting automated sentiment mining and mood detection in the cases of Pakistan, Egypt, and the Balkans, notably.[70] The findings of recurrent patterns in the data prior to major political events received significant attention and led to claims that "supercomputers can predict revolutions."[71] Other technological innovations and the democratization of existing applications of technology and data, such as satellite imagery, are further fueling the emergence and use of Big Data outside of the intelligence community.

Crisis maps based on multiple sources including text messages, tweets, and news reports have become a visual representation of Big Data applications.[72] Ushahidi and many other map-based applications are just some of the many applications that are transforming the web from a primarily text-based information platform for crisis prevention to a visual and multimedia one. Many of these are crowdsourcing platforms that enable the manual mapping of messages containing geographic references to increase situational awareness. Other progress toward the digitalization of data is the rapid emergence and diffusion of digital data collection tools such as the Open Data Kit, KoBoToolbox, or Magpi, which provide alternatives to paper-based data collection that are both rapid and efficient.

Together these tools provide academics, activists, and citizens with an unprecedented ability to monitor crisis-related data, and potentially prevent large-scale violence. The Satellite Sentinel Project–Now Signal Program at the Harvard Humanitarian Initiative is an example of such applications.[73] The project used satellite imagery analysis and field reports with Google's Map Maker to uncover evidence of alleged war crimes with the ultimate objective of deterring violence and the resumption of full-scale civil war between Sudan and South Sudan. Detailed satellite images did, for example, reveal potential mass graves and government efforts to conceal the site.

Applications of fourth generation of early-warning systems are also rapidly emerging, enabling civilian populations to contribute and access warning information. Crowdsourced data does not neatly fit under the definition of big data that we have outlined—because, as mentioned, it is actively produced by users to feed a given system, as opposed to data generated passively, but nevertheless it has become a major trend in working with communities at risks of conflict. Such systems mobilize communities or selected individuals within communities (which is then referred to as crowdseeding) to feed data from the ground, enabling a real-time information stream about events.[74] The advantages include a low-cost of implementation and ease-of-use among increasingly connected communities. These systems were in use, for example, in Kenya in anticipation of political violence during elections in 2010 and 2013, or in Kyrgyzstan during elections, when trained monitors at polling stations reported adverse events through a mobile messaging system. Similar text messaging systems implemented in connection with local villagers in DRC have been used to encourage rebels and child soldiers to defect.

[68] Maria Godoy, "Can Riots Be Predicted? Experts Watch Food Prices," *NPR*, October 2, 2012, available at www.npr.org/blogs/thesalt/2012/09/20/161501075/high-food-prices-forcast-more-global-riots-ahead-researchers-say .

[69] Ibid.

[70] Kalev H. Leetaru, "Culturomics 2.0: Forecasting Large-scale Human Behavior Using Global News Media Tone in Time and Space"*First Monday* 16, No. 9 (September 5, 2011), available at www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3663/3040 .

[71] Elizabeth M. Young, "Supercomputer Predicts Revolution," *Helium*, September 14, 2011, available at www.helium.com/items/2227645-supercomputer-predicts-revolution .

[72] See Crisis Mappers: The Humanitarian Technology Network available at www.crisismappers.net .

[73] See the Satellite Sentinel Project available at http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning/satellite-sentinel-project . It is worth noting that the project's focus is on a relatively small and well-defined geographical area, which does not result in very large quantities of data. The projected rise in meshed real time low orbit satellite technology will, on the other hand, result in far greater volumes of data.

[74] Patrick Meier, "From Crowdsourcing Crisis Information to Crowdseeding Conflict Zones." *iRevolution*, July 10, 2012, available at http://iRevolution.net/2012/07/10/crowdsourcing-to-crowdseeding .

The list of applications of Big Data to fields related to conflict may be endless, and a number of useful lessons and observations can be drawn from them. Two in particular are worth noting at this point. One is that none of these examples speak directly to conflict prevention as it has been practiced for years. For instance, as will be discussed in greater detail below, the actors, requirements, objectives, and "battlefields" of predictive policing are very different from those of typical early warning and response. Two, and relatedly, the practice of Big Data remains in its infancy when it comes to standards and guidelines to follow—first and foremost the principles of doing no harm. This will also be discussed further below. But these examples do point to avenues, risks, challenges, and desirable institutional frameworks for Big Data for conflict prevention to which the subsequent sections now turn.

How Can Big Data be Used for Conflict Prevention?

In light of the parameters and cases presented in the preceding two sections we start this new section by providing a few concrete examples of how Big Data could potentially help conflict-prevention initiatives, both structural and operational, before delving deeper into conceptual and normative considerations about its potential role(s) from a strategic and systemic perspective.[75]

DIGITAL PATTERNS AND SIGNALS FOR STRUCTURAL AND OPERATIONAL PREVENTION

It is first useful to distinguish what we might call "digital patterns" from digital "signals" in the data, and to clarify how these may relate to structural versus operational prevention.

Digital patterns refer to specific ways some processes and correlations may consistently show in the data—including some that may never have been previously seen. Such correlations may link two or more big data streams, or big data streams and other data streams—for example, climatological (rainfall, temperature) or economic (prices). On the other hand, digital signals refer to the occurrence of extreme or abnormal values in the data. Of course, neither concept is new—they respectively echo a long strand of research on pattern recognition as part of data mining, and the concept of "digital smoke signals" put forth by Global Pulse[76]—but they help structure the discussion.

On a broad level, as discussed previously, structural prevention requires understanding the socioeconomic and political processes at play in a given context to affect them in ways that will promote peace. On a broad level too, Big Data could help do so by "painting a finer picture" of a community as an ecosystem, as part of the aforementioned "real-time awareness" application of Big Data for development.

But before providing specific examples, one question that needs to be answered so as to delineate the universe of possibilities is how far one considers structural prevention to go. Some may argue that *any* development policy or program, and therefore *any* Big Data for development initiative, will automatically serve the purpose of structural conflict prevention (by aiming to address poverty, for instance), and should therefore be considered as a Big Data for conflict prevention initiative. But there are two caveats.

First, some development programs or policies may achieve goals that are largely unrelated to factors of instability and conflict—perhaps maternal mortality in some countries is a serious concern but does not stir tensions. On the other hand, programs may achieve development objectives but be insensitive to factors of instability and conflict.[77] The point here is that when conflict prevention is not an explicit goal of a program, we need to find those Big Data initiatives that can inform conflict prevention by uncovering the relationship between development goals and conflict dynamics.

Considering the subsets of Big Data for development initiatives that may realistically be useful for structural prevention, a number of options stand

[75] Other examples are discussed in GP's white paper and other articles including Emmanuel Letouzé, "Mining the Web for Digital Signals: Lessons from Public Health Research," *UN Global Pulse*, November 7, 2011, available at www.unglobalpulse.org/node/14534 and Vanessa Frias-Martinez and Enrique Frias-Martinez, "Enhancing Public Policy Decision Making Using Large-Scale Cell Phone Data," *UN Global Pulse*, September 4, 2012, available at www.unglobalpulse.org/publicpolicyandcellphonedata .

[76] Robert Kirkpatrick, "Digital Smoke Signals," *UN Global Pulse*, April 21, 2011 available at www.unglobalpulse.org/blog/digital-smoke-signals .

[77] The importance of conflict sensitive programming must be restated here. See Conflict Sensitivity Consortium, "Conflict-Sensitive Approaches to Development, Humanitarian Assistance and Peacebuilding: Resource Pack," available at www.conflictsensitivity.org/publications/conflict-sensitive-approaches-development-humanitarian-assistance-and-peacebuilding-res .

out. One important avenue is analysis of migration patterns through Big Data, with, for instance, a view to alleviate recurrent tensions between communities that may arise from such movements. This can be done using remote sensing or cell-phone data (CDRs),[78] or even email data.[79]

Another avenue is to study causes and expressions of concerns and stress in a given community—as has been done using Twitter in Indonesia[80]—in order to better understand and address them before they fuel grievances, for instance.

Yet another is to use CDRs to study slum dynamics[81] or the impact of human mobility on malaria transmission[82] to inform the design of conflict sensitive poverty reduction programs, or target vertical or horizontal inequalities.[83]

Overall, since there is growing evidence that "analysis of calling behavioral patterns can give an understanding of how citizens interact with their environments providing critical information relevant to areas like urban planning, crisis management or global health,"[84] it seems only fair to consider that this improved understanding could help structural prevention efforts.

These new data streams can provide information on individuals and communities in places where data is typically scarce, in close to real time, and at a finer level of specificity, which may help better understand how these human ecosystems function.

The potential for leveraging Big Data for operational prevention is equally promising. The question is how concretely Big Data may help detect these digital smoke signals of impending, ongoing, or the recent occurrence of violence.

The closest analogy is probably the use of Big Data for public health surveillance—or "Digital Disease Detection"—where, as in the famous cases of Google Flu and Dengue Trends, high-frequency and low-granularity data such as Google searches point to the specific timing and location of unusually high volumes of searches for key words.[85]

There are several actual and potential equivalents in the realm of operational prevention. The aforementioned use of satellite imagery to reveal alleged war crimes and mass movements is certainly one such case that falls neatly in the early warning category of Big Data for development.

Even closer to the Google Flu or Dengue Trend examples, conducting analysis of tweets or blog entries to detect rising tensions, frustration, or even calls to violence is also largely in the realm of possibility—and was done for hate speech ahead of Kenya's 2013 presidential elections.[86] In addition, a recent study of social media from Syria revealed that the locations of ceasefire violations or regime deployments could be identified within fifteen minutes of their occurrence. Another especially promising data type and avenue for operational prevention are CDRs and their analysis. However there is a need to build on current advances and formalization efforts to enhance the fast growing body of knowledge in the field.[87]

For instance, it would be greatly useful to try and analyze how known cases of violence are reflected in the data around the event location and date—

[78] See Joshua Blumenstock, "Inferring Patterns of Internal Migration from Mobile Phone Call Records: Evidence from Rwanda," *Information Technology for Development* 18, No. 2, February 3, 2012, available at www.jblumenstock.com/files/papers/jblumenstock_itd2012.pdf .

[79] See "You Are Where You E-Mail: Global Migration Trends Discovered In E-Mail Data," *Max-Plank-Gesellschaft Research News*, June 25, 2012, available at www.mpg.de/5868212/internet_demographics .

[80] "Twitter and Perceptions of Crisis-Related Stress," *UN Global Pulse and Crimson Hexagon*, December 8, 2011, available at www.unglobalpulse.org/projects/twitter-and-perceptions-crisis-related-stress .

[81] Amy P. Wesolowski, "inferring Human Dynamics in Slums Using Mobile Phone Data," available at www.santafe.edu/media/cms_page_media/264/AmyWesolowskiREUFinalPaper.pdf .

[82] See A. Wesolowski, "Quantifying the Impact of Human Mobility on Malaria," *Science* 338, No. 6104 (October 2012), available at www.sciencemag.org/content/338/6104/267.full.pdf .

[83] See notably Mats R. Berdal and David M. Malone, "Greed and Grievance: Economic Agendas in Civil Wars" (New York: Lynne Rienner, 2000) and Frances Stewart, "Horizontal Inequalities and Conflict: An Introduction and Some Hypotheses," in *Horizontal Inequalities and Conflict: Understanding Group Violence in Multiethnic Societies*, edited by Frances Stewart (Palgrave Macmillan 2010).

[84] Dr. Enrique Frias-Martinez, Head of the Smart Cities and Mobility Applications Initiative at Telefonica Research. Source: Frias-Martinez, "Enhancing Public Policy Decision Making Using Large-Scale Cell Phone Data."

[85] See Letouzé, "Mining the Web for Digital Signals: Lessons from Public Health Research," and "State of the Art in Digital Disease Detection," *iRevolution*, May 29, 2012, available at http://iRevolution.net/2012/05/29/state-of-the-art-in-digital-disease-detection . See also the Healthmap Project available at http://healthmap.org/about/ .

[86] Drazen Jogic, "Kenya Tracks Faceboo, Twitter for Election 'Hate Speech,'" *Reuters*, February 5, 2013, available at www.reuters.com/article/2013/02/05/net-us-kenya-elections-socialmedia-idUSBRE9140IS20130205 .

[87] Petteri Nurmi, "Data Analysis from Mobile Networks," Power Point lecture at University of Helsinki, September 2, 2012, available at www.cs.helsinki.fi/u/ptnurmi/teaching/LA12/Location_Awareness_LECTURE_VIII.pdf .

using existing conflict data sources. Key hypotheses that would need to be confirmed include:

1. How do call volumes change before, during and after a violent event? Do we notice spikes or collapses in call volumes?
2. How are mobility patterns affected? Are people moving away from or toward the event?
3. How are social graphs and networks affected? Are people changing their habits, contacting and reaching out to different people?

Again, as in the case of digital patterns and structural prevention, these examples and hypotheses make the simple point that individuals and communities change their behavior in the face of violence in ways that can be captured through digital devices and may act as smoke signals informing operational prevention efforts.

But the positive—i.e., factual—examples and arguments discussed up to this point also point to conceptual and normative considerations that need to be clarified in order to devise a truly strategic and systemic approach to Big Data for conflict prevention.

CONCEPTUAL CONSIDERATIONS AND FRAMEWORK

The foundational elements for thinking about and devising such an approach must now be put in place and in perspective. We highlight four considerations that inform the design of a simple conceptual framework.

The first and most important consideration is a proposition: just like different (theoretical) applications of Big Data for development have been put forth (as discussed in Section I), we propose that Big Data for conflict prevention be structured around three distinct functions:

1. **Descriptive**, i.e., Big Data can document and convey *what is happening*;
2. **Predictive**, i.e., Big Data could give us a sense of *what is likely to happen*, regardless of why;
3. **Diagnostic**, i.e., Big Data might shed light on *why things may happen*; the causes and nature of violent conflict.

A way to think about these is to recognize that functions two and three refer to different kinds of inferential analyses while, tautologically, function one is purely descriptive.

The potential for and implications of leveraging one or the other of these functions of Big Data for conflict prevention are very different. In particular, there is no evidence that innovations and improvements in information management platforms and visualization have been matched by similar innovations and improvements in our understanding of the structural factors and sequence of events that are correlated with or causally lead to violent conflict versus a peaceful outcome. In other words, while we are increasingly able to document what is happening (descriptive use), we remain, in the case of conflict, largely blind as to what will happen next (predictive use), and even more in the dark as to why this may be happening (diagnostic)—even if the literature on the causes of conflict—especially civil wars[88]—is vast and has improved our general comprehension of conflict dynamics over the years. Furthermore, being able to predict with any degree of confidence whether or not a conflict will occur does not imply understanding what would cause it or having the ability to stop it from happening. This is not to say that Big Data cannot help in doing all of the above, but we must first recognize the distinctive nature of these uses and the long road ahead.

One can also see how these functions can be complementary. Going back to the patterns versus signals dichotomy, it is clear that identifying the patterns is in most cases a prerequisite for detecting the signals, while in turn having observed the latter will help refine the modeling of the former. The underlying argument, true or false, is that human ecosystems and their inhabitants exhibit some normal behaviors picked up in the data, large deviations from which should act as warning signs or signals. Further, one can also argue that with a sufficient amount of trial and error, we may be able to infer causality out of correlations, and perhaps make better diagnostics. But, as discussed below, this takes much more than Big Data alone.

These three functions need to be connected to the practice(s) of operational and structural

[88] Christopher Blattman and Edward Miguel, "Civil War," *Journal of Economic Literature 48*, No. 1 (March 2010): 3-57, available at www.aeaweb.org/articles.php?doi=10.1257/jel.48.1.3 .

prevention to affect outcomes. But it is not clear how being able to better describe, and/or predict, and/or even understand the occurrence of violent conflict will generate better decisions let alone actions. Part of it speaks to what we will term a decision gap, characterized by the disconnect between information and action rooted in poor institutional design and/or functioning, and lack of political will.[89]

Information does not equal response. As was noted over twenty years ago vis-à-vis conflict early-warning systems, "There is little point in investing in warning systems if one then ignores the warnings!"[90] But the warning-response gap persists even though it is widely recognized that providing more information or analysis does not necessarily lead to a better outcome let alone any action. Conflict prevention is ultimately political. To this end, "early warning should not be an end in itself; it is only a tool for preparedness, prevention and mitigation with regard to disasters, emergencies and conflict situations, whether short or long term ones."[91]

While further analysis of this decision gap is largely outside of the scope of this paper, the relative democratization of Big Data also means that decisions are increasingly made by affected populations themselves, thus changing the nature and risks of decision gaps. In other words, conflict early response could possibly be crowdsourced rather than left to bureaucratic organizations, as is increasingly the case in disaster response.[92] Furthermore, "prevent[ing] violent conflict requires not merely identifying causes and testing policy instruments but building a *political* movement."[93]

A more hypothetical question is what would we do on the basis of available insights if there were no decision gap? Although this question has been asked many times in the conflict early warning arena over the years to try and avoid speaking about the elephants in the room—the institutional disconnect, the lack of political will—Big Data may bring about different challenges. For instance, how should predicting where and when a violent conflict may occur with some likelihood in a near or distant future affect policymaking and programming? The answer will be context dependent, but connecting points need to be in place.

Another aspect is that Big Data for conflict prevention may actually, over time, contribute to blurring the neat division between structural and operational conflict prevention. With very high-frequency data and the ability to tweak baseline models of human behavior in real-time, digital patterns and signals may become conceptually hard to distinguish. Big Data for conflict prevention could in time be concerned with unveiling digital signatures (in contrast to patterns versus signals) of various processes within human ecosystems, which may include signatures of peace and stability as much as signatures of mounting instability or pending violence. Under such an approach, structural and operational prevention may be merged under a new single "agile" conflict prevention category (and descriptive versus predictive uses merged into "nowcasting").[94]

Through this discussion we start seeing how a genuine need for greater conceptualization and structuring of a field of practice in the making (Big Data for conflict prevention) may err on the side excessive complexity. We propose a relatively simple conceptual framework that connects the three main functions of Big Data for conflict prevention (descriptive, predictive, diagnostic), the three major streams of big data for development, and the two main strands of conflict prevention (operational versus structural). A visual representation of the resulting conceptual framework in a three-dimensional space is presented in figure 2.

The proposed framework is a tool that can serve two purposes. One is to help think about and identify "hot spots" (in the form of smaller cubes)

[89] This point is discussed in further below.

[90] Meier, "New Strategies for Effective Early Response."

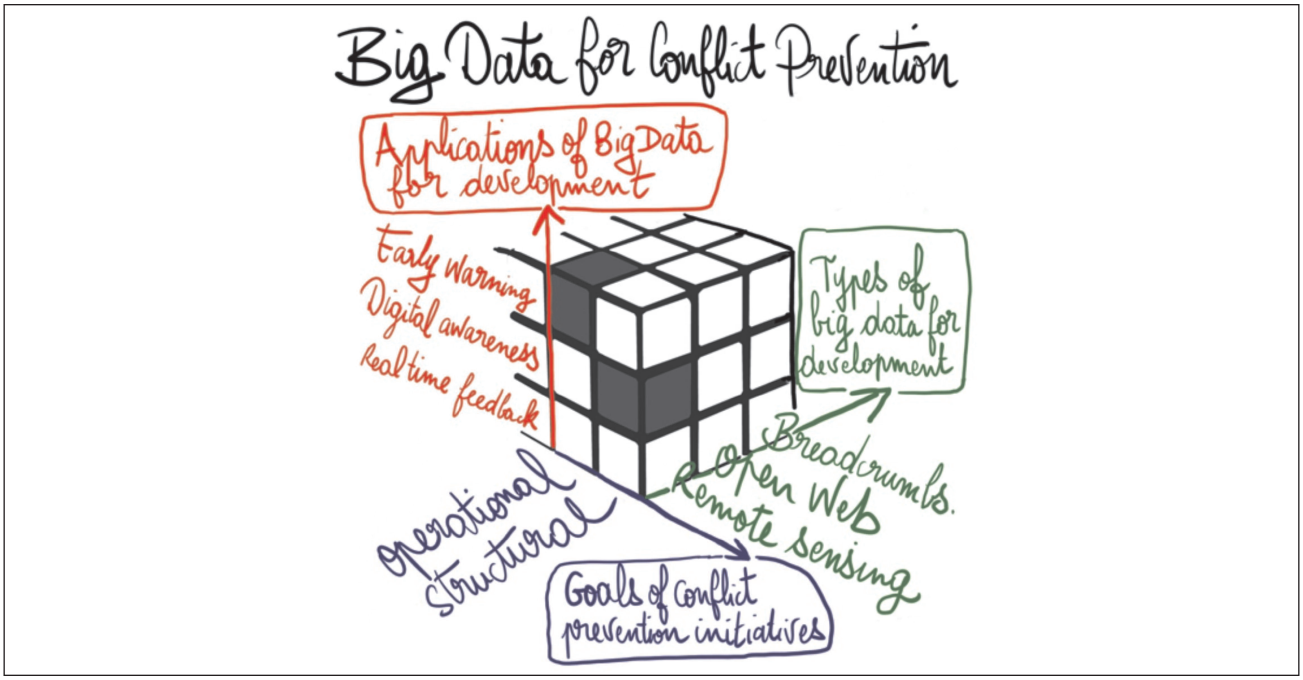
[91] Ibid.

[92] Patrick Meier, "How to Crowdsource Crisis Response," iRevolution, September 14, 2011, available at http://iRevolution.net/2011/09/14/crowdsource-crisis-response .

[93] See Rubin, "Blood on the Doorstep."

[94] This discussion touches on some of the arguments already developed in Emmanuel Letouzé, "Can Big Data From Cellphones Help Prevent Conflict?" *Global Observatory*, November 8, 2012, available at http://theglobalobservatory.org/analysis/380-can-big-data-from-cellphones-help-prevent-conflict.html . For more on agile development see Mitchell Toomey "Agile Development: What Human Development Can Learn from Software Development," *UNDP in Europe and Central Asia*, October 6, 2011, available at http://europeandcis.undp.org/blog/2011/10/06/agile-development-what-human-development-can-learn-from-software-development/ .

Figure 2: Framework


Big Data for Conflict Prevention
Applications of Big Data for development
Early Warning
Digital awareness
Real time feedback
Types of big data for development
Breadcrumbs
Open Web
Remote sensing
operational
structural
Goals of conflict prevention initiatives

with especially promising potential while not neglecting options that may not be immediately apparent. Certain cubes, rows or columns or combinations seem immediately more promising than others. For instance, there seems to be an obvious connection between the predictive function of Big Data for conflict prevention and operational conflict prevention (if and when the predictive function helps send warnings), and so across all three big data types. The same is true for the diagnostic function and structural prevention. But the framework also encourages its users to consider all possible combinations, such as, for example, whether and how the predictive use of Big Data for conflict prevention could actually inform structural prevention efforts if the prediction is about the likelihood of a negative event in some distant future. The model also helps think in terms of available or desirable data streams in a given context.

Another objective of the model is to allow communicating and presenting Big Data for conflict prevention to various target audiences and constituencies in an organized, structured manner. In other words it is envisaged as both an analytical and an advocacy tool.

Having laid out some options and tried to formalize the potential application of Big Data to conflict prevention on a conceptual and theoretical level, we must now turn to the identification of risks and challenges in the way before suggesting principles and institutions that may help alleviate them.

What are the Main Challenges and Risks?

GENERAL CONSIDERATIONS

A growing body of literature identifies the main risks and challenges of Big Data for development. The Global Pulse white paper dedicated a full chapter to the "Challenges" of Big Data for development, organized around two sub-sections: data and analysis.

The first data-related challenge identified in the paper pertains to the overarching privacy issue, defined by the International Telecommunication Union as the "right of individuals to control or influence what information related to them may be collected…and disclosed."[95] Privacy should remain the number one concern when developing Big Data for development and Big Data for conflict prevention in particular, given the peculiar security risks

[95] International Telecommunication Union, "Security in Telecommunications and Information Technology," December 2003, p. 2.

Six Provocations for Big Data

1. Automating Research Changes the Definition of Knowledge
2. Claims to Objectivity and Accuracy are Misleading
3. Bigger Data are Not Always Better Data
4. Not All Data Are Equivalent
5. Just Because it is Accessible Doesn't Make it Ethical
6. Limited Access to Big Data Creates New Digital Divides

Source: Boyd, Danah and Crawford, Kate, Six Provocations for Big Data (September 21, 2011).
http://dx.doi.org/10.2139/ssrn.1926431

that individuals may face in some highly dangerous environments. These concerns have also led to welcome progress on the way to "privacy-preserving data analysis,"[96] or simply to "balance privacy"[97] around ethical principles, technical solutions, and technological specifications that need to be supported. Another ethical consideration is the fact that data collection and analysis becomes part of the conflict context and changes the data producing actions of people, creating additional responsibility on the part of those creating and diffusing information.

The second set of data-related challenges discussed in the paper is access and sharing. One difficulty is simply the fact that a significant share of big data for development is privately held by corporations, notably telecom companies. And even if or when they are willing to share their data, many daunting legal and technological challenges come in the way. As in the case of privacy, options are also being developed, as discussed in the subsequent section. But, by and large, access to data is less of a technology problem than it is a partnerships challenge.[98]

With respect to analytical challenges, three clearly stand out—all of which are perhaps best articulated by Danah Boyd and Kate Crawford.

The major risk can be described as the effect of overconfidence that borders on arrogance, which can have serious consequences. A statement like the following is not exactly wrong but its assertiveness can be problematic in that it may reflect or fuel the belief that large-enough-quantities of data speak for themselves.

> New tools also enable remote assessment in places that are simply too risky for traditional on-the-spot evaluation. Analysts can use signatures—patterns of population movement, price fluctuations, market activity, or Internet usage, for example—to make informed judgments on the stability of a community over time.[99]

An inconvenient truth is that big data (and fine-grained measurement techniques) are terrific material for statistical shenanigans, biased fact-finding excursions that may lead to false discoveries, spurious correlations, confusion between correlation and causation, and more econometric and logical ills. The trouble with seeking a meaningful needle in massive haystacks of data, says Trevor Hastie, a statistics professor at Stanford, is that "many bits of straw look like needles." As a field, Big Data offers a high-tech twist on an old trick: I know the facts, now let's find 'em. That is, says Rebecca Goldin, a mathematician at George Mason University, "one of the most pernicious uses of data." Further, as Nassim Taleb warns, Big Data can lead to Big Errors.[100]

The "arrogant undercurrent in many Big Data debates where other forms of analysis are too easily sidelined,"[101] as much as the conviction that Big Data would make theory outright "obsolete"[102] are a particular concern in such complex and volatile

[96] Moritz Hardt and Guy N. Rothblum, "A Multiplicative Wights Mechanism for Privacy-Preserving Data Analysis," available at www.mit.edu/~rothblum/papers/pmw.pdf .

[97] See Groupe Speciale Mobile Association (GSMA) Director of Privacy Pat Walshe, Twitter profile available at @GSMA .

[98] UN Global Pulse, Twitter post, February 25, 2013, 8:52a.m., https://twitter.com/UNGlobalPulse/status/306084216804896768 .

[99] Kilcullen and Courtney, "Big Data, Small Wars, Local Insights."

[100] Taleb Nassim, "Beware the Big Errors of Big Data," *Wired Magazine*, February 8, 2012, available at www.wired.com/opinion/2013/02/big-data-means-big-errors-people .

[101] Danah Boyd and Kate Crawford, "Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon," *Information, Communication, and Society* 15, No. 5 (2012): 662-679, available at www.danah.org/papers/2012/BigData-ICS-Draft.pdf .

[102] Chris Anderson, "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete," *Wired Magazine*, June 23, 2008, available at www.wired.com/science/discoveries/magazine/16-07/pb_theory .

environments as conflict-affected or conflict-prone regions. It is especially imperative that analysts and policymakers remain vividly aware of the data and contexts they deal with—places where, among others, sample biases are typically large, where the accuracy and validity of big data remains widely questioned, especially where access to media and information technology is very limited.

In addition, as Alex de Waal warned over fifteen years ago about early-warning systems, "one universal tendency stands out: technical solutions are promoted at the expense of political ones."[103] But all conflict prevention is political.[104]

But other types of risks and challenge are especially salient in the case of conflict prevention.

SPECIFIC CONSIDERATIONS

For clarity purposes, we will distinguish "functional" risks and challenges and "institutional" risks and challenges.

The former refer to the substantive challenges and risks associated with the three functions of Big Data for conflict prevention proposed in section III. Some have been alluded to but are worth fully unpacking.

A first set of analytical challenges involves the predictive and diagnostic functions of Big Data for conflict prevention. Let us start by the identification of "smoke signals" as part of the predictive function, as discussed in section III. How confident can we be that "current attempts to build computer-based baseline of 'normal' human behavior on the basis of Big Data"[105] will ever be reliable enough to detect abnormality? As noted in the Global Pulse white paper (p. 34), "(e)ven within a well-specified human ecosystem—a village or a household—it is difficult to determine precisely ex ante a set of 'outputs' to be expected from a given set of inputs: adaptive and agile systems such as human groups will produce 'anomalies' provided the model forecasting expected behaviours or outputs is excessively stringent." It must be noted that a posteriori modeling exercises of the sorts discussed in Section II are hardly sufficient proof of their future reliability and usefulness: "forecasting (which we may arguably equate with predicting) is a real-time exercise, not a retrospective one."[106]

Further, event-based monitoring may indeed suggest signatures leading up to violence in the days and hours prior to the event, but robust prediction of rare events in a more distant future remains notoriously difficult.[107] A somewhat technical additional argument comes into play. Regardless of a predictive model's statistical accuracy, it can be shown that the expected number of errors known as "false positives" (here, predicting a conflict that actually never occurs) will always remain significant:[108] we may be getting very good at predicting which countries will not experience violent conflict but predicting only those that will is much harder.[109] In other words we are still very good at predicting ten of the next three conflicts—even if improvements in the specificity of these models (i.e., their ability to avoid false positives) in the specific cases of genocides and politicides are being observed.[110] If such predictions are made for allocation or attention purposes, they may not be that useful. The associated risk is that users not fully aware of these facts may indeed display overconfidence in their models.

How about diagnostic? Big Data's potential to actually improve of understanding of causal paths to violent conflict will be greatly undermined if we fail to be reminded and convinced that establishing causality requires much more than identifying

[103] Alex de Waal, *Famine Crimes: Politics and the Disaster Relief Industry in Africa* (Bloomington, IN: Indiana University Press, 2009).

[104] "Big Data for Development: From Information to Knowledge Societies," *iRevolution*, February 4, 2013, available at http://irevolution.net/2013/02/04/big-data-for-development-2/.

[105] See Patrick Wolfe in "Humans and Big Data: Who Is in Charge?," *BBC World Service*, November 24, 2012, available at www.bbc.co.uk/programmes/p010n7v4 . Whether and how this can be done is discussed in below.

[106] Ulfelder, "Supercomputer Predicts Revolution . . . or Not."

[107] Philip A. Schrodt, "Predictive Models for Political Instability," *White Paper in Response to SBE 2020*, available at www.nsf.gov/sbe/sbe_2020/2020_pdfs/Schrodt_Philip_157.pdf .

[108] George Box et al., "Detecting Malfunctions in Dynamic Systems," University of Wisconsin Center for Quality and Productivity Improvement, Report No. 173, March 1999), p. 4.

[109] For an overview of these concepts see GP's paper and for a more detailed discussion see Jay Ulfelder, "Why Political Instability Forecasts Are Less Precise Than We'd Like (and Why It's Still Worth Doing)," *Dart-Throwing Chimp*, May 5, 2011, available at http://dartthrowingchimp.wordpress.com/2011/05/05/why-political-instability-forecasts-are-less-precise-than-wed-like-and-why-its-still-worth-doing/ .

[110] See Chad Hazlett and Benjamin E. Goldsmith et al, "A Two-Stage Approach to Predicting Genocide and Politicide Onset in a Global Dataset," March 20, 2012, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2027396 .

correlations, whether spurious or real.[111]

These considerations point to the need, discussed in the subsequent section, to always clearly distinguish both functions—predictive versus diagnostic—as they involve or even require different research designs and serve different purposes.

Further, the non-representativeness of the data may be especially problematic in conflict zones if unequal access to technology—and thus to most data-generating devices—may mirror conflict fault lines (e.g., social or ethnic classes) or if it results from deliberate and targeted attempts at skewing the data (e.g., tweetbots). The potential consequence is that conflict prevention actors relying on these data could appear to be prejudiced against or partial to specific interest groups.

Institutional risks and challenges are no less serious. We already noted how the practice of Big Data remains in its infancy regarding standards and guidelines. In this respect, it is clear, for example, that the "general" challenge of big data privacy can soon turn into a security risk in conflict contexts, which poses the larger question of production, dissemination, analysis, use and archival within conflict zones. While Big Data in its civilian applications largely revolves around Open Data concepts, the risks associated with sensitive data related to conflict prevention are real. Even more troubling, it is already near certain that a number of authoritarian regimes, perhaps with the support of major donors and the participation of private corporations, are already engaging in advanced Big Data analytics "geared towards the command, control and censorship of inconvenient truths, identity groups and ethnic minorities."[111] There is no ready-made solution but this is one of the most critical aspects to bear in mind as we think about developing Big Data capacities in this area.

Another risk that was alluded to earlier is that of relocating the center of analysis from the field to headquarters, especially in, or more accurately, out of, dangerous places. As mentioned, Big Data may create a false sense of informed decision making being possible remotely, with no or little presence on the ground.

Yet another related risk is the possible emergence of a new digital divide. At the same time that technology and Big Data analytics reinforce the asymmetrical nature of warfare, we must also recognize the emergence of a growing digital divide—between the federal, state, and local levels of government, as well as between countries, as it relates to counterterrorism for example. A similar divide is emerging among conflict prevention actors, with remote actors being typically better served by technology, but not necessarily better informed on the local dynamic of conflict. Big Data may nurture an asymmetrical situation in which some agencies are able and willing to use Big Data (typically for predicting/forecasting purposes), while others don't. This would typically occur along the line of international versus national capabilities, which would hamper efforts to strengthen local capacities (and our understanding of conflict contexts). The fact of the matter is, "only corporate actors and regulators—who possess both the intellectual and financial resources to succeed in this race—can afford to participate [in big data analysis]," which may mean "that the emerging data market will be shaped according to their interests."[113]

This is especially concerning—or ironic—since, as stated earlier in this report, the recent literature on early warning and response systems has advocated for a people-centered approach: is the trend at risk of being reversed in the Big Data age?

The bulk of these concerns points to a final well-known and central challenge: how to make better information effect better outcomes. An aforementioned lesson from previous applications of technology to early warning and response systems is the response gap, which we can expand to a decision gap. Better insights—whether on emerging tensions, on causal paths to conflict, on early signs of violence—will not lead to better outcomes if the structural factors that underpin the decision gap are not changed. As Casey Barrs warned almost ten years ago:

> Today's prominent systems for warning about violence are designed to trigger this response

[111] Alex Howard, "Untangling Algorithmic Illusions from Reality in Big Data," *O'Reilly Radar*, March 4, 2013, available at http://radar.oreilly.com/2013/03/untangling-algorithmic-illusions-from-reality-in-big-data.html .

[112] Personal correspondence with Sanjana Hattotuwa.

[113] Cornelius Puschmann and Jean Burgess, "The Politics of Twitter Data," HIIG Discussion Paper Series No. 2013-01, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2206225 .

> from the outside to a growing crisis. Do these early warnings ever serve to get endangered civilians physically away from danger? Alerts, bulletins, and reports are sent around the world in real time. Yet they rarely touch ground where the killing happens. They fly through cyberspace, high over the victims' heads. People at risk on the ground might never learn that the demarches we write on their behalf even exist.[114]

But while, under most circumstances, "[a] democratic flow of information is the first condition for a democratic and open system of warnings and resolution,"[115] the specific nature of conflict zones may create a real dilemma and associated liability when the "democratization" of warnings and free flow of information may have to be balanced against the risk of panic or retaliation. Again, as in most cases, what is considered as the most appropriate course of action will be context dependent.

Let's end with a mention of a program that in many ways embodies all or many of the risks described above: the current development of "killer robots," i.e., "*fully autonomous* (our emphasis) weapons deployed on the battlefield."[116] Killer robots are not directly related to Big Data. But they are based on premises and paradigms that Big Data for conflict prevention must not embrace, chief of which is the notion that technology would make human inputs less and less relevant, when in fact quite the opposite is required. In general, the very notion of any system being "autonomous" when dealing with conflict zones should raise a bright red flag.[117]

Which Principles and Institutions Should Guide the Development of Big Data for Conflict Prevention?

The principles that guide the use of data in conflict-prevention efforts have largely been defined by academics and governmental or multilateral agencies. Such guidelines include, for example, regulations on the collection of data from human subjects[118] or on the use of sensitive data in human protection work.[119] This wide range of guidelines and principles are useful to the development of Big Data for conflict prevention. However, they are not always well-suited to handle emerging challenges that result from the increased speed and volume of data that is available and do not apply to actors who are increasingly outside of academia and government and multilateral agencies.

While enforcing a normative approach to Big Data on actors that are largely outside of formal institutions seems impossible, there is a consensus among these users that Big Data poses both legal and ethical issues, and that general principles are needed. Big Data for conflict prevention is particularly confusing because of the positive nature of its global aim. But this should not obscure the ethical concerns around accessing, for example, data on people's opinions or behaviors through systems with muddled privacy settings, nor obscure the fact Big Data can also do harm, whether purposefully or not.

The best principles and goals are useless if they are not translated into and supported by an adequate institutional architecture, broadly understood. The question here is what kinds of legal, technical, and administrative arrangements, agreements, protocols, and processes are best suited to the development of Big Data for conflict prevention as a field of practice? The truth is that answering this question is largely beyond the scope of this paper and should constitute a priority area for future research and discussion. What this section does, though, is sketch what such an institutional architecture may look like.

A useful way to think about the principles and institutions in relation to Big Data for conflict hinges on two main factors: the underlying human and institutional intent and capacity, which are

[114] Barrs, "Conflict Early Warning: For Who?"

[115] Kumar, *The Quest for a Disaster Early Warning System*.

[116] Human Rights Watch, "Losing Humanity," November 19, 2012, available at www.hrw.org/reports/2012/11/19/losing-humanity .

[117] For a current illustration may be found in the malicious use of Internet bots see "Bots for Civic Engagement at SXSW," MIT Center for Civic Media, available at http://civic.mit.edu/blog/kanarinka/bots-for-civic-engagement-at-sxsw .

[118] See for example the *Helsinki Declaration* (1964) available at www.onlineethics.org/Topics/RespResearch/ResResources/helsinki.aspx .

[119] See for example International Committee of the Red Cross (ICRC), "Professional Standards for Protection Work Carried Out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence," Geneva: ICRC, November 24, 2009.

merely amplified by technology.[120] Shaping the right intent depends primarily on abiding by sound principles, and building the right capacities depends largely on having in place appropriate systems and policies, which we lump under the generic term institutions.

PRINCIPLES

The principles that should shape the underlying intent of Big Data for conflict prevention fall at the intersections of several ethical and policy concerns. Key elements are identified here that build on already existing principles and reflect specific concerns that come with Big Data. These principles are closely intertwined, but it is useful to try and separate them for clarity purposes.

The first set of principles echoes the well-known ethic of first Do No Harm. Big Data for conflict prevention needs to be sensitive to the dynamic and nature of the local context and potential for violence to erupt. This requires being consistently and systematically mindful of well-identified risks and challenges especially those that have already materialized in the past or are clearly about to materialize—including the previously mentioned risks of overreliance and arrogance associated with Big Data. Included in the Do No Harm principle is the notion that the security of all involved in the process from data sources to intermediaries and data analysts must be ensured. This requires more careful guidelines on how data can be used (shared, transferred, analyzed, etc.). This also requires the use of data only at the needed level of detail and/or to carefully monitor or restrict access to data that may endanger the privacy and security of the individuals concerned. Another avenue to protect privacy and other individual rights in the long term is the possibility of using data that would come with an "expiration date," echoing ongoing current discussions on an Internet that is able to forget and the "erasable future of social media."[121]

For the purpose of Big Data for conflict prevention we will also include under the Do No Harm heading the notions of impartiality and neutrality that are central to humanitarian work. In particular, given the critics and risks around the representativeness, reliability, and statistical validity of Big Data in general and for conflict prevention in particular actors must strive to provide reliable, accurate, and updated information that is verifiable and at the required level of precision and detail for its intended use.[122] Big Data for conflict prevention must operate in a learning environment where feedback loops and lessons learned contribute to advancing its applications.[123] The risk for impartiality and neutrality is that flawed analysis will lead to potentially biased intervention. It is also possible that Big Data will be influenced under the mobilization of interest groups, leading to further intervention biases.

A second general key principle can be termed contextualization through empowerment (and vice-versa). The Global Pulse whitepaper defined contextualization in terms of both "Data context," referring to the fact that "indicators should not be interpreted in isolation" and "cultural context," referring to that fact that "knowing what is 'normal' in a country or regional context is prerequisite for recognizing anomalies. Cultural practices vary widely the world over and these differences certainly extend to the digital world. There is a deeply ethnographic dimension in using Big Data." The data context and cultural-ethnographic context are critical and highlight the importance of relying on local insight. "The big data and local insight must be integrated and used to shape a solution with the help of design thinking."[124] The need to consistently and constantly bear in mind this deeply cultural, anthropological, and ethnographic

[120] Kentaro Toyama, "Can Technology End Poverty?" *Boston Review*, November/December 2010 available at www.bostonreview.net/BR35.6/toyama.php .

[121] Mark Wilson, "What UIs Need Now: Built-In Options to Destroy Data," *Fast Company Design*, available at www.fastcodesign.com/1671882/what-uis-need-now-built-in-options-to-destroy-data and Felix Gillette, "Snapchat and the Erasable Future of Social Media," *Bloomberg Businessweek*, February 7, 2013, available at www.businessweek.com/printer/articles/95976-snapchat-and-the-erasable-future-of-social-media .

[122] See ICRC, "Professional Standards for Protection Work Carried Out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence."

[123] Quote from Goetz, "Harnessing the Power of Feedback Loops": "A feedback loop involves four distinct stages. First comes the data: a behaviour must be measured, captured and stored. This is the evidence stage. Second, the information must be relayed to the individual, not in the raw-data form in which it was captured but in a context that makes it emotionally resonant. This is the relevance stage. But even compelling information is useless if we don't know what to make of it, so we need a third stage: consequence. The information must illuminate one or more paths ahead. And finally, the fourth stage: action. There must be a clear moment when the individual can recalibrate a behaviour, make a choice and act. Then that action is measured, and the feedback loop can run once more, every action stimulating new behaviours that inch us closer to our goals."

[124] Kilcullen and Courtney, "Big Data, Small Wars, Local Insights."

dimension of Big Data is one of the most important messages of this report.[125] On the demand side, contextualization means that Big Data for conflict prevention should respond to the demands of local populations, not to international priorities.

Contextualization can also be understood as taking context as a starting point as far as using and developing local capacities are concerned in order to empower communities. Big Data for conflict prevention should strongly support capacity development and integration with local actors not only to tap into local insights, but as a means to avoid the advent of a new digital divide.

This should not be considered as rehearsed development lingo: there is a real risk that Big Data may undo years of efforts to try and use technology to put affected community at the center of conflict prevention, on both the demand and supply sides. Big Data for conflict prevention *must* be geared toward one major objective: empowering at risk communities.

The third related principle is that of incrementality. One aspect is to recognize that, as a field in the making and given the many challenges in the way, Big Data for conflict prevention should rather "start small"[126] to be subsequently scaled up as capacities are built and lessons learned according to some simple yardsticks.[127] For instance, this may first take the form of digitalization of the vast amounts of traditional forms of administrative, survey, and census data collected by and held by national statistical agencies and government departments. This too may sound like rehearsed speech, but we cannot stress enough that while capital and resource-intensive (and top-down) approaches to conflict prevention in the form of national security programs will continue to make enormous strides forward, the really exciting and responsible use of Big Data for conflict prevention should not be based on that model. At the same time, despite progress toward the development of people-centered approaches, many international organizations and NGOs remain stuck in the external, top-down approach to conflict prevention. Big Data for conflict prevention should provide an opportunity to depart from those practices rather than reinforce them.

The last key principle is that of clear intentionality. This especially refers to the need to specify which goal any Big Data for conflict prevention initiative is expected to serve—not just in terms of structural versus operational prevention, but in terms of the predictive versus diagnostic functions of Big Data for conflict prevention. As put by Jay Ulfelder:

> We might be able to develop a predictive model that accurately identifies emerging conflicts without really learning anything new about why those conflicts are happening or, maybe more important, which preventive actions might be more effective than others. And vice versa: a statistical analysis designed to test whether or not certain features or interventions reduce the risk of conflict usually wouldn't lead immediately to a better predictive model. One of the first decisions anyone interested in using Big Data for conflict prevention has to make for any given project is this one. Over time, the two should complement each other, but any single project will need to pick. Equally important, consumers of these analyses need to understand that models constructed from these data don't magically make this dilemma disappear.[128]

But a daunting task remains: how can these principles inform and be translated into appropriate institutional design and affect outcomes on the ground? Even more so than in the case of these ethical and policy principles, our goal is to sketch desirable features and suggest potential avenues rather than providing a fully fleshed-out proposal. But starting to talk about institutions is critical.

PRIORITIES FOR INSTITUTIONAL DESIGN

The most promising institutional modality is that of partnerships and collaborative work, understood in

[125] For a good overview of the debates see "The Ethnographer's Complete Guide to Big Data: Small Data People in a Big Data World (Part 1 of 3)," *Ethnography Matters*, May 28, 2012, available at http://ethnographymatters.net/2012/05/28/small-data-people-in-a-big-data-world/ and notably, Panthea Lee, "Reaching Those Beyond Big Data," Ethnography Matters, March 6, 2013, available at http://ethnographymatters.net/2013/03/06/reaching-those-beyond-big-data/ .

[126] Bill Franks, "To Succeed with Big Data, Start Small," *Harvard Business Review Blog Network*, October 3, 2012, available at http://blogs.hbr.org/cs/2012/10/to_succeed_with_big_data_start.html .

[127] CMO Network, "Unleash the Brawn of Big Data With Small Steps," *Forbes*, February 12, 2013, available at www.forbes.com/sites/onmarketing/2013/02/12/unleash-the-brawn-of-big-data-with-small-steps/ .

[128] Personal correspondence with Jay Ulfeler reproduced with his authorization.

several complementary ways. One set of partnerships needs to be built around and support the concept of "Data Philanthropy"[129] put forth by many observers to avoid "the tragedy of the data commons."[130] Indeed, as mentioned in the previous section, a large share of big data for development is held privately. Getting private corporations to share their data and finding ways for them to do so in a privacy-preserving way is a necessity. But in light of all the aforementioned risks another appealing type of partnerships could be devised around the concept of "analytics philanthropy."[131] Concretely, institutional arrangements would link complementary actors, both local and internationals, around specific research projects, in full recognition and observance of the ethical and policy principles described above. A wide range of possible administrative modalities and workflow models can be envisaged from the more traditional—fellowships, technical assistance, joint papers, MoUs, focal points, working groups, fully integrated structures—to more innovative approaches that only beg to be imagined. To suggest only one for discussion, it may be possible to envisage the creation of regional Big Data hubs pooling together resources and personnel from various surrounding countries and institutions. The point is that the admittedly difficult task of linking grassroots groups and bigger organizations is a key to the sound development of Big Data for conflict prevention.

A second set of institutional requirements involves coming up with appropriate underlying technical protocols, technological tools, legal frameworks, and data standards needed to support any data and/or analytical philanthropy arrangements. For instance, how may data be shared in a privacy-preserving way? As a case in point—although the relevance to conflict contexts may need to be thought through and debated more deeply—Global Pulse has proposed four ways for sharing data that largely reflect the aforementioned ethical and policy principles and could serve as a starting point for discussion. Similarly, an expiration feature added to some or all data could be coded at the XML/metadata level so that information gathered during emergencies and/or for a specific purpose do not live on platforms forever.[132] This clearly requires working closely with technology teams.

The case of legal frameworks and data standards is also highly complex. Although neither can be seriously addressed in a few lines, it is clear that National Statistical Offices will, in most cases, have to be involved along with the legislature to devise standards and rules. Difficult questions will certainly arise in the case of authoritarian governments and repressive regimes.

Conclusion

The application of Big Data to conflict prevention raises many hard questions that will continue to be discussed for some time to come. This paper has sought to provide an improved conceptual foundation for future debates.

In order to do so, we narrowed the definition of big data to those data that are unintentionally generated by human actions and picked up by digital devices, or as the digital translation (understood in its literal sense) of human actions. We excluded purposefully generated information (e.g., crowdsourcing) while recognizing its value for conflict prevention.

Big Data for conflict prevention may be a subset of the applications of Big Data for development, sharing many common features. But it is also a growing field of practice with its own characteristics and challenges. In this paper, we argued that Big Data for conflict prevention can serve three distinct functions—descriptive, predictive, and diagnostic. These applications are at very different levels of practice and much theoretical development is needed before we can establish and act upon accurate and reliable prediction and diagnostics of conflicts.

Much can be learned from innovations in the fields of counter-terrorism and law enforcement

[129] Michael J. Coren, "Data Philanthropy: Open Data for World-Changing Solutions," *Fast Company Design*, available at www.fastcoexist.com/1678963/data-philanthropy-open-data-for-world-changing-solutions .

[130] Jane Yakowitz, "Tragedy of the Data Commons," February 2011, available at http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=jane_yakowitz .

[131] "Big Data Philanthropy for Humanitarian Response," *iRevolution*, June 4, 2012, available at http://irevolution.net/2012/06/04/big-data-philanthropy-for-humanitarian-response/ .

[132] Wilson, "What UIs Need Now."

and uses of Big Data among academics, activists, civil society organizations, and even general citizens. But there is also a need to go beyond pilot projects and occasional applications of Big Data for conflict prevention, and examine its potential by investing in long-term development and learning processes.

What is also needed is a structured and systematic way to address the emerging ethical challenges and principles that should guide the responsible use of Big Data for conflict prevention. This paper outlined and discussed these issues, proposing a basic set of principles and ways of working, but how this will be applied in practice remains to be seen.

Big Data for conflict prevention must be developed bearing in mind the lessons and insights from the field of conflict prevention and conflict early warning and early response. The fact is that many such efforts have failed, not so much for lack of information as for lack of political will. We mentioned in particular that there is no evidence that we would be better prepared to prevent the Rwanda genocide today than we were in 1994. So a key dimension is bridging the decision gap. Until and unless we are ready and willing to do so, Big Data, no matter how big, will not affect outcomes and save lives.

Fundamentally, this must be done through the democratization of information, access to technology, and empowerment. A dimension that will require further work is whether and how Big Data can empower nonviolent, civil resistance movements. Even—or especially so—with Big Data, a more distributed and decentralized approach to conflict prevention is still the most promising path forward. Conflict prevention is and remains a primarily political issue. As we noted, the advent of Big Data runs the risk of turning this inherently political issue into a technical optimization challenge.

As our title suggests, there may be something ironic, naïve, or even risky, about considering that this “new oil,” dismissed at times as a mere buzzword, could help fight a blaze that has consumed so many lives for so long. Our main hope is that this paper will provide an analytical and conceptual basis on which future discussions of the complex ethical, political, institutional, technological, and legal dimensions of Big Data for conflict prevention can take place so that perhaps new oil can indeed contribute to abating old fires.

Using Information and Communication Technologies for Violence Prevention in Latin America

Robert Muggah and Gustavo Diniz[1]

Latin America is the developing world´s most digitally connected region, but also its most violent. Indeed, Latin America is witnessing a digital revolution: almost half of its population is online, and the continent is fast becoming the planet´s largest producer and consumer of social media.[2] Part of this surge is driven by rapid economic growth and the demographic and sociocultural constitution of societies in Central and South America. Yet Latin America also features the world´s highest rates of organized and interpersonal violence, with most perpetrators and victims under the age of thirty. While not confronted with war in the conventional sense, many societies bare all the hallmarks of armed conflict. Not surprisingly, governments and civil societies are evolving new and dynamic approaches to mobilizing information and communication technologies (ICTs)[3] to strengthen the voice and capabilities of citizens to prevent and reduce violence.

This paper reviews the character and shape of ICTs for violence prevention in Latin America. In drawing primarily on the cases of Brazil, Colombia, and Mexico, it highlights the history and evolution of digital approaches to tackling violence and crime across the region. It considers the density and diversity of ICTs for violence prevention since the 1990s; the factors shaping their onset and spread; the role of governments, international organizations, and citizen groups in fueling the information revolution; and wider outcomes and impacts. It is worth noting that the topic is comparatively nascent in Latin America, and that experiences are still very much untested. Indeed, this paper constitutes the first overview of ICT's emergence and spread in the area of violence prevention. Thus, while issuing some recommendations on lessons learned, these are very tentative and preliminary. Indeed, further research is urgently required to test interventions and measure outcomes.

Spread and Impact of Latin America´s ICT Networks

Latin America is undergoing a digital revolution having witnessed a massive regional expansion of Internet use, especially among younger population groups. Almost half of the population of Central and South America are connected to the web—far ahead of counterparts in Asia or Africa.[4] Roughly two thirds of all users are under the age of thirty-five. Online access has grown thirteen-fold over the past decade, with a tenfold increase in mobile subscriptions over the same period. Countries as diverse as Argentina, Brazil, Chile, El Salvador, Honduras, Panama, and Uruguay have one cell phone per inhabitant with smartphone ownership increasing rapidly.[5] What is more, Latin American Internet users are coming online using mobile devices, not laptops, thereby increasing the spread of certain features over others.[6] It is worth emphasizing, however, that the regional and subregional distribution of users is still unequal: there are massive disparities in Internet penetration rates that also mirror the inequities within many Latin American societies. Indeed, there are strong correlations between Internet access and wider

[1] Robert Muggah is the research director of the Igarapé Institute, a principal of The SecDev Group, and a professor at IRI-PUC in Rio de Janeiro, Brazil. Gustavo Diniz is a researcher at the Igarapé Institute.

[2] Gustavo Diniz and Robert Muggah, "A Fine Balance: Mapping Cyber (In)security in Latin America," Igarapé Institute, Strategic Paper 2, June 2012, available at http://pt.igarape.org.br/a-fine-balance-mapping-cyber-insecurity-in-latin-america/ .

[3] Information and communication technologies include information collection, sharing, and analysis via Internet and communications through various platforms.

[4] Roughly 43 percent of Latin American residents are online (or 255 million people) as of 2012 compared to 27.5 percent of Asian residents and 15.6 percent of African residents. See www.internetworldstats.com .

[5] Although 3G technology allowing remote access to Internet is still incipient in the region, telecoms are investing heavily in this domain and an increase in this market is expected for the coming years. Industry analysts predict that by 2016 smartphones capable of accessing high-speed Internet will account for over 50 percent of all cell phone sales in the region.

[6] In other words, GPS, microphones, and camera usage is becoming a more common aspect of the online experience. Personal interview with Google Ideas, January 2013.

Figure 1: Internet Penetration in Latin America[7]

Country	Internet Users	Penetration (% of population)	HDI (global ranking 2011)
Argentina	28,000,000	**66.4**	45
Colombia	26,936,343	**59.5**	87
Chile	10,000,000	**58.6**	44
Uruguay	1,855,000	**55.9**	48
South America	189,982,457	**48.2**	—
Brazil	88,494,756	**45.6**	84
Ecuador	6,663,558	**43.8**	83
Costa Rica	2,000,000	**43.1**	69
Panama	1,503,441	**42.8**	58
Venezuela	12,097,156	**41.0**	73
Mexico	42,000,000	**36.5**	57
Peru	9,973,244	**36.5**	80
Central America	51,452,595	**32.6**	—
Suriname	179,250	**32.0**	104
Guyana	250,274	**32.0**	117
Bolivia	3,087,000	**30.0**	108
El Salvador	1,491,480	**24.5**	105
Paraguay	1,563,440	**23.9**	107
Belize	74,700	**22.8**	93
Guatemala	2,280,000	**16.2**	131
Honduras	1,319,174	**15.9**	121
Nicaragua	783,800	**13.7%**	129

patterns of poverty, inequality, socioeconomic class, and urbanization (see figure 1).[8]

Nevertheless, given the sheer scale and demographics of Latin America´s digital natives, it is hardly surprising that they are among the world´s most active users of social media. Indeed, six Latin American countries are included in the top ten most actively spending time in web-based social networks.[9] Both Facebook and Twitter are spreading rapidly, reaching membership levels equivalent to upper-income settings (see figure 2).[10] Moreover, given that populations across the region share language and cultural affinities, Latin America´s cyberspace is one of the world´s richest in terms of social media production and consumption. That said, Latin Americans are comparatively timid in terms of their use of ICTs to express wider political and social grievances. Latin America has not witnessed events as intense as an Arab Spring or an Occupy movement. The closest analogous experiences are the Chilean student protests and the Mexican pro-democracy movements known as #YoSoy132 and #1DMx. Brazil only recently experienced incipient movements in this direction,[11] although there are strong indications that things are changing quickly and digital mobilization will increase across Latin America in the years to come. At any rate, so far the expansion in Internet use and,

[7] See Internet World Stats, www.internetworldstats.com (results from June 30, 2012).

[8] In Brazil, for instance, while 50 percent of households in São Paulo, Rio de Janeiro, Minas Gerais, and Espírito Santo have Internet access, this number is only 22 percent in the Northern region. What is more, on average the richest people spend much more time on the Internet than the poor. The proportion of those who go online at least one time per week is about 80 percent for upper-class users, 65 percent for middle classes, and less than 50 percent for lower classes. See www.cetic.br/usuarios/tic/2011-total-brasil/index.htm .

[9] These are Argentina, Brazil, Chile, Colombia, Mexico, and Peru.

[10] See http://semiocast.com/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US for a review of twitter trends in selected countries and cities.

[11] The conservative candidate Celso Russomano, counting with solid support of the Neo-Pentecostal churches, was leading polls for the municipal elections in São Paulo by a large margin. A movement started on the web—called #ExisteAmorEmSP (ThereIsLoveInSP)—reversed the results with only a few days left before the voting, helping labor party's candidate Fernando Haddad to be elected. Another interesting case of digital mobilization in Brazil involved the indigenous group Guarani-Kaiowá (see www.huffingtonpost.com/2012/10/31/guarani-kaiowa-eviction_n_2051454.html).

Figure 2: Facebook Penetration and Growth, 2011–2012[12]

Subregion	Facebook Accounts		Penetration (% of population)	
	Mar 2011	Mar 2012	Mar 2011	Mar 2012
South America	69,594,760	112,531,100	17.4 %	28.1%
Central America	28,090,240	41,332,940	18.0%	26.5%

by definition, information and communication technologies has generated a host of paradoxical outcomes across political, social, and economic spheres.

On the positive side of the ledger, there appears to be a marked surge in ICT use by governments to enhance citizen participation in elections, as well as in decision making and planning. After decades of dictatorships and repressive governance, some governments in Latin America are going online in a bid to modernize public institutions and service delivery functions through e-gov platforms and to publicize expenditures and activities through open-data initiatives. Likewise, small- and medium-sized businesses are investing heavily in e-commerce sites, while most large banks have made the shift to e-banking services. A growing number of public and private universities and schools are also investing in distance learning, while civil society groups are using the net to recruit members, raise funds through crowd-funding mechanisms, and increase public awareness. There are grounds for cautious optimism that such activities will grow in pace and scale. Even grassroots movements are pushing for more access to bridge the digital divide and strengthen their demands, such as the *autochthon* peoples in Bolivia, Brazil, and Peru.

More negatively, cyberspace has become fertile territory for criminal activity. New and emergent forms of digital criminality are taking advantage of expanding (and poorly regulated) connectivity across Latin America. Much of this is economically driven and includes criminal hacking (cracking), data and identity theft, advanced credit card fraud, phishing, and online child exploitation. What is more, "old" crime is increasingly migrating online with a combination of narco-cartels and drug dealers, gang members, human traffickers, and others seeking recruits and also selling wares using Google, Facebook, Twitter, and Youtube services.[13] Latin America has seen a rise in the use of social media for the open selling of illicit drugs through Facebook and Orkut, as well as in the so-called "deep web" (e.g., Silk Road), but also for money laundering, extortion, and other organized criminal activities. In the most extreme cases, as with cartels in Mexico, social media is effectively being "hijacked" to send messages of intimidation and harassment to public officials, political and economic elites, journalists, activists, and others. There are widely publicized accounts of prominent social media users being targeted and killed in Latin America, and likely many more cases that go unreported.[14]

There is also a "gray zone" of social media activity that persists in Latin America, as in other parts of the world. Hacktivism in particular is growing, including with prominent engagement from major decentralized networks such as Anonymous and LulzSec. These and other groups have undertaken massive "denial of service" attacks against Latin American governments, banking establishments, and private businesses in retaliation for what they see as injustices. Often they threaten to release sensitive and confidential data to expose corrupt authorities, while in other cases they dump such information into the mainstream media. While serving a "watch

[12] For comparison, Facebook penetration rates worldwide are the following: North America (49.9 percent), Oceania/Australia (38.4 percent), Europe (28.5 percent), Middle East (9.4 percent), Asia (5.0 percent), Africa (3.9 percent). See Internet World Stats.

[13] See Nacha Cattan, "How Mexican Drug Gangs Use YouTube Against Rival Groups," Christian Science Monitor, November 5, 2012, available at www.csmonitor.com/World/Americas/2010/1105/How-Mexican-drug-gangs-use-YouTube-against-rival-groups and also Sarah Womer and Robert Bunker, "Sureños Gangs and Mexican Cartel Use of Social Networking Sites," *Small Wars & Insurgencies* 21, No. 1(March 2010): 81–94, available at www.tandfonline.com/doi/abs/10.1080/09592310903561486 .

[14] See, for example, Neal Ungerleider, "Mexican Narcogans' War on Digital Media," *Fast Company*, October 6, 2011, available at www.fastcompany.com/1785413/mexican-narcogangs-war-digital-media and "Delincuencia organizada infiltrada en redes socials," *Blog del Narco*, April 9, 2011, available at www.blogdelnarco.com/2011/04/delincuencia-organizada-infiltrada-en-redes-sociales/ .

dog" function, they also test the balance between online freedom and security. Owing in large part to a relatively under-regulated cyberspace and an under-developed cyber-security infrastructure, they see Latin America as a safe haven for the privacy and protection of individual rights on the net.[15] What is more, cyberactivism's comparative appeal is enhanced in environments where more traditional grassroots activism is less welcome.

Governments and private sector actors are gradually responding to cybercrime and hacktivism, albeit in a piecemeal manner. Specifically, cybersecurity interventions are expanding, some of them targeting computer, content, and copyright crime, as well as "digital violence" involving targeted harassment, intimidation, and extortion. Most states across the region are developing units under the framework of the Organization of American States' Inter-American Strategy to Combat Threats to Cybersecurity established in 2004. The most common institutionalized responses are so-called computer security incident response teams, the elaboration of criminal legislation for cybercrime offenses, the formation of specialized cybercrime units in law enforcement and justice departments, and the development within civil society of awareness-raising services and reporting on violence, victimization, and human rights abuses.

Dynamics of Violence in Latin America

While Latin America has witnessed a massive expansion and spread in Internet connectivity and ICT use, it has also experienced an unprecedented surge in organized and interpersonal violence. And while all countries and societies around the world experience violence in distinct ways, the scope and scale of organized and interpersonal violence is distinctly more virulent in Latin America. For example, Central America and the Caribbean register homicide rates of 29 and 22 per 100,000, respectively—three to four times the global average.[16] Just as alarming, it appears that homicide rates are increasing across these two regions. There are, of course, strong differences in the distribution and scale of violence and insecurity across Latin American states and cities.[17] While a range of factors shape the high incidence of homicidal violence and victimization, there is some evidence that organized crime groups, drug trafficking organizations, and gangs (*maras* and *pandillas*) play a prominent role.

Globally, young males are four to five times more likely to be killed by violence than females.[18] This is also true in Latin America, where the overwhelming majority of those perpetrating and being victimized by violence in Latin America are fifteen to twenty-nine year-old males.[19] The risk of becoming a victim is especially high: homicide rates of young people are over 35 per 100,000 in the region, more than in any other part of the world.[20] Given the demographic trends in Latin America—a particularly youthful region—there are concerns that the challenges of youth violence will deepen before it improves. There are currently roughly 140 million young people in the region, and in some countries those under twenty-four years of age account for up to 60 percent of the population.[21] And while countries have to some extent already reached the peak of their youth bulge, the proportion of young people in the population will remain at a high level in the coming years.[22]

[15] An exception to the rule is Cuba where the national authorities undertake routine surveillance and filtering. See the OpenNet Initiative at http://opennet.net/ .

[16] See United Nations Office on Drugs and Crime (UNODC), "2011 Global Study on Homicide: Trends, Contexts, Data," Vienna: United Nations, 2011 and Kieth Krause, Robert Muggah, and Elisabeth Gilgen eds., *The Global Burden of Armed Violence* (Cambridge: Cambridge University Press, 2011).

[17] Homicide rates are concentrated in countries of Central America, with El Salvador and Honduras among the most violent. By contrast, countries in the southern cone (Argentina, Chile, Uruguay, and Paraguay) report the lowest youth homicide rates of the continent.

[18] According to United Nations Office of Drugs and Crime, "the risk of becoming a victim of homicide is highest for young men in the 15-29 age group and declines steeply with age thereafter." See UNODC, "2011 Global Study on Homicides," p. 64.

[19] See UNODC, "2011 Global Study on Homicide."

[20] Latin America also exhibits comparatively high rates of violence against women, particularly in urban areas. The difficulties of assembling and analyzing data related to gender-based, domestic- and intimate-partner violence are arguably more challenging than is the case for homicide and violent crime. Absolute levels of such violence are hidden owing to low reporting rates and weak sentinel surveillance systems. See Krause, Muggah, and Gilgen eds., *The Global Burden of Armed Violence*.

[21] Diniz and Muggah, "A Fine Balance."

[22] See Peter Imbusch, Michel Misse, and Fernando Carrión, "Violence Research in Latin America and the Caribbean: A Literature Review," *International Journal of Conflict and Violence* 5, No.1 (2011): 87-154; Catheryn Meurn, "The Role of Information and Communications Technologies in Violence Prevention," Background paper: Institute of Medicine of the National Academie, 2011, available at http://iom.edu/~/media/Files/Activity%20Files/Global/ViolenceForum/2011-DEC-8/BackgroundPaper-website.pdf .

No monolithic factor can explain why so many of Latin America's countries and cities present spiraling levels of violence. In Latin American societies, as elsewhere, collective and interpersonal violence remains an extremely complex phenomenon with roots that can be traced to the interaction of overlapping factors—some neurobiological, social, and cultural with others more economic and political.[23] Alongside structural factors are proximate "drivers" such as arms, alcohol, and drugs which are routinely singled out as vectors that tip social tensions into outright organized or interpersonal violence.[24] Societies in Latin America and the Caribbean are in fact militarized, particularly through private security companies, but less so than neighboring United States. And while these characteristics are complex and overlapping, understanding the multifaceted dynamics of criminal violence is essential for designing and implementing effective citizen security strategies that enhance state legitimacy, promote access to basic police and justice services, and ensure effective penal and prison systems.

A growing movement is oriented toward the promotion of new and innovative strategies to prevent and reduce organized and interpersonal violence in Latin America. Over the past decade, so-called *mano dura* approaches that promote repression, penalties, and incarceration have unintentionally radicalized gangs, expanded violence, and filled the region´s prisons to bursting point. Across the region prisons are known colloquially as "universities of crime," deepening networks of gang members rather than contributing to rehabilitation. Fortunately, some enlightened leaders in the region are calling for more investment in citizen security. With support from international agencies such as the Inter-American Development Bank and the United Nations, many states and cities are making progress in reversing violence and promoting social cohesion.[25] Indeed, governments, civil society groups and others are starting to engage with ICTs in order to expand safety and security.

Using ICTs for Violence Reduction

The use of digital tools and ICTs has the potential to re-organize the way researchers understand patterns of violence. Indeed, big data researchers associated with large firms such as Google and Microsoft, but also Harvard and smaller research think tanks, are exploring a combination of methods to understand inductively how violence shifts and transforms in Latin America. For example, Monroy-Hernadez et al have assessed social media trends and in particular Twitter hashtags to examine the drug war in Mexico.[26] In assessing literally millions of tweets and using specialized (and colloquial) word searches they have detected tensions between Twitter users, traditional media, government actors, and cartels.[27] They have also followed the rise of so-called civic media curators, a small number of central individuals who are responsible for a disproportionate number of violence-related real-time tweets. Likewise, Coscia and Rios have undertaken similar assessments using Google data to track Mexican drug trafficking organizations.[28] They have elaborated low-cost methods of gathering intelligence on the mobility and modus operandi of

[23] The circumstances behind, nature of, and society's attitude toward violence varies greatly from one setting to another. See World Health Organization (WHO), "Global Report on Violence and Health," Geneva: WHO, 2002. A number of studies in Latin America and the Caribbean reveal that while the sub-regions feature a history of armed conflict (especially in Central and South America), specific structural and proximate risk factors offer a more convincing explanation for the growth in interpersonal violence in recent years. These include growing up in a violent or broken home, a history of victimization, substance abuse, social isolation, rigidly proscribed gender roles, as well as personal characteristics such as poor behavioral control and low self-esteem.

[24] UNODC, "2011 Global Study on Homicides" has noted that in forty-six counties across the Americas and Caribbean, a 15-34 year old male is six times more likely to be killed with a firearm than a bladed weapon.

[25] See, for example, the IADB and WOLA map of citizen security activities at http://seguridadciudadana-centroamerica.org/ .

[26] Andrés Monroy-Hernández, Emre Kiciman, Danah Boyd, and Scott Counts, "Narcotweets: Social Media in Wartime," Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media, 2012, available at www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/viewFile/4710/5046 and André Monroy-Hernández et al., "The New War Correspondents: The Rise of Civic Media Curation in Urban Warfare," *CSCW* '13, February 23–27, San Antonio, Texas, 2013, available at http://research.microsoft.com/en-us/people/amh/cscw2013-civic-media-warfare.pdf .

[27] See, for example, Onook Oh, Manish Agrawal, and H. Raghav Rao, "Information Control and Terrorism: Tracking the Mumbai Terrorist Attack Through Twitter," Information Systems Frontiers 13, No. 1 (2011): 33-43 and Andres Monroy-Hernandez, "Shouting Fire in a Crowded Hashtag: Narco Censorship & 'Twitteroristas' in Mexico's Drug Wars," Readwrite Social, September 5, 2011, available at http://readwrite.com/2011/09/05/shouting_fire_in_a_crowded_hashtag_narcocensorship for a review of how these tensions are playing out in settings as diverse as India and Mexico.

[28] Michele Coscia and Viridiana Rios, "How and Where do Criminals Operate? Using Google to Track Mexican Drug Trafficking Organizations," Center for International Development Research Fellow & Graduate Student Working Paper No. 57, August 2012, available at www.gov.harvard.edu/files/videos/CosciaRios_GoogleForCriminals.pdf .

criminal groups using Google´s search engine and by generating visual plots and maps charting the market strategies of criminal enterprises over the past decade. Finally, Osario has also examined almost 10 million data points through a review of new and old media to disaggregate the micromechanisms of drug-related violence, testing models of agency and structure.[29]

Alongside big data research, there are a range of recent innovations in the use of ICTs to prevent and reduce various types of violence in Latin America. Some tactics are pursued by governments and citizens and address organized criminal violence associated with cartels and gangs. Others are mobilized by international agencies and local nongovernmental organizations and intended to address more discreet forms of interpersonal, domestic, and child-related violence. Still others involve advocacy organizations and are focused on state-led violence and repression, or other structural forms of violence associated with injustice and privations of freedom of expression. The approaches being adopted are diverse. They include the use of mobile and fixed Internet-based platforms intended to collect and transfer information within government agencies and between them ("vertical" ICTs) and more decentralized and spontaneous modalities developed and shared within civil society and the private sector ("horizontal" ICTs). There are also interconnected mechanisms designed to transfer information from governments to civil society, and vice versa. All of these are treated superficially below, drawing primarily on the cases of Brazil, Colombia, and Mexico (see figure 3).

It is also worth noting the distinction between data-generating and data-analyzing ICTs. On the one hand, there are systems that seek to promote information harvesting through anonymous dial-in systems, crowdsourcing modalities, gaming approaches, and other means. On the other are platforms that seek to interpret and parse out data, as well as report it through big-data analytics, blogs, and other social media. For example, the emergency services telephone number (911) and the comparative statistics system used by the New

Figure 3: Vertical and Horizontal Application of ICT in Latin America

Type	Approach	Functions	Examples
Vertical: government–government	ICTs developed by and for intra- and intergovernmental use	Real-time and social media surveillance and big data analytics for hot-spot mapping and internal accountability (data gathering)	Infocrim, Igesp, Terracrime (Brazil), Sala de Evaluación del Desempeño Policial (Mexico), CUIVD (Colombia)
Vertical: government–citizen	ICTs developed in cooperation with governments and citizens to enhance security delivery	Tailored data fusion systems to enhance mapping of incidents, bespoke applications for citizen reporting (data gathering/data analysis)	Attorney general of Coahulia (Mexico), IADB-UNICEF and Igarapé Institute assistance (Brazil)
Horizontal: citizen–government	ICTs developed by private or nongovernmental groups with applications for governments and citizens	Tailored (open) data systems using a combination of ICTs that allow for anonymous reporting on actual or suspected crimes (data gathering/data analysis)	Disque Denuncia, Unidos pela Segurance (Brazil), Citivox-Monterrey (Mexico), UN WOMEN–assisted interventions
Horizontal: citizen–citizen	ICTs developed by private, nongovernmental, and activist groups for citizen safety and security	Social media and network systems using existing models (Google, Facebook, and Twitter) or bounded systems (data analysis)	Blog del Narco, NAR, Notinfomex, Tehuan platform, narcowiki (Mexico), Hollaback! Say no to Violence, Bem Querer Mulher (Brazil)

Source: Authors

[29] Javier Osario, "Democratization and Drug Violence in Mexico," Paper prepared for a workshop of the Program on Order, Conflict, and Violence at Yale University, 2012, available at www3.nd.edu/~fosorioz/Papers/Osorio_Democratization_drug_violence_OCV.pdf .

York City Police Department (COMPSTAT) are both data-generating tools, while blogs covering violence are data analyzing ones. As more and more data exists online—referred to in some circles as "digital exhaust"—there are emerging questions about what types of ICTs will prevail. Put another way, will horizontal approaches be in a position to analyze data at scale, or will only centralized organizations using vertical approaches and sitting on large regularized datasets be in a position to meaningfully engage with it? While such questions are outside the scope of the present assessment, they are nevertheless emerging in the Latin American context.

Vertical Government-to-Government ICT Interventions

There is considerable evidence of vertical state-led applications of ICT for violence prevention and reduction. It is worth noting that law-enforcement and public-security experts across the region have long emphasized the importance of technology—and increasingly web-based innovations—in shaping effective preventive strategies, as well as the potential for transferring such innovations across hemispheres and between countries. Across Latin America, and in particular in Brazil, Colombia, and Mexico, there have been efforts to enhance the digital capacities of law-enforcement entities (both military and civil police) and courts, improve the use and connectivity of surveillance cameras, increase the quality of mobile communication systems, install GPS and related tools in patrolling vehicles, and, more recently, harvest and analyze large quantities of raw data. The most common platforms emerging across Latin America are COMPSTAT-style systems combining traditional surveillance measures with georeferenced data collection from conventional administrative data sources as well as citizen and police reporting.[30]

In Brazil, São Paulo's secretary for public security undertook a pioneering effort beginning in 1999 to modernize the state´s information gathering capacity. To help its policing of a city of some 20 million, the office launched Infocrim. The system registers data from police reports into a central database and is automatically updated every other hour. The system features information on the types of crime committed, its location and the time it took place, the nature of the incident, and other variables. The system is now online and generates real-time maps. It is credited with massively reducing annual homicide rates from 12,800 in 1999 to some 7,200 by 2005.[31] Similar initiatives have been launched in neighboring Minas Gerais state, including the Public Security Integration and Management System (Igesp), which is based on New York´s COMPSTAT system. Indeed, Igesp is credited with reducing homicides by more than 20 percent in the state's capital, Belo Horizonte. Another initiative supported by the Brazilian federal government is Terracrime, a geoprocessing tool fielded by the National Secretariat of Public Security (SENASP), which operates in six cities in Brazil.[32]

Meanwhile, Mexico, Colombia, and some countries in Central America are also developing similar types of digital platforms to enhance surveillance capacities but also promote accountability within police forces. For example, the Federal Secretary of Public Security of Mexico City also drew on New York City´s COMPSTAT process in 2008 to upgrade its capacities. The Police Performance Evaluation Room (Sala de Evaluación del Desempeño Policial) introduced a digitized system to evaluate the capital´s tens of thousands of police.[33] In Colombia, Bogota´s police force also adopted a unified information system on violence and crime (CUIVD) in 1995, also drawing on COMPSTAT's principles.[34] Building on this program, Colombia´s 150,000-strong national police force also upgraded their cell phone system in 2007 with support from Microsoft. As a result,

[30] COMPSTAT (short for computer statistics or comparative statistics) is a system of management for police departments equivalent to Six Sigma or TQM, though it was not actually a computer system in its original formulation. It now refers to a multi-tier crime reduction and quality of life improvement process which combines GIS (geographic information systems) to map the incidence of crime. On the basis of these maps, weekly meetings are undertaken with local level officers to review challenges, discuss tactics and improve the standard of living in selected areas. The system was pioneered in New York City, but is now in action in Austin, Baltimore, San Juan, Los Angeles and elsewhere. Interview with Ray Kelly, October 2012.

[31] See Marina Lemie, "São Paulo: mapas do crime contribuíram para a redução dos homicídios," *Comunidade Segura*, October 4, 2006, available at www.comunidade-segura.org/pt-br/node/75 .

[32] See Marina Lemie, "Terracrime: geoprocessamento na batalha contra o crime," *Comunidade Segura*, October 5, 2006, available at www.comunidadesegura.org/pt-br/node/83 .

[33] See Compstat: Sala de Evaluación del Desempeño Policial, available at www.ssp.df.gob.mx/TecInformacion/Pages/Compstat.aspx , accessed November 2012.

[34] See Eduardo Moncada, "Toward Democratic Policing in Colombia? Institutional Accountability through Lateral Reform," Comparative Politics 41, No. 4 (July 2009): 431–449, available at http://emoncada.files.wordpress.com/2009/12/cp-moncada-july09.pdf .

the police are now better able to ensure integrated audio and video conferencing and more communication in real time, making them better equipped to fight crime.[35] Finally, in Central America, as part of the Central American Regional Security Initiative, a new regional police systems reform program is seeking to improve policing capabilities. The approach explicitly advocates COMPSTAT techniques and community policing.[36]

It is also worth noting that Colombia in particular has witnessed the vertical development of ICT tools in the context of the long-standing conflict against the guerrilla groups, including the Revolutionary Armed Forces of Colombia (FARC). What is particularly intriguing is the way that early initiatives pursued by the Colombian army and its auxiliaries in cyberspace spurred on FARC applications and, later, activities by the political elite. Specifically, the Colombian armed forces and paramilitary groups often posted polemical blogs to communicate with the public and throw a veil of ideology over their actions. FARC guerrillas also used the Internet to run an "international front," routinely posting statements and producing videos for their website. Civil society groups then began organizing mass rallies online. Much later to catch-on were Colombian politicians, not least the ex-president Uribe, who are now avid users of Twitter and conduct bitter debates on government policy online.[37]

At the regional level, there are nascent indications of governments seeking to share and even harmonize data on criminal violence. For example, within the Americas there is the Regional System of Standardized Indicators of Peaceful Coexistence and Citizen Security (RIC) supported by the Inter-American Development Bank (IADB).[38] This effort is intended to enhance more than a dozen key indicators of violence and ensure sharing across countries. Likewise, the South American Common Market (Mercosur) has elaborated a system for security exchange (SISME) to share data digitally with members, including Bolivia, Chile, Colombia, Ecuador, Peru, and Venezuela.[39] It should be stressed that intergovernmental sharing of information on issues of organized violence continues to be uneven, in large part owing to concerns of sovereignty but also due to low levels of regional integration. Rather, information on specific dynamics of violence tends to be shared on a bilateral basis, between defense, intelligence, and police branches. Indeed, the old adage "garbage in, garbage out" should be recalled, since poor and incorrect reporting can generate biases and false positives that in result in structural irregularities and frustrate comparisons between cases.[40]

Vertical Government-to-Citizen ICT Interventions

Notwithstanding a rapid growth in "citizen security" across Latin America, there are relatively few examples of ICT use connecting state entities and civilians to prevent and reduce violence. Indeed, a long legacy of repressive policing and state violence has limited the opportunities for such exchange, though there is some evidence that this may now be changing. For example, in cases where extreme forms of organized violence are occurring, as in northern Mexico, special efforts are being made to improve interactions with communities to gather information, including anonymously. Examples of this are the efforts by the Mexican state of Coahuila to reach out to its citizens through the official Twitter accounts of its public security institutions: Procuraduría General de Justicia del

[35] More recently, Colombian National Police established a network of Voice over Internet Protocol (VOIP), to replace their antiquated Internet Protocol telephony system. This not only saved on cost, but allows for more effective internal communication, and therefore, in theory, more effective crime-fighting. See Microsoft, "National Police Force Improves Efficiency, Cuts Costs with Unified Communications," Microsoft Office System Costumer Solution Case Study—Colombia, December 2009, available at www.microsoft.com/casestudies/ServeFileResource.aspx?4000012870 .

[36] See William R. Brownfield, "Working Toward a More Secure Central America," *DipNote: US Department of State Official Blog*, March 13, 2012, available at http://blogs.state.gov/index.php/site/entry/inl_central_america .

[37] A full account of the Colombian experience is being produced by the Igarapé Institute and SecDev Group as part of the Open Empowerment Project, to be published later in 2013.

[38] See Regional System of Standardized Indicators in Peaceful Coexistence and Citizen Security (RIC) Project, available at www.seguridadyregion.com/en/about-the-project.html .

[39] See *Sistema de Intercambio de Informacion de Seguridad de Mercosur (SISME)*, available at www.mercoszur.int/msweb/CCCP/Comun/revista/N%204/09%20SISME.pdf .

[40] For example, the authors visited a special hotline service—190—in Rio de Janeiro in December 2012. The service received some 650,000 calls a month. One of the primary calls received is related to "bank robbery" suggesting a very serious epidemic of crime. It turns out, however, that most reports were triggered by bank system misfires registering frequent false positives. Yet these same false positives are recorded in the 190 logs dataset.

Estado (@PGJECoahuila) and Secretaría de Seguridad Pública (@SSPCoahuila).[41] Likewise, in Brazil, as processes of pacification move forward in Rio de Janeiro, the military police are exploring new ways of reaching out to affected communities before, during, and after territories are re-secured and permanent community police posts installed.[42]

There are also increasing examples of federal and, more commonly, municipal authorities working with major private firms and international agencies to enhance their ability to harvest and disseminate information on public security to citizens. Indeed, Google, IBM, and Microsoft have all started developing and selling products to enhance public safety in Latin America. Rio de Janeiro is one of two cities seeking to connect all disaster response capabilities to enhance police action in hot spots using the "Smart City" initiative. Also, organizations such as Igarapé Institute are working with private partners to develop applications with Rio de Janeiro's military police to enhance accountability and interactivity with citizens in pacified communities.[43] Likewise, organizations such as the Inter-American Development Bank and UNICEF are developing new ICT projects, albeit cautiously, to begin tracking violence and measuring the performance of interventions. A prominent example is UNICEF's development of participatory mapping tools in Brazil, which focused initially on environmental hazards and are now being extended to promoting safer communities.[44] Finally, other groups are also beginning to monitor various types of crime in Latin America, though still experimenting with "big data."[45]

Horizontal Citizen-to-Government ICT Interventions

There are also a number of ICT initiatives being developed from the "bottom up" and in some cases working with government entities. In most cases, the originators of the data-management and -collection platforms are nongovernmental organizations or small start-up companies. In some instances, they collaborate with local metropolitan authorities and law-enforcement agencies, either on the basis of a contract or in the spirit of partnership. What differentiates these activities from vertical interventions is their primary reliance on citizen participation and their multi-dimensional forms of information capture and dissemination. Such ICT activities tend to combine spatial and temporal analysis of violence trends while also seeking to use this data to improve the accountability and responsiveness of state institutions.

In Brazil, there are several prominent and well-regarded examples of horizontal citizen-government ICT activities. The most widely known is Disque Denúncia (Call to Denounce), which was created in 1995 in Rio de Janeiro during a particularly violent episode. Indeed, a surge in homicidal violence, kidnapping and ransom, and other forms of violence precipitated a response from private entrepreneurs, nongovernmental organizations and the local government. Inspired by the United States Crime Stoppers model, the system was designed to help community residents inform the police anonymously about actual or suspected crimes. A nongovernmental agency served as the intermediary and filtered, managed, and mediated interactions between the community and the police. The intervention has now been scaled up across Brazil to all twenty-seven states and exported as a model to other countries across Latin America. A more modern and pilot-based approach is the Unidos pela Segurança (United for Security) initiative developed by a private company called STAL IT. While still searching for a public partner, the initiative uses crowdsourcing methods from a bounded network of some 1,000 participants (with some curators more active than others) to track violent

[41] These accounts have substituted an unofficial account of the Fiscalía del Estado (@FiscaliaCoah), which had more than 75,000 followers. However, these two new accounts together have no more than 3,000 followers each. See " Nuevas cuentas de Twitter y Facebook para seguridad del Estado," *El Diario de Coanuila*, April 26, 2012, available at www.eldiariodecoahuila.com.mx/notas/2012/4/26/nuevas-cuentas-twitter-facebook-para-seguridad-estado-290307.asp .

[42] See Robert Muggah and Albert Souza Mulli, "Rio Tries Counterinsurgency," *Current History* 111, No. 742 (February 2012).

[43] Another example of this kind of tool, while not based on designing an app for a mobile phone, but still focused on real time visual and audio feeds, is an initiative launched in Brasilia in 2012. This tool draws from technology piloted during the US Salt Lake City Olympics and is now in service in 200 US cities. See "Câmeras acopladas aos policiais gravam ações nas ruas," *Fantastico*, February 12, 2012, available at http://g1.globo.com/fantastico/noticia/2012/12/cameras-acopladas-aos-policiais-gravam-acoes-nas-ruas.html .

[44] See "Transferem tecnologia de mapeamento de riscos ambientais para comunidades cariocas," UN Children's Fund (UNICEF), MIT, and Public Laboratory for Open Technology and Science, available at www.unicef.org/brazil/pt/por_dentro_MIT.pdf and "Oficina internacional capacita adolescentes e jovens para mapeamento comunitário," UNICEF, available at www.unicef.org/brazil/pt/media_21477.htm .

[45] See the work of Global Pulse at www.unglobalpulse.org/projects/rivaf-research-assessment-potential-impact-economic-crisis-decisions-undertake-unsafe-inter and www.unglobalpulse.org/projects/rivaf-research-monitoring-impact-global-financial-crisis-crime .

incidents in selected states of Brazil. It has a linked web-based platform that is filtered by the ICT manager and seeks to provide verified information to Disque Denúncia and the military police.[46]

In Mexico groups such as Citivox have developed ICT tools to support hot-spot mapping.[47] On the basis of a simple open-access system, Citivox has worked with private companies, nongovernmental groups, and the city authorities of Monterrey to track electoral violence. The tool is based on real-time reporting using crowdsourcing methods. First, citizens are expected to report and share information on what they identify as the principle problems affecting their communities. Second, decision makers are then in a position to use the platform to better understand and respond to citizen complaints. This is achieved by first converting reports into manageable and visual feeds showing trends in visual (geothermal), temporal (line charts), and other forms. Citivox has replicated these tools in other Latin American settings, but also in Eastern Europe.[48]

Horizontal Citizen-to-Citizen ICT Interventions

The most dynamic area of innovation for ICTs to promote violence prevention and reduction is occurring within civil society. Designed neither for public authorities nor police actors, such tools are emerging spontaneously from the private sector, academic and research institutions, and nongovernmental organizations themselves. It should be noted, however, that while some of these ICTs may appear to be entirely locally based, they may also have outsiders supporting and funding them. The largest generators of such tools are in Mexico, largely as a result of the self-imposed censorship of mainstream conventional media outlets and public authorities. ICT growth is thus driven by residents' intense desire to protect themselves and to promote awareness of public security issues. A number of exceedingly high-profile and brutal instances of violence committed against Internet activists and hacktivists has in turn unleashed a wave of measures from within civil society intended to reduce the strength of cartels (and their sympathizers), but also defend the public against them and other forms of violence.

Citizen reporting systems and blogs are two common horizontal citizen-to-citizen ICT tools for violence prevention, the most prominent examples of which are "narco-blogs" and "narco-tweets" in Mexico.[49] Indeed, the wildly popular *El Blog del Narco*, or the narco-blog, posts graphic images, stories, and posts on the drug war not published elsewhere and was sustained anonymously for five years before being shifted to another less popular venue.[50] Related sites include *Notinfomex/Narco-violencia* and *Nuestra Aparente Rendición* (NAR), which advocate more pro-peace messages and sustain communication networks among activists.[51] Other more proactive sites seeking to "out" suspected cartel members and known criminals include the Tehuan platform run by the Center for Citizen Integration.[52] The platform seeks to incentivize citizen engagement while also using crowdsourcing methods. Another fascinating approach to tracking violence in the absence of "administrative" data sources is http://es.elnarco-trafico.wikia.com/wiki/Wiki_Narco, which uses a mixed method of crowdsourcing, a wiki platform, and Google maps to visualize trends across Mexico. The tool allows for a better understanding of incidents of violence, but also fluctuations in the demarcation lines separating specific cartels.[53]

Across Latin America, various e-networks and specialized applications are emerging more or less spontaneously that report and share information on various types of violence. For example, in Brazil there are blogs that actively reflect on violence-prevention measures in recently pacified slums, or *favelas*, of Rio de Janeiro. Community residents, many of whom are now purchasing tablet

[46] See UNIDOS Pela Segurança, available at http://upseg.org/mapa.upseg .

[47] See Citivox, available at www.citivox.com .

[48] Personal interview with Jorge Soto, director of Citivox, January 2013.

[49] See Monroy-Hernandez, "Shouting Fire in a Crowded Hashtag."

[50] See "Colocan narcomantas para el Gobernador de Tamaulipas," Blog del Narco, March 21, 2013, available at www.blogdelnarco.com/ .

[51] See Notinfomex, available at www.notinfomex.info/ and *Nuestra Aparente Rendición*, available at nuestraaparenterendicion.com/ .

[52] See "Presentan plataforma para denuncia ciudadana," *Milenio*, October 18, 2011, available at http://monterrey.milenio.com/cdb/doc/noticias2011/b32314e81b62a0b97b6f539b86534a2d .

[53] See Xeni Jardin, "Wikinarco: Mapping Narcoviolence," *Boingboing*, September 2012, available at http://boingboing.net/2011/09/12/wikinarco-mapping-narcoviolence.html .

computers and smartphones and actively using Facebook, are tracking trends.[54] Other ICT tools designed to prevent sexual violence and developed outside of Latin America, including Hollaback!, are establishing chapters in the region. Two other prominent examples are Say No to Violence, a social-mobilization platform established in 2009 and connected to UNiTE and Bem Querer Mulher (Cherish Women), supported by UN Women.[55] To be sure, new ICTs are routinely emerging that explore ways of enhancing the protection of women and girls from violence in Brazil, Colombia, and Mexico, but also elsewhere.[56]

It must be stressed that the use of ICTs is not the preserve of activists and proponents of violence prevention. At one extreme are citizens who are using ICTs to circumvent initiatives intended to reduce violence. For example, in Brazil and Mexico, citizens are using Twitter to avoid anti-drunk driving campaigns (e.g., Lei Seca in Brazil), much to the consternation of public authorities.[57] Citizens are also known to have abused ICTs, falsely reporting information and generating panic.[58] There is also a surge in ICT use by civilians for meting out vigilante justice against alleged criminals, often resulting in ugly retributive violence.[59] More ominously, and at the other extreme, is the parallel growth in ICT use (and monitoring of ICTs) by criminal groups, organized gangs (*pandillas* and *maras*), and drug cartels. For example, there are a number of cases of drug cartels infiltrating activist networks, identifying personal information, and ultimately killing the activists.[60] This has in some cases led to the emergence of new forms of online engagements, including the expansion of activities against the Zetas by the online activist collective Anonymous (and vice versa).[61] What is more, citizens also frequently fear retaliation from the police, who themselves may be compromised by citizen reporting. For example, interviews conducted by the authors in poorer areas of Brazil, Colombia, and Mexico confirm that citizens are fearful of using ICTs to report denunciations for fear of being tracked down and punished.[62]

Recommendations and Lessons Learned

While there is a terrific growth in ICTs for violence prevention across Latin America, it is still too early to assess their broad impacts in the aggregate. Indeed, there is anecdotal evidence of some vertical ICT interventions generating important reductions in homicidal violence and improved intelligence and rationalization of police forces.[63] There is considerably less information on the outcomes of horizontal measures. The "field" is itself rapidly evolving and highly decentralized, not easily amenable to controlled scientific measurement on the ground. This makes the determination of definitive lessons learned difficult at this stage. Nevertheless, there is an apparent rapid growth in ICT use for violence prevention which is, in turn,

[54] See "What if Technology Undermines Drug Violence?" *Rio Real*, September 2, 2012, available at http://riorealblog.com/2012/09/02/what-if-technology-undermines-drug-violence-2/ .

[55] See Say No – Unite, available at http://saynotoviolence.org/about-say-no and Bem Querer Mulher, available at http://bemquerermulher.webnode.com/ .

[56] See María Isabel Bavidziuk and María Alejandra Davidziuk, "Mexico, Argentina, Brazil and Colombia: Cross-country Study on Violence Against Women and Information Communication Technologies," 2009, available at www.genderit.org/sites/default/upload/APC_WNSP_MDG3_VAW_ICT_en_lac_dec2009_1.pdf and Flavia Fascendini and Kateřina Fialová, "Voices from Digital Spaces: Technology Related Violence Against Women," Association for Progressive Communications, 2011, available at www.genderit.org/sites/default/upload/apcwnsp_mdg3advocacypaper_full_2011_en_0.pdf .

[57] See "AGU quer impedir divulgação de blitz da lei seca em microblogs em Goiás," *Jornal da Globo*, June 2, 2012, available at http://g1.globo.com/jornal-da-globo/noticia/2012/02/agu-quer-impedir-divulgacao-de-blitz-da-lei-seca-em-microblogs-em-goias.html and Alberto Nájar, "Twitteros en la mira de la policía," BBC Mundo, January 19, 2010, available at www.bbc.co.uk/mundo/participe/2010/01/100118_0026_twitter_alcoholemia_gm.shtml .

[58] In Mexico, the false reporting of a kidnapping and shooting led to panic and chaos in a particular neighborhood. The person who created the false tweet and others who retweeted were arrested on the charge of terrorism. Twitter users who use hashtags to report violence ironically started calling themselves "twitterrorists." See Monroy-Hernandez, "Shouting Fire in a Crowded Hashtag."

[59] For an example, see *Justicia Final*, available at http://justiciafinal.blogspot.com.br/ . See also Steven Dudley, "Vigilante Blogs Leave Bloody Trail in Guatemala," *In Sight Crime*, Wednesday 7, 2011, available at www.insightcrime.org/news-analysis/vigilante-blogs-leave-bloody-trail-in-guatemala .

[60] See "Delincuencia organizada infiltrada en redes socials," *Blog del Narco*, April 9, 2011, available at www.blogdelnarco.com/2011/04/delincuencia-organizada-infiltrada-en-redes-sociales/ .

[61] See Scott Stewart, "Anonymous vs. Zetas Amid Mexico's Cartel Violence," *Stratfor*, November 2, 2011, available at www.stratfor.com/weekly/20111102-anonymous-vs-zetas-amid-mexico-cartel-violence .

[62] Interviews were conducted by the Igarapé Institute with residents in favelas such as Maré, Rocinho, and Complex do Alemão between November and December 2012 and January and March 2013. Likewise, communications with colleagues working with InsightCrime in Colombia and CIDE in Mexico in January and February 2013 also suggested the pervasive fear among residents in poorer areas to report crime, either formally to police or online.

[63] See Meurn, "The Role of Information and Communications Technologies in Violence Prevention."

suggestive of a wider appetite. An increasing number of public entities—police and metropolitan authorities are the tip of the iceberg—are actively enhancing their capabilities. While in some cases proceeding cautiously owing to structural concerns with transparency, it is now accepted wisdom that (especially mobile) ICTs—including the use of crowdsourcing, geospatial and geothermal mapping, and other data fusion techniques—are essential to map hot spots, prioritize resources, plan interventions, and assess outcomes. Likewise, citizen groups are experimenting with frontline data harvesting techniques and paving the way for a new generation of big-data research.

Notwithstanding the enthusiasm for technology-driven approaches to security promotion, Latin America is still a long way off from a genuinely democratic public-security project. Indeed, many government institutions have yet to fully embrace new technologies on "sensitive" issues of organized and interpersonal violence, sometimes with good reason. New technologies can often dilute and diffuse information, an anathema to the older establishment that favors centralized forms of data management (such as some of the hotline systems documented above). As for citizens, many have engaged actively in innovative approaches to promoting safety, albeit sometimes at considerable risk and personal cost.

Yet, a similar number have yet to engage in the digital revolution, either because they are systemically excluded or because of fears of retribution. This speaks as much to the failures of the social contract as to the spectacularly brutal forms of violence meted out by cartels, such as the Zetas, on those who seek to denounce them. Nevertheless, there appear to be more and more examples of social media bringing previously "untold" stories to light, including those that demonstrate how underserviced and vulnerable populations are affected by violence. New media transmits information faster than conventional media, often visually and in real time, and it is transforming the ways in which information is produced, consumed, and disseminated.

This final section sets out a number of tentative entry points and recommendations for stakeholders involved with violence prevention in Latin America. The focus is on international organizations, national and municipal governments, and civil society entities. It is, of course, challenging to issue standardized guidance given the extraordinary heterogeneity of Latin American states and societies. Indeed, a critical finding of this paper is the highly uneven penetration of Internet and mobile technology not just between regions, but also within them. Indeed, the variegated access to ICTs also extends to states, cities, and neighborhoods. This variation must be accounted for in the design of any strategies to mobilize ICTs for violence prevention and reduction.

INTERNATIONAL ACTORS

- **Acknowledge that there is already massive engagement with ICTs in Latin America and that this is likely to expand in the foreseeable future.** The basic demographic calculus of the region suggests that ICT use will grow even as it "matures" across the population. Moreover, there is evidence that social media, new forms of data-fusion technology, and digital activism are creating a new arena for monitoring and responding to violence in the region.
- **Seek to encourage the mainstreaming of ICTs in regional and national public-security plans, but also recognize that ICTs alone will not resolve the challenges of organized and interpersonal violence.** There are many factors shaping violence intensity and organization, and ICTs are one important factor that can shape this violence positively and negatively. That said, national and metropolitan authorities, including public security personnel, are increasingly composed of digital natives and are open to innovation in many settings. There is a need to support exposure and training in ICTs for violence reduction as well as to caution against their limitations.
- **Encourage South-South sharing within Latin America and beyond.** The fact is that Latin America´s experimentation in ICTs for violence prevention is comparatively advanced. While there was evidence of vertical and horizontal engagement with ICTs as early as the 1990s, it should be noted that these systems were not established in a vacuum. Indeed, many of the contemporary applications using new technologies were built on, and intended to enhance, existing or older systems. In other words, "new" digital technologies may increase the pace and

scale of communication, but they are not necessarily new in form or content. Identifying and analyzing these earlier systems may provide some possible innovations for other countries in the region and internationally.

NATIONAL ACTORS

- **Capitalize on the growing acceptance and interest in ICTs for violence prevention among the young generation of Latin Americans.** Police forces, municipal planners, and citizens are all more digitally aware than in generations past. They are more inclined to experiment with and adopt new technologies. There are remarkable examples of police and citizens developing tailor-made solutions using crowdsourcing, geovisualization, gaming methods, and other media-monitoring tools, all of which reflect a curiosity and willingness to explore new approaches to tackle old problems.[64] That said, there is a need to make investments in improving digital literacy. Indeed, there continues to be a significant digital divide that mirrors broader social and economic inequalities. Support for ICTs must be accompanied with investments in education and in strengthening technical capacities from below.
- **Develop and build on North-South and South-South transfers of ICTs for violence prevention.** While there are examples of ICT technologies that are directly transferable from upper-income to lower-income settings, there is also ample room for adaptation, experimentation, and replication among southern contexts. Indeed, particularly with respect to horizontal ICT transfers, there is already a strong tradition of learning about and sharing technologies for violence prevention. There are some examples where public-private partnerships have incentivized replication, and these offer some interesting cases for further study.[65]

CIVIL SOCIETY

- **Acknowledge that while some ICTs for violence prevention emerged in a top-down manner, many also emerged spontaneously owing to failures in conventional media.** In countries such as Colombia and Mexico, but also throughout Central America, the mainstream press and public authorities have self-censored reporting on violence either due to direct intimidation from organized armed groups or owing to a general secrecy around reporting. This has in turn triggered new forms of citizen reporting within social media and the blogosphere, and the development of more proactive reporting systems. This may have longer-term implications for the public legitimacy of traditional media outlets and also for the wider debate on freedom and justice in these countries. There are important opportunities to engage with citizen reporters and promote quality and ethical standards in reporting.
- **Tools that guarantee anonymity are critical for shaping citizen use of ICTs for violence prevention in Latin America.** Throughout the region, violence rates are high, but actual reporting on conventional crime is comparatively low. This reflects a long-standing mistrust of law-enforcement entities and court systems that were seen to favor an unequal status quo and that have ingrained impunity. As a result, citizens seldom personally report crimes and in some cases actively avoid reporting for fear of retribution. The introduction of anonymity into ICTs, including in relation to direct dial-in, SMS, email, and other systems, has transformed reporting rates. What is more, the use of avatars, such as a Twitter handle, still enables reporters to receive "credit" for their participation.
- **Identify and reward valuable human resources among the population.** There is a noticeable shift in the approach citizens are taking to reporting on violence. Due in part to the factors identified above, some advocates of ICT —especially civic media curators in horizontal networks—are adopting ever more proactive approaches to preventing violence. Far from being mere passive citizen tweeters, they are in some cases actively denouncing violence. Likewise, some hacktivist groups are countering cyber-extortion methods adopted by crime groups (using denial of service

[64] See Maja Bott and Gregor Young, "The Role of Crowdsourcing for Better Governance in International Development," *Praxis: The Fletcher Journal of Human Security* 27, (2012): 47–70, available at http://fletcher.tufts.edu/Praxis/~/media/Fletcher/Microsites/praxis/xxvii/4BottYoungCrowdsourcing.pdf for a review of crowd sourcing methods .

[65] For example, the New York City Police Department created COMPSTAT with Microsoft. The NYPD now makes a minimum of a 20 percent royalty on all new sales of COMPSTAT. Personal interview with Ray Kelly, NYPD police commissioner, December 2012.

attacks against those who will not pay up) with the very same methods, even outing collaborators, often with lethal consequences. Identifying and rewarding skilled individuals to promote a culture of legality might be a promising strategy so long as the threat of retaliation from criminal actors is prevented.

This paper offers an initial overview of how social and political actors are appropriating ICTs in Latin America in order to understand, cope with, and fight back against organized and interpersonal violence. The fact that Latin America is simultaneously the developing world's most connected region but also its most violent ensures that it presents a vivid, real-life laboratory for the new field of ICTs for violence prevention. Indeed, the paper shows that there is considerable room for more investment and engagement in Latin America, even as the experiences of social-media revolutions in the Middle East take center stage. What is clear is that cyberspace provides avenues for the development of smart solutions for both structural challenges and proximate threats. A key challenge will be to find ways to incentivize institutions and individuals to embrace a meaningful and accountable digital revolution, one that promotes safety and security on- and off-line.

Early Warning and the Role of New Technologies in Kenya

Godfrey M. Musila[1]

Introduction

How can we prevent disputes from arising between parties or prevent existing disputes from escalating into full-blown conflicts? How can we limit the spread of conflict when it occurs? Conflict-prevention activities can incorporate a variety of elements, according to the UN Secretary-General, including early economic, social, and development engagement in the relevant country.[2] Today, the UN and regional multilateral organizations are demonstrating that preventive action can accommodate a range of interventions that go beyond traditional preventive diplomacy.[3] These include preventive deployments of troops (mainly to contain emerging crises), preventive disarmament, fact-finding missions, early warning, inspections, monitoring, and peacekeeping.[4]

Although the separation of early warning from conflict prevention has been urged by some, it is clear that early warning is an important form of preventive action. Elements or measures that constitute early warning include collection, analysis, and dissemination of information on various aspects of a conflict, including root causes, triggers, and factors that perpetuate conflict. However, early warning is more than the mapping of conflict and violence. Early warning only makes sense if the information collected, analyzed, and disseminated is linked effectively to early action to prevent breakout or escalation of conflict.

In Kenya, an early-warning mechanism managed by the National Steering Committee on Peace Building and Conflict Management (NSC) was created in the Office of the President. The NSC, a joint initiative between the government and civil society organizations, was established in 2001 to coordinate all peace-related activities in Kenya. Within the Office of the President, it is domiciled in the Ministry of State for Provincial Administration and Internal Security. (The NSC has received financial and technical support from UNDP since 2005.)

The NSC became operational in November 2002 with the establishment of a secretariat. The NSC brings together representatives from relevant government ministries and departments, umbrella civil society organizations, development partners, and UN agencies. The establishment of the NSC was aimed at harmonizing, strengthening, and integrating various conflict-management initiatives undertaken by state and nonstate actors (mostly civil society organizations). The NSC serves as Kenya's Conflict Early Warning and Response Unit (CEWERU) for the implementation of the regional Conflict Early Warning and Response Mechanism known as CEWARN. CEWARN is a collaborative effort of the member states of the Intergovernmental Authority on Development (IGAD): Djibouti, Eritrea, Ethiopia, Kenya, Somalia, Sudan, and Uganda.

This paper considers the structural uses, impact, and limitations of technologies in conflict prevention and early warning in the Kenyan context, with specific focus on the NSC's early-warning system. These technologies include social media (Facebook, Twitter), cell phones, wireless radio, and GIS mapping. To place this analysis in perspective, the paper outlines and analyses the Uwiano Platform, an ad hoc early-warning mechanism jointly initiated by the government and civil society actors with support from UNDP in the lead up to

[1] Godfrey M. Musila is Director of the Nairobi-based African Center for International Legal and Policy Research (CILPRA).

[2] UN Secretary General Report, "Agenda for Peace: Preventive Diplomacy, Peacemaking and Peace-keeping," UN Doc. A/47/277, June 17, 1992; David J Francis et al., "Dangers of Co-deployment: UN Co-operative Peacekeeping in Africa" (Aldershot: Ashgate, 2004), p. 23.

[3] Ibid.

[4] For example, the UN peacekeeping mission in Macedonia (UNPREDEP) from 1995–1999 was regarded as a preventive deployment of troops to contain an emerging crisis there. The African Union (AU) has created the AU Continental Early Warning System (CEWS), as provided for by Article 12 of the *Protocol Relating to the Establishment of the Peace and Security Council* (PSC). The Organisation of African Unity and its successor, the AU, have also sent observer and monitoring missions to a number of countries, including Comoros, Congo, and Rwanda.

the 2010 referendum on the constitution. Further, the paper reviews IGAD's ICT4Peace project that was initiated by the intergovernmental body to test the use of technologies to prevent conflict among pastoralist communities in the Karamoja Sector. The analysis of IGAD's ICT4Peace is aimed at drawing lessons for national and regional early-warning systems on the potential for the use of technologies in early warning and conflict prevention.

History and Anatomy of Conflict in Kenya

Kenya is situated in a region on the African continent that has been challenged by conflict of varying intensities for decades. These conflicts in the greater East Africa region include those in the Horn of Africa and the Great Lakes region. They are often violent and transboundary in character. Over the last two decades, conflict has broken out in Burundi, the Democratic Republic of the Congo (DRC), Ethiopia, Rwanda, Somalia, Sudan, and Uganda. Although Kenya itself has enjoyed relative peace over the years and had been described as "an island of peace" in a troubled region, the fragility of this peace became clear when violence broke out in 2007 and 2008 after a disputed presidential election.[5]

In reality, many structural drivers of conflict have remained unresolved since Kenya's independence in 1963. These included the centralized structure of the state, exclusionary (in economic, social, and political terms) and oppressive rule, persistent instrumentalization of ethnicity for political ends, inequitable distribution and access to vital resources, corruption, limited democratic space, limited rule of law in the peripheries, and lack of respect for fundamental rights. In fact, politically orchestrated violence and the suffering, death, and displacement that came with it had been associated with electoral cycles since the return of multiparty politics in 1992. The post-election violence in 2007 and 2008 differed only in geographic scope and the extent of the impact on lives, communities, and the economy.[6]

Since independence, conflicts in Kenya have ranged from benign disagreements over policy and other matters to violent conflict resulting in significant loss of life and property, displacement, and disruption of law and order. Some of these conflicts have been localized, while others have been national in scope and character. Other conflicts have been transboundary, emanating from or linked to instability in neighboring states. The types of conflicts experienced in Kenya include:

- cross-border conflicts, involving theft of livestock and other property and loss of lives, particularly along the borders with Uganda, Sudan, Ethiopia, and Somalia;
- intercommunal conflicts in pastoralist areas and marginalized regions of northern Kenya, and in parts of Eastern and Coast Provinces;
- resource-based conflicts and environmental conflicts linked to resource exploitation, use, and conservation;
- land-related conflicts in many parts of the country;
- agro-pastoralist conflicts;
- religious or faith-based conflicts.[7]

Conflict Prevention and Early Warning: The Kenyan Case

Since the return to multiparty democracy in 1992, various governmental actors (including provincial administrations), intergovernmental actors, and nongovernmental organizations have engaged in diverse ways and settings to develop effective conflict-prevention strategies in Kenya. Initially ad hoc and dispersed, responses have become increasingly sophisticated and coordinated.

[5] On the post-election violence generally, see South Consulting Reports; Elisabeth Lindenmayer and Josie Lianna Kaye, "A Choice for Peace? The Story of Fourty-One Days of Mediation in Kenya," New York: International Peace Institute Report, August 2009.

[6] On cyclical political violence and displacement, see: Kenya National Commission on Human Rights, "Report of the Judicial Commission Appointed to Inquire into Tribal Clashes in Kenya" (Akiwumi Report), 1998; Kenya National Commission on Human Rights, "Report of the Commission of Inquiry into Post-Election Violence" (Waki Report), 2009; Prisca Mbura Kamungi, "The Current Situation of Internally Displaced Persons in Kenya," Jesuit Refugee Service, March 2001; Human Rights Watch (HRW), "Divide and Rule: State-Sponsored Ethnic Violence in Kenya," New York: HRW, November 1993.

[7] See "National Policy on Peacebuilding and Conflict Management," Kenya Office of the President and Ministry of State for Provincial Administration and Internal Security, December, 2011.

Perhaps the earliest coordinated approach to conflict prevention and resolution was the creation of District Peace and Development Committees. The origins of these committees can be traced back to peace committees in the greater Wajir district in North Eastern Province in the early 1990s, when local communities in the pastoralist area started using traditional conflict-management mechanisms to resolve interclan and intercommunity conflicts. Later, these peace committees spread to other parts of the northern region and Coast Province (Mandera, Garissa, Marsabit, Moyale, Turkana, Pokot, and Tana River). The success of this model in addressing resource-based conflicts among pastoralist communities led to its formal adoption by the NSC, initially focused on hot-spot areas. With the support of UNDP and Oxfam, District Peace and Development Committees were piloted in the named districts in northern Kenya to spearhead preventive action at the district level. Later, the initiative was accelerated and expanded to other parts of the country, particularly following the post-election violence of 2007 and 2008.

Membership of District Peace and Development Committees consists of representatives of

- the local community (including elders, women, youth, and persons with disabilities);
- the District Security and Intelligence Committees;
- civil society organizations;
- provincial administrations (chiefs and their assistants, district officers, and district commissioners);[8] and
- the private sector.

The District Peace and Development Committees are hybrid structures that integrate traditional conflict-resolution mechanisms in various communities with the modern, formal dispute-resolution process. The objective is to prevent, manage, or transform conflicts. As such, District Peace and Development Committees have a fairly broad mandate, which includes the following objectives:

- promote peace education and a culture of peace and nonviolence;
- enhance conflict early warning and response;
- oversee the implementation of peace agreements and social contracts, in consultation with the security and intelligence committees and other stakeholders;
- facilitate trainings, community dialogue, sensitization, and awareness raising;
- put in place mechanisms to address interdistrict and cross-border conflicts;
- network with other peace forums to enhance harmonious relationships;
- monitor, evaluate, and report on peace- and nation-building programs.

Following its operationalization in 2002, the National Steering Committee took an overall coordination role for the District Peace and Development Committees. In addition, the NSC domesticated the CEWARN early-warning mechanism to serve its purposes through the National Conflict Early Warning and Early Response System (NCEWERS). Whereas the CEWARN mechanism (outlined in greater detail below) focuses on conflicts related to pastoralist activity in the Karamoja and Somali clusters, the NSC has broadened the scope of application of conflict-analysis tools developed under CEWARN to conflicts other than pastoral conflicts.

The NSC has divided the country into three clusters—urban, rural, and pastoral—reflecting the broad categories of conflict areas and types of conflict. Each of these clusters has different conflict dynamics and indicators. Conflict-early-warning information is collected in each of the clusters by peace monitors and members of District Peace and Development Committees who report directly to the NSC. Each of the forty-seven counties in Kenya is manned by at least one peace monitor.

[8] In Kenya, the provincial administration is part of the Executive. It is appointed and linked hierarchically to the Office of the President. Its members are in charge of a geographic area that increases in size from the village to the province (Kenya had eight provinces, now split into forty-seven counties). From the lowest level upward, there is the assistant chief (assisted by elders who are not civil servants), chief, district officer, district commissioner, and provincial commissioner. The membership of District Peace and Development Committees will change in view of the restructuring of provincial administration.

Structural Uses of Technology for Long-Term Prevention

PRELIMINARY

The use of innovative information communication technology in early warning in Kenya is a new phenomenon. Its adoption has been largely ad hoc and experimental, with an initial focus on limited geographical spaces, or hot spots. The national policy on peacebuilding and conflict management, which has been in development for more than seven years, does not foresee its use at a structural level. However, recent proposals by a group of civil society organizations could, if adopted, see the entrenchment of the use of such technologies in the national policy on peacebuilding and conflict management.[9]

Various national institutions have pioneered the use of innovative information communication technology in early warning, in particular security agencies and the National Cohesion and Integration Commission, which monitors hate speech. The commission is one partner in a conflict-prevention initiative called the Uwiano Platform for Peace, which includes a web-based data collection and analysis system and a short messaging service (SMS) system. The Uwiano Platform for Peace is a unique partnership between the National Steering Committee, the civil society organization PeaceNet Kenya, the National Cohesion and Integration Commission, and UNDP. It was established in the lead up to the historic referendum on the constitution in August 2010.[10] Each of the key Kenyan partners had a strategic niche: the National Cohesion and Integration Commission has a mandate to address hate speech; the National Steering Committee has close contact with the government security organs by virtue of being under the Ministry of Provincial Administration and Internal Security; and the civil society organization has a large grassroots network. Following training of District Peace and Development Committees on the use of the early-warning and early-response system, the Uwiano platform targeted particular hot spot areas in 2010.

Any member of the public can send an alert in relation to any conflict situation in the country. The information is transmitted to the platform and to security officials. The system is supported by a funding provision to facilitate quick response and intervention by actors on the ground. According to the National Cohesion and Integration Commission, the Uwiano platform strengthened constructive negotiation and consensus formation among communities in conflict across the country.[11] It is reported that through the rapid-response disbursement to District Peace and Development Committees and civil society organizations, the platform facilitated community dialogues and intercommunal mediation and reconciliation fora in identified hot spots. These were aimed at building trust among communities in a charged context of debates around the draft constitution. It is reported that these peace initiatives could have helped avert violence following the circulation of leaflets containing hate speech and inciting violence, which targeted specific communities and interests. The platform has also strengthened national and local capacity and coordination of partners in responding to conflict in Kenya. An iteration of the platform known as Uwiano Re-Loaded is in use by the same key partners and has been expanded to include various stakeholders for early warning and conflict monitoring.

NATIONAL INFORMATION NETWORK

As noted, the National Conflict Early Warning and Early Response System was essentially established to implement and domesticate the regional early-warning system CEWARN. This national information network is located at both local and national levels. At the local level, the network comprises the peace committees, security intelligence committees, the CEWARN field monitors, and National Conflict Early Warning and Early Response System peace monitors. At the national level, the network comprises data clerks, data analysts, and National Steering Committee staff based at the NSC secretariat, who are tasked with evaluating the data received from the field.

[9] Draft policy proposals on file with the author.

[10] National Cohesion and Integration Commission, "Milestones of the National Cohesion and Integration Commission," *The Star*, September 10, 2012.

[11] Ibid.

Information on conflict is received from various sources: peace monitors and field monitors, peace committees in the districts, members of the provincial administration that forms part of the national executive administrative structure,[12] local or district security and intelligence committees, civil society organizations working in the area (nongovernmental and faith-based organizations), and members of the public.

The information is received at the secretariat by data clerks and analysts who sift through it and verify it by making follow-up calls to the security structures on the ground (in particular those of the provincial administration), field monitors, and peace monitors. The communication between NSC staff in the control room and informants on the ground serves in part to verify information and also to alert relevant officials to act in respect of the incidents reported.

While the composition of District Peace Committees is varied and there is strength in this diversity, it is reported that information from government officials (in district intelligence and security structures, and the provincial administration) is treated as more credible than that from nongovernmental sources (NGOs, faith-based organizations, community-based organizations, and monitors). While concerns relating to credibility of information are valid, the apparent overreliance on state sources and state officials as the main source of credible information could undermine the objective of having a wide array of sources of information, which includes clergy and members of the communities. However, experience shows that the dynamics of ethnicity and other cleavages in communities often undermine the credibility of information provided by monitors due to bias.

An additional challenge is that of duplication of effort. Although the CEWARN field monitors and NSC peace monitors have been sensitized on the need to work together, synergy has not been created—especially in situations where the monitors hail from the conflicting communities. This has undermined, among other aspects of early warning, the horizontal sharing of information at the source and action points.

GIS MAPPING AND CROWDSOURCING

Kenya's National Conflict Early Warning and Early Response System is pioneering the use of crowdsourcing to gather peace and conflict information through two main media. The first is through SMS using a 108 SMS shortcode. The NSC has partnered with Safaricom, the leading cell phone operator in Kenya, to enable the public to send peace and conflict alerts to the National Steering Committee through a 108 SMS code. The public has been made aware of the SMS code through print (newspapers) and electronic media. The SMS is charged at the normal network rate. Through an inter-phased program, the text messages sent are presented in an online system in the NSC secretariat, showing the location of the individual, their phone number, and the peace or conflict issue reported. This allows the data clerks to call the individual and clarify details of the incident reported.

Amani 108 Online Reporter is the second mode of crowdsourcing. Through the reporter, online peace and conflict reports can be made in three ways: through email, Twitter, or Facebook. The Amani Kenya website also monitors the occurrence of hate speech in social media (Twitter, Facebook) in real time.

The National Steering Committee, through the National Conflict Early Warning and Early Response System, is also working to incorporate geographic information system (GIS) mapping as another conflict-mapping tool. Using this tool, the locations of conflict situations and conflict actors can be geographically represented on a map to the highest degree of accuracy possible.[13] This map can then be analyzed to assess force to space ratios, for instance, meaning the amount of security "force" required to manage a given space in a particular set of circumstances. Although the Amani Kenya 108 online platform has a map, the map represents the validated reports submitted and verified by the data analysts at NSC from emails, text messages, and social media. Media reports provide an additional source of information, both for GIS Mapping and Amani Kenya platform discussed above. Once

[12] In terms of the new constitution, the provincial Administration is to be restructured to be aligned with the devolved system of government under the new constitution in which power is shared between national and forty-seven county governments.

[13] See www.nscpeace.go.ke/108/report.php . GPS Mobile Mappers have an accuracy of +/- 25 centimeters for instance.

information is verified, it is used to inform the deployment of security personnel to a particular space.

REGIONAL PERSPECTIVES

East Africa's Intergovernmental Authority on Development (IGAD) pioneered use of technology in the early-warning context. Its pilot project, ICT4Peace, was rolled out in 2006. The five-year pilot period expired in 2012. Although the subsequent review of the project had yet to be published at the time of writing, perspectives documented below partly reflect views of individuals closely associated with the ICT4Peace project. To begin with, a background of the CEWARN mechanism is provided in order to place the ICT4Peace project in its proper context.

The CEWARN Mechanism

In recognition of the vital role played by early warning, IGAD decided in 2000 to establish the Conflict Early Warning and Response Mechanism (CEWARN) under its Peace and Security Division.[14] CEWARN was officially established by a protocol signed by IGAD member states during the ninth summit meeting held in Khartoum, Sudan, in 2002.

The mandate of CEWARN is to "receive and share information concerning potentially violent conflicts as well as their outbreaks and escalation in the IGAD region."[15] Although the CEWARN protocol outlines several types of conflicts, the focus of CEWARN between 2002 and 2011 was the monitoring of cross-border pastoral and pastoral-related conflicts.[16] The rationale for this focus was that cross-border pastoral conflicts were of mutual concern to all IGAD member states and as such would encourage cooperation between CEWARN and the Horn of Africa states.

In its post-2012 strategy, CEWARN has expanded its conflict mandate to incorporate the unique conflict concerns of each of the IGAD member states. In Kenya, for instance, an election violence monitoring and analysis component has been incorporated into the mechanism in anticipation of the March 2013 general elections. CEWARN's primary programmatic focus is the "collection of data and analysis of pastoral conflicts and the linkages of these assessments to timely response actions."[17]

CEWARN focuses on two issues: early warning and early response. The aim of CEWARN is to anticipate potential conflict situations, facilitate the peaceful settlement of disputes, and respond to violent conflicts in the region. The CEWARN mechanism in Kenya operates in two "areas of reporting." The first is identified as the Karamoja cluster, which encompasses the cross-border areas of Ethiopia, Kenya, Uganda, and South Sudan.[18] The second is identified as the Somali cluster and covers the cross-border areas of Kenya, Ethiopia, and Somalia.

STRUCTURE OF CEWARN

CEWARN has a trifurcated structure comprising local, national, and regional networks and institutions. At the regional level, it comprises the CEWARN Unit, the Technical Committee for Early Warning, and the Committee of Permanent Secretaries (CPS). While at the national level it includes the assistant country coordinators, country coordinators, the National Research Institute, and the Conflict Early Warning and Early Response Units. At the local level, it comprises field monitors.

REGIONAL STRUCTURE

The heads of the national Conflict Early Warning and Early Response Units (CEWERUs) collectively form the Technical Committee for Early Warning (TCEW). The technical committee convenes twice a year to discuss and analyze the CEWARN Mechanism. The focus of the TCEW is early-warning reports and response options, and its recommendations are submitted to the Committee of Permanent Secretaries (CPS), the policymaking organ of CEWARN, which comprises senior government representatives designated by member states. The Committee of Permanent Secretaries in turn reports to the Council of Ministers, which in

[14] "CEWARN Strategy (2007-2011)," Addis Ababa: CEWARN Unit, November 2006, pg 3.

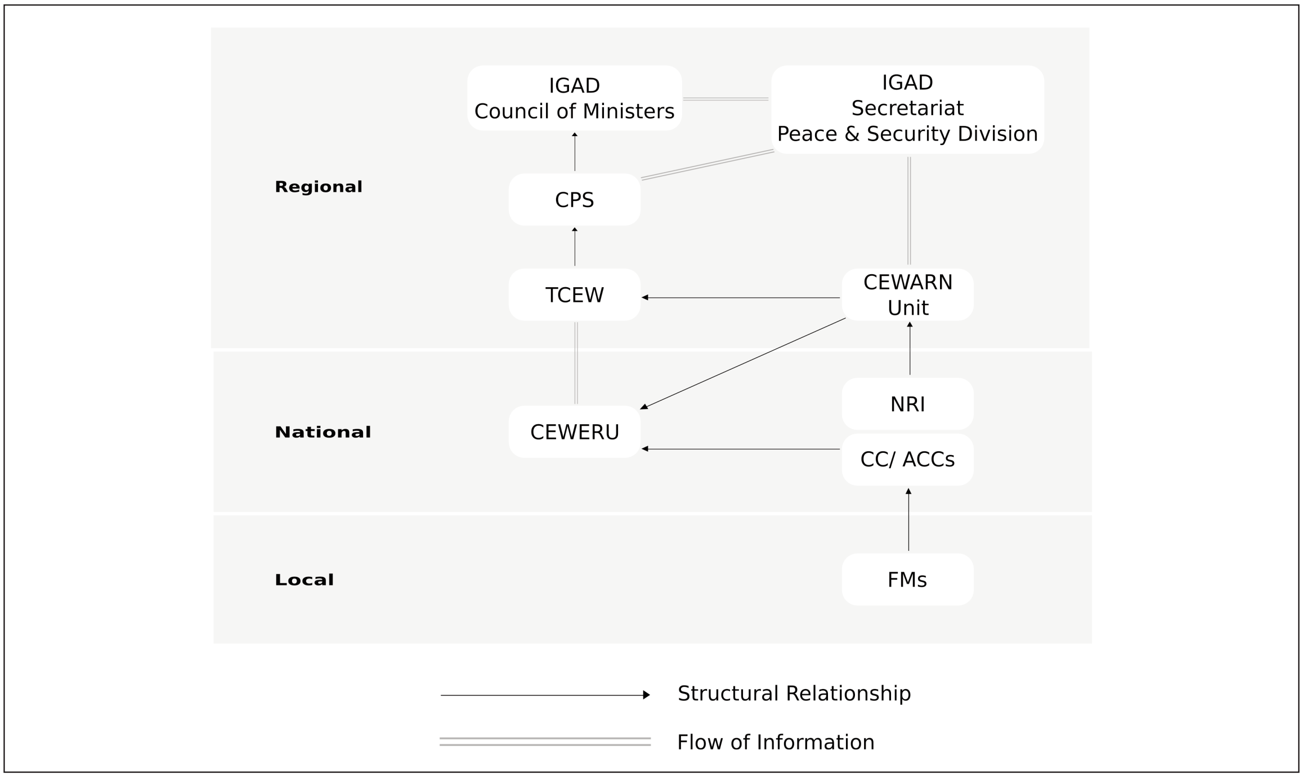
[15] Ibid.

[16] Decision adopted by the 5th Committee of Permanent Secretaries (CPS) Meeting, May 2006 in Nairobi, Kenya.

[17] "CEWARN Strategy (2007-2011)," CEWARN Unit, p. 5.

[18] This was the initial pilot area for the CEWARN Mechanism in 2003.

Figure 1: The CEWARN Structure



turn reports to the Assembly of Heads of State and Government. The Executive Secretary, the Director of Peace and Security Division (IGAD Secretariat), and the Director of the CEWARN Unit are ex-officio members of the CPS.

NATIONAL STRUCTURE

The CEWARN unit headquarters[19] is the regional "knowledge bank" for data collection, conflict analysis, information sharing, communication of response options, and data quality control.[20] It collects information and data through an established system of local information collection networks. Each network is composed at national level, of field monitors trained to collect information, categorize the information within given parameters, and enter the information into prescribed reporting formats. The field monitors are supervised by assistant country coordinators and country coordinators. In Kenya, there are twelve field monitors in the Karamoja cluster and nine field monitors in the Somali cluster. Each cluster is supervised by an assistant country coordinator, and the entire process is managed by a country coordinator.

CEWARN has identified and contracted national research institutes as partner organizations for the mechanism. National research institutes are primarily responsible for the collection and analysis of the field data. The field monitors, assistant country coordinators, and country coordinators are contracted and administered by the research institutes. The current institute in Kenya is The Consulting House, a multidisciplinary policy and security think tank working in the Great Lakes region. The Consulting House has only recently been incorporated into the CEWARN mechanism; as such, its capacity to analyze the data collected has yet to be tested and realized.

At the national level, the CEWARN mechanism works through Conflict Early Warning and Early Response Units (CEWERUs). The units are directed and managed by CEWERU heads, who are nominated by the member states. Each CEWERU is mandated to form a steering committee, which should include, inter alia, representatives of relevant ministries and provincial administrations,

[19] The CEWARN Unit is based in Addis Ababa, Ethiopia.
[20] "CEWARN Strategy (2007-2011)," CEWARN Unit, p. 15.

security bodies (such as police, intelligence, and military), legislative bodies, civil society organizations, academia, and religious organizations. The national research institutes work closely with their respective CEWERUs to validate and interpret the data and to help formulate response options. In Kenya, the CEWERU is the National Steering Committee on Peacebuilding and Conflict Management (NSC) formed in 2001.

CEWARN's Use of Technology: Early-Warning Tools

THE CEWARN REPORTER

In undertaking their tasks in early warning and early response, country coordinators use the CEWARN Reporter. The CEWARN Reporter is a network software program specifically designed for early-warning purposes and used by the country coordinators to enter and store the standardized field reports submitted to them by the field monitors. The reports submitted by the field monitors are based on a set of security audit questions (indicators) that monitor local issues, including communal relations, peace and security, natural disasters and resources use, economic activities, civil society activities, and community movement.

The CEWARN Reporter has fifty-seven indicator questions that serve to monitor factors that accelerate, trigger, and/or mitigate violent incidents. Based on the data gathered in the field, the following reports are produced: alerts on impending violence, situation briefs (as needed), quarterly country updates, and cluster reports.

The reports generated are shared with each national Conflict Early Warning and Early Response Unit for response actions. The CEWARN unit uses its website as one of the channels for disseminating the early-warning reports produced. However, the reports available on the website are infrequently updated.

The reporter has three main functions.[21] First, it enables users to analyze the reports. Second, it provides users with a system for data management. Third, it presents a graphic display of incident frequency over time. Fourth, it allows for analysis of field data with a view to identifying emerging trends. Ideally, the reporter "assists in the understanding and analysis of how changes in pastoral behavior are likely to lead to more tension and conflict, or co-operation."[22] The reporter is accessed online and is open only to IGAD officials, CEWERU representatives, national research institutes, and the staff of the CEWARN Unit.

Although CEWARN has a database spanning approximately ten years of qualitative and quantitative field data detailing cross-border pastoral conflicts, this information has not been fully processed. The information collected is purely descriptive, chronicling the incidents and situations of violent conflict. In-depth analysis of the data and accurate prediction of potential violent situations is a critical challenge faced by the mechanism. In addition, the CEWARN mechanism depends solely on the field monitors and the knowledge of country coordinators for its information and analysis. In some instances, the information provided by the field monitors is not objective, and this may hinder the effective working of the mechanism. The CEWARN Reporter does not, as yet, integrate structural data—that is, data on ethnicity, culture, the climate, and natural resources available in an area. Yet this information is necessary to contextualize and interpret the data relating to field events or incidents.

CEWARN ICT4PEACE PROJECT

The ICT4Peace project was designed to exploit ICTs for timely transmission of early-warning information on violent conflicts to decision makers in IGAD member states, to facilitate a timely response. It was conceived by CEWARN with the support of the East Africa division of the United States Agency for International Development (USAID/EA).

The pilot ICT4Peace project focused on the Karamoja cluster (consisting of the border areas of Uganda, Kenya, Sudan, and Ethiopia), which is prone to resource-based conflicts and livestock rustling. Research commissioned by CEWARN and USAID/EA in the early 2000s had shown that while the conflict-prone locations in the CEWARN areas

[21] "CEWARN Strategy (2007-2011)," CEWARN Unit, p. 17.
[22] Ibid.

of reporting had very poor communications infrastructure, the Karamoja cluster was highlighted as having the poorest communications infrastructure. The target areas of Turkana in Kenya, the Karamoja in Uganda, and the regions of South Sudan and Ethiopia directly bordering Kenya have limited telecommunications coverage.

Without telecommunications coverage, the only means available to CEWARN's field monitors to report on situations of potential or actual conflict was to walk or hitch a ride to areas with communications coverage in order to transmit the information. The research also indicated that some hot spots were up to 400 kilometers away from telecommunication coverage.

Largely because of these factors, early-warning information would take days or even months before assistance was available. When the assistance came, it would be too late: lives were needlessly lost, property destroyed, and communities and families dislocated. It was noted that ICTs could help by instantly delivering information from the hot spot to the relevant actors for intervention. This is how ICT4Peace was born.

Although a number of ICT options were considered for use by CEWARN, high-frequency radios were chosen as the most sustainable solution for reasons including mobility and sustainability. Accordingly, through this project, CEWARN provided high-frequency radios and high-gain antennae phones to local peace structures in conflict-prone areas. The project piloted in the Karamoja cluster described above.

During the pilot period, the radios were used for communication between the local peace committees and field monitors, and among the field monitors themselves. At the time of writing, the high-frequency radios are not in frequent use. Only two radios remain fully operational, and they are rarely switched on. A proposition has been made to supply satellite phones to the field monitors in areas with limited network coverage. This proposal has yet to be implemented.

Assessing the ICT4Peace Project

At the time of writing, CEWARN was undertaking a review of the pilot ICT4Peace project. In addition to points made in the integrated analysis below, the following broad points can be made about the project in review. First, initial sentiment captured suggests that the project was a major disappointment. The manner in which the project was conceived appears to have rested on flawed assumptions. Second, the timely flow of information between field monitors, local peace committees, and governmental security agencies was undermined by a variety of factors, including inadequacy of base radios (only one purchased). Third, mistrust among communities in the target area engendered by a long history of violent conflict meant that field monitors were often seen as spies for rival communities. Bias among certain field monitors appears to have further undermined the credibility of the information shared. Fourth, the choice of technology was not appropriate, since high-frequency radio was an outdated technology. Lastly, lack of community buy-in, due in part to lack of consultation, was perhaps the major drawback of the entire enterprise. Though well intentioned and timely, the initiative can be said to have broadly failed to meet its objectives.

CEWARN and Early Response

As noted above, CEWARN focuses on early warning and early response. Yet, one of the weakest elements in the CEWARN system is the link between early warning and early response. A variety of factors—structural and operational—can be blamed for this state of affairs. The assumption is that information sharing is a critical factor in early response, that the nature of information shared (whether it is credible and actionable) and the timeliness of sharing are key to determining the effectiveness of early response. But the capacity of national actors to respond appropriately, including their ability to absorb and act on that information on a timely basis, are equally important factors.

Kenya's Conflict Early Warning and Early Response Unit (CEWERU), which implements CEWARN at the national level, offers several advantages in terms of early warning. First, its domicile in the Office of the President ensures that it is linked to security infrastructure, which is critical for early response. This linkage is supported by the fact that the current head of the National Steering Committee (NSC) doubles up as the CEWERU head and thus sits in security meetings. Second, the diversity in NSC's membership ensures that a broad spectrum of relevant actors is linked to early warning. The membership includes representatives of relevant ministries and provincial administrations; security bodies, such as police, intelligence, and military agencies; a variety of civil society organizations; and representatives from academia. A contracted national research institute works closely with CEWERU to validate and interpret data received and to help formulate response options.

In spite of the advantages that may be derived from the location of the national early-warning and -response unit, the challenge has been to “civilianize” the mechanism in a way that promotes information sharing in a context where there is a tendency to see security through a narrow lens: that of state security.

The greatest impediment to early response relates to the channels established to facilitate vertical sharing of information between the regional and national actors. It is reported that previously, it would take up to six months for information to be transmitted from the field to member states. Information would be sent to the CEWARN unit in Addis to be processed: input into the system, analyzed by conflict analysts, and transmitted onward to states for action.

The disconnect between the regional component of CEWARN and the national centers of action was that there was an inadequate number of conflict analysts—the only persons authorized to access the system to generate graphs (showing trends). Field monitors could input data but apparently had no authority to retrieve it! The time lapse between reporting, retrieval, and sharing of information did undermine effective early response. The initial response to this problem was to train field monitors and hire additional conflict analysts. But CEWARN continues to face serious capacity challenges, resulting in the current predicament: there is ten years worth of data that has yet to be analyzed and exploited for the prevention of conflict. It is reported that there are plans to introduce more flexibility in the retrieval of information to facilitate early action. The expansion of the national early-warning and -response unit’s focus beyond pastoralist conflicts and the introduction of new technology tools at the national level appear to be eliminating reliance on regional sources and the dysfunctions associated with them. However, the persistence of cross-border conflicts continues to necessitate the improvement of existing information sharing in CEWARN.

Opportunities, Impact, and Challenges in the Use of ICTs

Several inferences can be drawn from the discussion on structural uses of technology in early earning in Kenya. Broadly, it should be noted that the use of innovative communication technologies in early warning remains a new phenomenon, and despite its potential to enhance preventive action, its absorption is somewhat tentative. While cost is a factor, the lack of a coherent and comprehensive national policy on the broad issue of peacebuilding, and in particular on the potential for technology in early warning, is partly to blame for the current state of affairs.

OWNERSHIP

Given the manner in which innovative communication technologies have been introduced to the early-warning context—partly a factor of cost and capacity—the issue of ownership appears to recur in discussions. While the role of donors in particular is appreciated and celebrated, there are also a number of unanswered questions associated with the purpose of such an undertaking and regarding who owns, can access, and can use the information collected—whether the government, grassroots actors, civil society organizations, donors, or third countries.

The issue of outside donors raises questions beyond the ownership debate. Many donors do more than provide direct financial support to government: they fund and empower civil society organizations and other community groups. Donors are known to intervene directly in communities, and are involved in peacebuilding activities at various levels. Even where donor agencies are engaged in purely humanitarian work, the geographic spaces in which they are engaged are often in conflict or are prone to conflict. A good example is remote northern Kenya, which is afflicted by both inclement weather and resource-based conflict and interethnic conflict. Apart from its geographic remove, this is also a region with limited government reach. To achieve durable solutions to problems being addressed by these agencies, provision of humanitarian assistance must be coupled with peacebuilding initiatives.

In view of these realities, a claim may be made that donor agencies engaged in these areas are entitled to information that can enable them to fashion structural interventions that more effectively contribute to preventive action or early response. In fact, donor agencies and development organizations such as UNDP and Oxfam have been involved in training various actors, especially District Peace Committees and civil society organizations, to enhance their capacity to play a more effective role in early warning and early response.

Yet, as noted elsewhere, the structure of the state and the secrecy arising from the manner in which state security has been understood does privilege state actors when sharing of relevant information.

Similar concerns can be expressed in relation to nonstate actors at the community level (such as elders, clergy, and civil society organizations) that are not adequately integrated into response measures from an information-sharing perspective. Frequently, their role is largely restricted to providing information and validating action by state officials.

Some of the critical questions that remain to be addressed are the following: What kind of information and data can and should be accessible to donors and humanitarian and development agencies? Given legitimate national security concerns surrounding information sharing in this context, what arrangements should be put in place to ensure that certain kinds of information are reserved for governmental actors without undermining preventive action and early response?

FINANCES

Most ICT tools have been introduced into conflict-early-warning mechanisms with the support of donor funding (e.g., USAID, UNDP, Oxfam GB). The drawback of this approach lies in its questionable sustainability, especially when ICTs are not maintained and fall into disrepair. This was the case with the high-frequency radios that were introduced to the Karamoja cluster as part of the ICT4Peace project. It is critical that maintenance budget lines be incorporated into the overall monitoring budgets at both national and regional levels to maintain the ICT tools required.

APPROPRIATENESS OF TOOLS

The experience of the ICT4Peace project shows that the choice of tools is critical. Given the lack of physical and technological infrastructure, and the inaccessible nature of many of the conflict areas, self-sustaining and low-maintenance tools are often the best choice. Literacy levels also dictate the kind of technologies that can be used. Part of the reason why this project had a limited impact was that the tools chosen (high-frequency radios) were not appropriate for the target regions, as well as being inadequate. All field monitors (manning a total six high-frequency radios) were served by only one base radio, located in the region of one of the communities in the conflict. It is noted that because high-frequency technology is so dated, there were also serious problems linking up field monitors with the police communication network. It appears that no feasibility study was done before the launch of the project and that the process failed to include or did not adequately involve target communities.

CAPACITY

Capacity is a critical factor. One must have the right skills in sufficient quantities to operate the system over time. In the case of the National Steering Committee, it has a skeletal staff in Nairobi charged with receiving and analyzing a large amount of data on a daily basis. The same applies to CEWARN, which operated a system where only the handful of analysts located in Addis Ababa could access the system to generate graphs showing trends for use by national actors. To entrench structural uses of technology, the capacity and systems to process and use data appropriately need to be built. The full potential offered by the pool of information obtained from various sources can only be tapped if the right skill sets are assembled to make sense of the data and to channel it for action at state and community levels to enhance preventive action and early response. For long-term planning and structural intervention, there is a need to build capacity to analyze data for trends.

Indeed, capacity building of all key actors in the peace and security system is critical. In particular, initiatives aimed at strengthening the link between early warning and early response, such as those undertaken in 2010 with donor support, should be replicated and accelerated. These initiatives saw the Uwiano platform focus training of District Peace Committees in select hot spots on the use of the early-warning and early-response system.

HORIZONTAL AND VERTICAL SHARING

The state appears to be the main beneficiary of information in the system run by the National Steering Committee; District Peace Committees and chiefs are informed to act on incidents only once information is verified. In general, horizontal sharing of information at the societal level is limited. There is a sense in which access to information collected, insofar as it relates to security, is treated as restricted (only accessible on a need-to-know basis) and is shrouded in secrecy. Dysfunctions and competition at the local level could also be responsible for undermining the horizontal sharing of information. The multiplicity of state actors (security, intelligence, provincial administrations) in a context of weak interagency linkages and collaboration also poses unique problems.[23] The ongoing reform process (foreseen in the new constitution) must create proper collaboration and information-sharing frameworks between agencies and different levels of government, as well as with nonstate actors or grassroots actors when appropriate.

CULTURAL AND POLITICAL APPROPRIATENESS

While preventive action should move apace with technology, a factor that should not be overlooked is contextual (cultural, historical, and political) appropriateness. Culture presents a structural challenge to the use of technologies in conflict prevention. In the case of the ICT4Peace project, it was noted that certain cultural factors were not sufficiently considered or ignored altogether, and this undermined the initiative in the end. For instance, the fact that two of the major communities in the pilot space were engaged in conflict with each other for decades meant that field monitors selected from those communities were compromised in a context of deep suspicion. The location and control of the sole base radio by one community ensured that no information could be shared. With respect to the current National Steering Committee initiatives, the deep suspicion and fear that Kenyans have for the police and security establishments in general could be instructive. As demonstrated in the ICT4Peace project, structural impediments are due not only to an illiberal state context but also a cultural one.

CREDIBILITY OF INFORMATION

The credibility of information received, especially when crowdsourced or when monitors are deployed, must be a key concern. A major challenge noted when dealing with the field monitors is that they tend to be biased in favor of their community. This bias manifested itself in at least two ways: reports submitted were in some instances drafted in non-neutral terms. For instance, rather than report on a conflict situation or incident as it happened verbatim, the field monitor would use the term "we" for his or her community and "them" for the perceived aggressors. Second, some monitors have previously not reported when a community they view as an enemy or threat has been attacked. They would only report when their own community was attacked and would sometimes exaggerate the extent of damage. This shows that technology has its limits: even where technology is used, the credibility of the data is not automatically guaranteed. Comprehensive training and sensitization of field monitors is required to enable them to undertake neutral conflict reporting.

INTERCONNECTIVITY

The initiatives by the National Steering Committee and the ICT4Peace project by CEWARN raise important concerns related to interconnectivity. It was noted that there was difficulty linking high-frequency radios and police communication, which undermined response. In part because the project was cross-border, signals could not be sent and received across international borders, which meant that communication could also not be made to authorities across the border to apprehend retreating livestock raiders. Although civil society organizations made attempts to empower local leaders on either side of the border, these initiatives were not undertaken between governments and thus had limited effect. Linkages between technologies are necessary for purposes of cross-referencing and verification, to enhance credibility of information. In remote Turkana, located in northern Kenya toward the Ethiopian border, the fact that field monitors had to travel for two weeks to reach a

[23] The Waki Report decried the lack of collaboration between security agencies, especially intelligence and enforcement (i.e., police). This lack of collaboration is partly blamed for inadequate and belated response to PEV.

center where they could send an email relating to particular incidents greatly undermined the objectives of the project.

DELETERIOUS EFFECTS OF TECHNOLOGY

While the positive impact of the use of technology can be emphasized, certain negatives should be acknowledged. It has been noted in respect of the ICT4Peace project that with the introduction of high-frequency radios, livestock rustling and banditry became more lethal, precise, and more difficult to respond to and police. Cases were reported where livestock rustlers and bandits had been able to obtain information relating security strength and movement and to strike vulnerable areas. The integrity of the technologies chosen is thus critical.

Recommendations

GOVERNMENTS

ICTs have the potential to positively impact and enhance conflict prevention and early warning. In a long-term preventive context, their use cannot be ad hoc. Full benefits can only be obtained if the use of ICTs is secured by policy and structurally entrenched. Where various technologies are in use, such as in the Kenyan case, it is necessary to link them. One benefit is that cross-referencing of information from various sources ensures credibility of the system. In addition, pooling data in this way could facilitate analysis and identification of trends and structural factors that could be addressed to more effectively prevent conflict. Overall, the government and other relevant actors should invest in infrastructural development, capacity building, and in creating the right policy environment to anchor the use of technologies in early warning. The importance of investing in analytical capability both at national and local levels cannot be overemphasized. IGAD's CEWARN system now has a huge pool of information that should be analyzed for trends and used by national and regional authorities.

It is critical to understand that the new Kenyan constitution has impacted society deeply. Several factors introduced by the new constitution will have a bearing on several aspects of early warning, in particular the use of ICTs. These factors include: the inclusion of the right to information in the constitution; the right to access to justice; restructured and rationalized national security architecture subjected to full civilian control; and a more open and democratic dispensation based on the rule of law and respect for human rights—where security considerations will no longer be a trump.[24] All these will impact the use of ICTs from an information-sharing perspective.

DONORS AND INTERNATIONAL ACTORS

Donors, and the international community more broadly, have played and will continue to play an important role in peacebuilding in Kenya. Yet, the cases of ICT use for conflict prevention in Kenya and East Africa described above indicate several things.

First, the appropriateness of ICTs (and other measures) adopted raises concerns about ownership and the role of the beneficiary communities. There is a need for donors to involve beneficiaries more in these decisions.

Second, while donors may be well intentioned, their interventions and push for certain responses could evoke suspicion (largely among government actors), especially in relation to the use of technologies that raises state-security concerns.

Third, the viability and sustainability of the technologies to be instituted (which is a factor not only of financial considerations but also developments in the field of technology itself) ought to be afforded more thought, if long-term prevention and impact is desired.

CIVIL SOCIETY

Civil society groups continue to play an important role in peacebuilding. Various groups, including faith-based organizations, have initiated projects in conflict hot spots to prevent violence. Civil society organizations are represented on District Peace Committees and other local structures. While they are an important source of information from an early-warning perspective, they frequently lack the

[24] Recent High Court decisions have confirmed a paradigm shift: state security will no longer be an all-trumping consideration, especially where rights are concerned.

capacity to act beyond certain limits where state actors are absent or weak. Their access to actionable information also tends to be restricted. Both of these factors undermine preventive action.

Civil society organizations can be credited with some of the earliest uses of technology in a preventive context. A good example of civil society recognizing the potential for technology to help address conflict is the Ushahidi platform, a collaborative initiative of Kenyan citizen journalists created during the post-election violence of 2008. The initiative consisted of a website that was used to map incidents of violence and peace efforts throughout the country, based on reports submitted via the web and cell phones. According to Ushahidi, the website had 45,000 users in Kenya at that time. Its success catalyzed the expansion of the initiative and creation of a platform based on it, which is now in use by others around the world.[25] Since early 2008, the initiative has grown "from an ad hoc group of volunteers to a focused organization." According to Ushahidi, the team is currently comprised of individuals with a wide span of experience ranging from human rights work to software development. The platform is customized on a consultancy basis for multiple purposes worldwide, including in monitoring elections or crises and to "crowd source an experiential marketing campaign for a brand or event, or even to organize a music group's fans and shows." Ushahidi has built a strong team of volunteer developers primarily in Africa, Europe, South America, and the US.[26]

By enabling civil society actors to trigger early response, ICTs can help bridge the gap between civil society organizations and government structures in situations of weak or nonexistent communication infrastructure. It is critical to empower these actors, not least by sharing information appropriately. Indeed, the new Kenyan constitution will likely facilitate access to this kind of information, which could relate to trends in relation to certain conflicts or systemic factors underlying these conflicts in certain areas. Regardless, the horizontal linkages that exist between actors who have the ability to respond quickly, effectively, and appropriately should be strengthened.

[25] See www.ushahidi.com .

[26] See www.ushahidi.com/about-us .

Conflict Cure or Curse? Information and Communication Technologies in Kyrgyzstan

Anna Matveeva[1]

Introduction

Kyrgyzstan has not yet acquired a critical mass of Internet users in order for the "online" to start producing a visible impact upon "offline" street politics. However, when it comes to information and communication technologies (ICTs), Kyrgyzstan is the most advanced among Central Asian countries, and the public is becoming more tuned-in: "the Internet is becoming a source of information for the masses."[2] While other Central Asian governments have been blocking critical websites almost since the Internet became available, Kyrgyzstan started the practice only in 2005. Despite such restrictions, this remains the most liberal regime in the region with the most robust sociopolitical activity and a relaxed media policy.

Officially, the development of a national ICT policy started in 2000, when the government announced that Kyrgyzstan "chooses information society."[3] This initiative was actively supported by international organizations, such as the United Nations Development Programme (UNDP), the US-based nonprofit IREX, and the Soros-Kyrgyzstan Foundation. With donor support, in 2002 Kyrgyzstan adopted the National Strategy Information and Communication Technologies for Development of the Kyrgyz Republic, which was approved by a presidential decree, and a program for ICT development.[4] Annual conferences were conducted to assess progress, but the practice came to a halt in 2006.

The present study seeks to answer two research questions. First, it asks what role new ICTs play in preventing violent conflict, and in conflict gestation and escalation to violence. It explores the ways technologies allow data about perceptions of risk and safety to surface, which data is trusted, and how recipients respond to data they trust in conflict conditions. Second, given the substantial international presence in Kyrgyzstan and experience accumulated in early warning and conflict prevention, the study examines lessons the international community can draw from the use of ICTs to strengthen its voice and action.

The paper outlines the conflict background in Kyrgyzstan and the state of ICT development in the country. It analyses the role ICTs played in the crises of 2010 and continues to play in the postconflict situation, and discusses the use of ICTs by the government and the diaspora. The paper concludes with an analysis of internationally sponsored efforts in the use of ICT for early warning and conflict prevention, and a reflection on its advantages and limitations.

Background to the Conflict in Kyrgyzstan[5]

Kyrgyzstan is a small, landlocked country in Central Asia that borders China and Kazakhstan. It achieved independence in 1991 and since then has undergone two forceful transfers of power, termed "revolutions," in 2005 and 2010. Kyrgyzstan is affected by a north-south split, and the two parts of the country have distinct cultural and political identities. The south experienced outbreaks of interethnic conflict between the Kyrgyz majority and Uzbek minority in 1990, when more than 300 people died, and in June 2010, when an estimated

[1] The author held the position of Head of Research Secretariat for the international Kyrgyzstan Inquiry Commission (KIC) in 2010 based in the south of Kyrgyzstan. This paper draws upon field research material gathered in 2010 for the KIC.

[2] Personal interview with Daniil Kislov, founder and editor of Ferghana.ru, Moscow, September 2012, by Skype.

[3] EU–Eastern Europe and Central Asia Gateway for ICT Research, Development and Policy Dialogue, "Kyrgyzstan," available at www.eeca-ict.eu/countries/kyrgyzstan .

[4] Kyrgyztan Ministry of Transport and Communications, "National Strategy Information and Communication Technologies for Development in the Kyrgyz Republic," 2002, available at www.unapcict.org/ecohub/resources/national-strategy-information-and-communication-technologies-for-development-in-the-kyrgyz-republic .

[5] This section draws upon the author's earlier work "Kyrgyzstan in Crisis: Permanent Revolution and the Curse of Nationalism," Working Paper No. 79, Crisis States Research Centre, London School of Economics, September 2010 and "Violence in Kyrgyzstan, Vacuum in the Region: The Case for Russia-EU joint Crisis Management," Working Paper 02.11, Civil Society & Human Security Research Unit, London School of Economics, December 2011.

470 people died.[6]

The latter conflict was preceded by an April 2010 uprising against the rule of President Kurmanbek Bakiyev, whose ascent to power followed the 2005 Tulip Revolution. The anti-Bakiyev protests in 2010—termed the "second revolution" or "April events"—turned violent, leading to the ousting of Bakiyev in the capital Bishkek and the death of 86 people.[7] The events brought to power a provisional government that consisted of representatives of the opposition forces, oppressed by the previous regime. Roza Otunbayeva, a former international diplomat, was elected as the chair of the provisional government and became an interim president thereafter.

As political change unfolded in the capital, located in the north, the situation in the south was deteriorating. Bakiyev had come to power with significant popular support in the south, where he is from, and now the ex-president's clan tried to cling to power. Meanwhile, the two transfers of power, split regional loyalties, low morale, and widespread corruption all served to weaken the security sector. The removal of Bakiyev's regime, which had previously played a centralizing role in organized crime, created a vacuum that opened up competition between rival groups and contributed to a free-for-all environment for raiding assets and racketeering. The Uzbeks were more vulnerable to crime, since they had a low standing among the police and prosecutors.[8] Intercommunal relations worsened. Uzbek leaders expressed their concerns regarding their language, representation, and safety from crime. At the same time, the Kyrgyz community felt ostracized by the new government, which, in their view, preferred to rely on Uzbeks. Low-level intercommunal violence became common.

Enthralled with political reform and the opportunity to introduce a new constitution, the provisional government lost sight of the south. Police reports of a rise in interethnic tensions were ignored, and the provisional government did not trust the law-enforcement apparatus they had inherited from the previous oppressive regime. The first outbreak of interethnic conflict occurred in the southern town of Jalalabad, in which six people were killed; but as violence subsided, so did the government's attention.

On June 10th the police in Osh—the largest city in the south—were unable to make an angry Uzbek crowd disperse. The crowd clashed with police and Kyrgyz residents who mobilized against them, and beatings and burnings ensued. The police and army paratroopers opened fire on the protesters during the night, and bystanders died in the process. By the early hours, interethnic violence had spread throughout the city. Crowds of rural Kyrgyz advanced toward Osh, and the situation deteriorated when they surrounded the city. The Uzbeks set up defenses to prevent Kyrgyz crowds from entering their neighborhoods. The Kyrgyz seized weapons from the army, police, and border guards, and captured military vehicles. After firefights, retreats, and sieges, the Kyrgyz crowds overpowered the Uzbek defenses and poured into Osh. Killing, looting, rape, and arson attacks unfolded on a massive scale. On June 13th violence subsided as information came in that fighters from Uzbekistan were approaching to take charge. This turned out not to be true, but it motivated many Kyrgyz attackers to leave.

However, on June 12th violence had spread to Jalalabad province, where Uzbeks tried to set up defenses to prevent Kyrgyz from the north from joining rioters in Osh. This tactic created a standoff between Kyrgyz and Uzbek communities. Some rural Kyrgyz went to Jalalabad to rebuff what they saw as an Uzbek plot to establish autonomy and undermine "Kyrgyz statehood." Street fighting, looting, and arson followed for two days. Altogether, up to 470 people were killed; 74 percent of the dead were Uzbek, 25 percent were Kyrgyz, and 1 percent belonged to other ethnic groups. More than 90 percent of those who died were men.[9]

[6] Kyrgyzstan Inquiry Commission, "Report of the Independent International Commission of Inquiry into the Events in Southern Kyrgyzstan in June 2010" (KIC Report) available at http://reliefweb.int/sites/reliefweb.int/files/resources/Full_Report_490.pdf .

[7] Anna Matveeva, "Kyrgyzstan in Crisis: Permanent Revolution and the Curse of Nationalism," Working Paper No. 79, Crisis States Research Centre, London School of Economics, September 2010.

[8] Anna Matveeva, Igor Savin, and Bahrom Faizullaev, "Kyrgyzstan: Tragedy in the South," Ethnopolitics Papers 17, Exeter Centre for Ethnopolitical Studies/Specialist Group Ethnopolitics of the Political Studies Association of the UK, April 2012.

[9] Information provided by Kyrgyzstan's Ministry of Healthcare, figures of dead by Kylym Shamy, Kyrgyzstan's NGO. They slightly differ from the Prosecutor General Office's figure of 439 in December 2010, but prosecutors acknowledged that the number may grow slightly as investigations proceed. Information provided to the KIC Report, p. 44, para 222.

The central government was not in a condition to deal with a crisis of such magnitude so early in its term, and it underestimated warning signals from the south. The State Committee on National Security (GKNB) was caught unprepared. It was only during the crisis that the provisional government uncovered the true condition of the security agencies. Military, police, and border guards became easy targets for seizing weapons and equipment, and some started to flee. Crisis management and response was chaotic and at times nonexistent. The defense minister, the main person in charge, could not be reached for several hours on June 11th, as he was outside of mobile network coverage and did not have a satellite phone.[10] Bishkek attempted to send troops from the north and called in reservists, but this was ineffective. Some among the deployed army and police sympathized with the Kyrgyz rioters and facilitated their attacks on Uzbek *mahallas* (urban quarters).

The provisional government recognized on June 11th that the country did not have sufficient capacity to cope with the crisis and needed external help.[11] Members of the Uzbek diaspora used Russian media channels to make their appeal for intervention public. On June 12th President Otunbayeva appealed to Russian President Dmitry Medvedev for a peacekeeping deployment and on June 14th to the Collective Security Treaty Organization (CSTO). Both appeals were declined. Nonetheless, by June 15th violence subsided, and Kyrgyz security forces gradually got the situation under control.

Mobile Technology in the June 2010 Conflict

A common view in Kyrgyzstan is that mobile technology worsened the situation in the June clashes. This is because oral transmission of information through cell phones is susceptible to distortion and can be easily put to negative use.

First, cell phones allow for rapid mobilization. Typically, when tensions escalate in Kyrgyzstan, two groups are called up on mobile phones to assemble at a scene and take action: "sportsmen" (young thugs affiliated with political and criminal leaders) and "special purpose female units" known by the acronym OBON (middle-aged women whose tactics include abuse and physical assault).[12] Apparently, the phone calls are organized on a network marketing principle, which enables them to reach many people whose numbers are stored in advance. This system was instrumental in mobilizing groups for fighting in June 2010.

Second, cell phones can be used to spread negative propaganda as conflict gestates. When tensions were brewing in the run-up to the June clashes, video clips were spread through cell phones, depicting scenes of interethnic abuse, humiliation, and assault. Although the authenticity of these images could not be verified and it was often unclear to which side the perpetrators belonged, the mostly young audience took them as fact, proving "their" aggression against "us."

Third, cell phones are used to convey threats in the aftermath of conflict. Ethnic Uzbek refugees who fled to Uzbekistan after the clashes received messages from Kyrgyzstan with threats that, if they did not return immediately, their land and houses would be taken away from them and the elderly would lose state pensions and other benefits. Messages were not signed, but it was believed that the state was behind them.[13]

An investigation by the Kyrgyzstan Inquiry Commission revealed that the belief that cell phones played a crucial role in mobilizing people to fight in Osh is only partially correct. This is valid for urban areas and district centers, but most villages are outside of cell phone network coverage. For example, in the Alay district, from which large numbers of rural Kyrgyz advanced toward Osh on June 11th, only the capital Gulcha has cell phone reception.[14] The head of the Alay district learned about fighting in Osh only at 8am on June 11th (the action started at 10.30pm the previous night), when

[10] Personal interview with Omurbek Tekebayev, a member and former speaker of the Kyrgyz Parliament, Bishkek, November 2010.

[11] Anna Matveeva, "Violence in Kyrgyzstan, Vacuum in the Region: The Case for Russia-EU joint Crisis Management," Working Paper 02.11, Civil Society & Human Security Research Unit, London School of Economics, December 2011.

[12] In Russian, OBON stands for "Отряд баб особого назначения," or "special purpose female units," and is analogous to the acronym OMON, used for special purpose police units.

[13] Personal interview with investigators from Uzbekistan's Prosecutor General's Office, Tashkent, November 2010.

[14] The author visited nearby villages from where men assembled and can confirm the absence of reception.

he arrived at work from his village. He discovered that hundreds of Alay men already amassed in the Osh suburbs and were preparing to storm the city. A similar picture was reported in the Kara-Kulja and Chon-Alay districts. Apparently, men were mobilized either using landline phones or when people drove from village to village and raised the alarm.

What can be said with certainty is that cell phones played a role in filling an information vacuum in urban areas. The scarce, late, or distorted coverage of the June events by the national media during the clashes created a dangerous void. Initially, migrants from Kyrgyzstan in Russia heard about the outbreak of violence on the Russian news and started to call their families. Then Otunbayeva appealed to the public on television to resist provocations. Officials gave understated accounts of casualties and of how the security situation was developing. Bakhtiyor Fattakhov, an ethnic Uzbek government official called on by the provisional government, tried but failed to address the Uzbek community through Osh TV.[15] The central television station NKTR was handicapped, as its Uzbek operator was beaten up while shooting street footage. A crowd of 500 Kyrgyz besieged the NKTR building, but its director managed to defuse the situation. As riots spread, Russian and Western media produced coverage, while Kyrgyz state channels aired animated films, readings of the Kyrgyz epic Manas, and the soccer World Cup.[16] Rumors of atrocities proliferated, became accepted as fact, and motivated people to take up arms.

Text messages and cell phone calls from friends and relatives filled the void. Witnesses saw elderly women fleeing in panic while listening to their mobile phones. When the violence started, the Kyrgyz relied even more on mobile phones, because Kyrgyz-majority neighborhoods are widely dispersed around Osh, making it more dangerous to move across the city. Low-technology warning signals played an even bigger role. Uzbek men drove around in cars in the Uzbek-majority areas, calling upon *mahallas* to prepare for resistance; they used calls from mosques to alert the communities to danger and banged on pipes to wake residents during the night.

ICT Now: State of the Art, Popular Resources, and Their Consumers

WHO USES WHAT

Kyrgyzstan's population was estimated at 5.5 million in 2011,[17] of which about 1 million are thought to migrate to Russia for work. In 2010, by the time of the crises, Kyrgyzstan had 482,000 fixed telephone lines (60 percent penetration).[18] By the end of 2011, Internet penetration constituted 39 percent.[19] Internet cafes and dial-up Internet access are available countrywide, mainly in urban areas. The most dynamically growing market segment in Kyrgyzstan is mobile telecommunications. Data from the Ministry of Transport and Communication shows that mobile subscribers numbered 4.9 million by the end of 2010 and that investment in ICT rose by 54 percent relative to 2009.[20] Kyrgyzstan is home to six mobile operators. More than 1 million users access the Internet with mobile communication through basic smartphones.[21] However, not all of them realize that they are Internet users.[22] "The State of Broadband 2012: Achieving Digital Inclusion For All" reports that 20 percent of the population used the Internet and 4 per 100 inhabitants were active mobile-broadband subscribers in 2011.[23]

The reality is more complicated. Internet speed varies greatly, affecting quality and coverage

[15] Personal interview with Bakhtiyor Fattakhov, head of State Agency on Local Self-Government, Bishkek, November 2010.

[16] Personal interviews with KIC and author's personal observation.

[17] See www.worldbank.org/en/country/kyrgyzrepublic .

[18] Bolot Bazarbaev, "Information and Communications Technology Development in Kyrgyzstan: Rise of the Machines," Presentation at the University of Washington, August 22, 2010, available at: www.slideshare.net/bolot/ict-development-in-kyrgyzstan-presentation-for-university-of-washington .

[19] Internet World Stats, "Internet Users in Asia," December 31, 2011, available at: www.Internetworldstats.com/stats3.htm .

[20] "Mobile Subscribers Top 4.9 Million, MoTC Says (Kyrgyzstan)," *International Telecommunication Union*, February 8, 2011, available at www.itu.int/ITU-D/ict/newslog/Mobile+Subscribers+Top+49+Million+MoTC+Says+Kyrgyzstan.aspx .

[21] Alexander Wolters, "The Changing Media Landscape in Kyrgyzstan and Central Asia," French National Audiovisual Institute, March 29, 2011, www.inaglobal.fr/en/ideas/article/changing-media-landscape-kyrgyzstan-and-central-asia .

[22] Phone interview with Bektour Iskender, The Kloop Media Foundation, Bishkek, September 2012.

[23] International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization, "The State Of Broadband 2012: Achieving Digital Inclusion For All" A Report by the Broadband Commission, September 2012, available at www.broadbandcommission.org/Documents/bb-annualreport2012.pdf .

nationwide, and the web is barely accessible in some regions. Kyrgyzstan is a mountainous country with a harsh continental climate. Electricity problems are endemic, as this energy source is often used for heating because of a scarcity of gas and coal. While the country has vast hydropower potential, this alternative energy source suffers from underinvestment. As cold weather settles in, the electricity supply becomes unreliable; power cuts are frequent due to the decaying infrastructure, and the electricity current is too weak to hold a continuous Internet connection. Jumps in the current upset the modems and make computers crash—a routine predicament in offices during the winter. Field observation in Osh province showed that computers distributed by UNDP's Preventive Development program to the civil society organizations they helped establish are underused because of electricity problems and the absence of spare parts.[24]

The high number of mobile subscribers, which appears to exceed the population size, can be explained by the fact that many people have more than one subscription due to the unreliability of Internet providers and uneven coverage. Mobile technology is generally cheaper, quicker, more widespread, and more reliable than fixed-line Internet connections. In January 2012 the Kyrgyzstan operator Megacom launched its first 3G network in the capital Bishkek, which will expand to the rest of the country. While only young people—mostly in cities—use text messaging, men are more likely to use mobile technology extensively. Older women, especially in rural areas, only answer mobile calls and typically resist attempts to be trained to do anything more. The Internet is largely an urban phenomenon.

Things are still changing with regard to Internet and cell phone usage. One indication of this was the Kloop foundation's online coverage of an earthquake in the remote Batken province in July 2012, which generated comments from the affected areas in the middle of the night.[25] It is possible that the Internet will become more universally accessible in future, but since de-modernization processes are also underway in Kyrgyzstan, the direction of change is hard to predict.

The main political online news agencies are the semi-official AKIpress and the privately owned 24.kg, which does not interact with readers online. AKIpress runs a *Reader Opinions* weblog, but comments are few and exchanges absent.[26] Serious political debate unfolds in person among several thousand people, many of whom know each other, as the audience for critical reflection is small: "We are a tiny country and what's happening here is a puppet theater," said one interviewee. On- and offline debates are affected by geography, as "the south is a different country where different rules apply."[27]

The most influential site for political debate is Russia's www.ferghana.ru. This news agency is privately owned by a Russian from Uzbekistan. It publishes its own analysis and commentary, and maintains a blog where information that appears credible, but cannot be verified, is placed. Kyrgyzstan's most prominent interactive resource for political issues is *Belyi Parus* (White Sail), which produces its own content and re-publishes news and analysis from other sources. It is privately owned by an ethnic German businessman from Uzbekistan. It is under attack from Kyrgyz nationalists, as it is run by an ethnic Russian female editor. It is read mostly in the cities of Bishkek and Osh, and by people from Kyrgyzstan living abroad. In the words of its editor, "We are influential among a thousand people."[28] The donor-sponsored Kloop Media Foundation provides coverage in Russian, Kyrgyz, and Uzbek, the latter being the least widely spoken of the three in present-day Kyrgyzstan.[29]

Kyrgyzstani NGOs and journalists believe that blogging and Twitter played an unprecedented role

[24] UNDP's Preventative Development Program has since been renamed the Peace and Development Program.

[25] Interview with Iskender.

[26] See http://akipress.org/comments/ .

[27] Phone interview with website editor, September 2012.

[28] The editor regularly receives virtual threats, e.g., "we will throw you down a balcony of a ten-floor block," phone interview with Elena Avdeeva, editor of *Belyi Parus*, September 2012. She does not take the threats seriously.

[29] Humanistisch Instituut voor Ontwikkelingssamenwerking (HIVOS) is one of the donors. Its website says that "The Kloop Foundation was founded by two former journalism students in the autumn of 2006 to carry out this youth website project. Kloop wants to focus on digital media projects in Kyrgyzstan. Kloop Media is a young organisation strongly connected with the Children's Media Centre (CMC). This former partner of Press Now has been working in the field of youth journalism since 1999. The Kloop office is housed in the capital Bishkek. Kloop's mission is to raise awareness of young people in social, political, and economical processes occurring in the Kyrgyz Republic." Internet archive of Kloop Media Foundation can available at http://archive.is/6eEv .

in the run-up to the April power change.[30] As Alexander Wolters put it,

> The first news about the protests did indeed appear on Twitter, followed by short videos that were posted on YouTube and later reposted on regionally based video websites. One could follow the events live on Twitter, where hashtags like #freekg and #newskg organized the flow of information for "followers." Professional news services like Russian RT quickly stepped in and used the online material for coverage of the events.[31]

Bektour Iskender, *Kloop* editor and blogger, and the author believe that the role of social media in the April power change has been exaggerated. The protesters and the online community were two different groups. The young men who rallied in the streets of Talas and Bishkek did not do so because of Internet postings. Rather, it was witnesses like journalists, students, and NGO representatives posting their impressions in real time on the web who created the effect of a general politicization.

DATA CREDIBILITY AND DATA MANIPULATION

The main flow of information in Kyrgyzstan unfolds offline, through social networks. Kyrgyzstan is a heavily networked society because both kinship and neighborhood ties are strong. Information is passed orally through networks of family, friends, neighbors, and business associates, a pattern that reflects the country's social fabric. Many more readily trust such information, which supposedly comes from insiders with "knowledge" and is considered more credible in the local context than official sources—a tradition that originates from the Soviet era when state sources were distrusted. Rumors constitute an important source of information. A prominent feature of new ICTs is that they more rapidly promote rumors in a society where people are inclined to trust rumors anyhow. Thus, ICTs need to be considered not in isolation but in how they relate to conventional, face-to-face social interaction: they magnify the messages already in public domain.

Mobile phones contributed to the proliferation of rumors in the aftermath of the June 2010 conflict and at turbulent political points—e.g., parliamentary (2010) and presidential (2011) elections. Rumors play a bigger role on the periphery, as sources of information are more limited than in the capital and it is harder to verify the facts. Sometimes respected online media respond to rumors to dispel them. However, editors are hesitant went it comes to "low-life" gossip.

The June conflict situation was illustrative in terms of how information can influence communal behavior. The Internet played a significant role as information from the central media was not trusted in the south. The *Ferghana* website became a major source of early warning. People from both communities read its updates and spread messages through mobile phones on crowd movements and on which neighborhoods were under attack. This was how many Uzbeks organized defenses and evacuations—by following what *Ferghana* reported. Users were posting comments on the website in real time, providing signals of the developing trouble that they were witnessing or hearing about. Such comments served as signals for journalists to investigate, and if the information was credible, it went on the site straight away as an early warning. As a result, the website became a concern for the authorities, as they realized the influence virtual information could have on behavior in real life. A ban on the website was contemplated several times.[32]

Some also spread disinformation in an attempt to prevent conflict. The editor of *Belyi Parus* used her influence when she published the "news" during the most acute fighting in Osh that Russian paratroopers were on their way from a base in central Russia and would descend on Osh soon, in full knowledge that this "news" had no factual basis to it. This was meant to scare the Kyrgyz mobs into retreat.[33] There were similar news items published by Russia's information agencies at the time. People looked into the dark sky at night in Osh and "saw" *spetsnaz* troops parachuting into the city.[34]

[30] Interview with Avdeeva.
[31] Alexander Wolters, "The Changing Media Landscape in Kyrgyzstan and Central Asia."
[32] Interview with Kislov.
[33] Interview with Avdeeva.
[34] Phone interviews with respondents in Osh, June 12, 2010.

NEGATIVE ONLINE USE

As a society is politicized, there is a general sense that "it is easier to use ICT for negative mobilization than for positive action."[35] It was noted that social media is often exploited by aggressively minded people who work to escalate tensions, while a peacebuilding constituency may not be active.[36] Discussing the situation today, an NGO leader expressed the following: "The Internet lives and breathes hatred. Perhaps those who write these nationalist messages are unlikely to take to the streets to freeze in cold winds and risk being beaten by police. However, such outpour[ing]s of hate speech are not normal and cannot be good. I don't know where this [will] lead."[37]

The author's monitoring of the online debate on *Belyi Parus* (August 10–September 10, 2012) revealed that by far the most discussed topic was that of identity—interpretations of the historical events of 1916, when a Kyrgyz revolt was suppressed by the Russian army. Other popular topics, in diminishing order, were Kyrgyz and Russian language use in parliament, the viability of Kyrgyzstan's statehood, citizenship without the registration of ethnicity in passports, Russian politics and relations between Russia and Kyrgyzstan, Western reactions to the conviction of Pussy Riot, and the formation of the new government.[38]

Diesel is the biggest online forum (http://diesel.elcat.kg) in Kyrgyzstan. It republishes information from other sources and runs sections on all aspects of life, from selling shoes to online dating to military bases. It has a "politics and society" section, which is moderated and seeks to maintain the standards of "civilized debate." Detailed rules for online behavior are available for the forum's participants. Extracts from the rules read as follows:

> Calls for illegal actions are prohibited. Examples: remarks demanding the Kyrgyz Republic to join Kazakhstan, Russia, Uzbekistan, USA, or any other foreign country; calls for military coups, wars, pogroms, recruitment into prohibited religious and social organizations (movements and parties) etc.
>
> Criminal and administrative codes are valid at the forum exactly the same way as they are valid in real life. In certain cases—i.e., when law-enforcement and judicial bodies open criminal or administrative prosecutions—disclosure of the user's personal details can be made.

The rules were apparently inefficient to instill standards of debate. Discussion on ethnic feelings (Kyrgyz versus minorities) and language proved the most popular theme and demonstrated high levels of intolerance and interethnic abuse, while numerous comments were banned by the Diesel moderator. The latest rule bans any discussion of ethnic, language, or other identity issues, because "the discussion only results in insults, abuse and expressions of intolerance from all parties."

> In other words, nothing should be said about race, ethnicity, and language. The meaning of the ban is not to discuss [these issues] in polite terms, but precisely not to say anything at all.
>
> *Signed Very Angry Administrator*[39]

Interviewed editors and journalists expressed the view that serious interest in social and political affairs and commitment to the values of multiethnic society, political freedoms, and aboveboard politics are stronger among the older generation than among young people. There is also a perception that many politicians and journalists are more motivated by financial considerations than by bigger, societal causes. Thus, although the new ICTs are predominantly the domain of the young, there is a concern that they may not put them to constructive use. "Yes, use of ICTs is growing, but it is unclear what for."[40]

The Internet, like print media, is used for crude lobbying. Political actors and business and ethnic lobby groups offer to pay editors to get their content published. The prices start from $300 for a short article. One agency reporting the phenomenon said that sometimes they notice the content previously

[35] This was the common sentiment expressed by the individuals interviewed for this research project.

[36] Personal nterview with Andrei Khanzhin, adviser at the OSCE High Commissioner on National Minorities (HCNM), The Hague, September 2012.

[37] Interview with Kadyrova.

[38] See www.paruskg.info .

[39] See http://diesel.elcat.kg/index.php?act=announce&f=76&id=86 .

[40] Interview with Iskender.

offered to them then being published by others and assume that they took the money.

THE POWER OF IMAGES

Videos often generate a bigger emotional resonance than written entries. Videos posted on YouTube during and after the June events were trusted as fact and made people react to the "opponent" group with anger and sometimes physical violence. Later investigation revealed that not all of these videos were authentic. The Kyrgyzstan Inquiry Commission (KIC) amassed a collection of video footage, handed over as "unique" and "confidential" evidence by sources from both ethnic communities in Kyrgyzstan and witnesses who fled to Russia and Kazakhstan. However, a large proportion of this "evidence" had already been seen by the KIC experts on YouTube.

Random sampling and examination of "evidence" by international forensic experts revealed that at least 50 percent was definitely not authentic. There were few examples of tampering with the actual filming, but it emerged that much footage of fighting and atrocities was shot in previous years—when Kyrgyzstan was peaceful—leading to the conclusion that these scenes came from conflicts elsewhere. In several cases the same video footage was brought to KIC by representatives of both sides, claiming evidence of violence by "them" against "us." A dramatic example was footage of two young men being set on fire and burned alive amid a cheering crowd.

Videos of the June conflict were uploaded on the Internet by diaspora Uzbeks, and some people watched them through anonymizers—i.e., proxy servers. Interpretations of the videos, with various exaggerations, were circulated by word of mouth, absorbed back into society, and created a swell from the Internet back to the people. Intercommunal tensions got worse and confrontations started on the streets.[41]

International media is perceived by the Kyrgyz majority as biased against them and siding up with the Uzbeks. International coverage, even if not related to the interethnic conflict, continues to be interpreted from this perspective. For example, a short video of police harassment was aired on the BBC, showing Kyrgyz-looking policemen stopping cars and beating and extorting bribes from Uzbek-looking drivers. This created a big outcry against the BBC and Westerners among the Kyrgyz majority.[42]

It is hard to predict which clip uploaded on YouTube will generate a public reaction, but there have been powerful reactions, and they have been difficult to control. The recent hot issue was videos showing "patriotic" Kyrgyz men punishing young Kyrgyz women in Russia for going out with non-Kyrgyz men, some quite violent. Online and media discussion revealed shock and horror among parts of society, and enthusiastic support from a puritan constituency. The resonance was such that Kyrgyzstan's parliamentary delegation went to Moscow to try to find a solution.

Still, there are signs that videos on the Internet are making a positive impact on public issues. A video shot in Kara-Suu district of Osh province showing a school headmistress beating a student was posted on the Internet and led to an investigation and the eventual sacking of the headmistress. Police harassment of foreign tourists posted on the web led to investigation into the officers' wrongdoing. Police posted their own video of the arrest of a corrupt ex-cop on the Bee Line network.

Actors Using ICT for Conflict Prevention

MIGRANTS AND DIASPORAS

By creating virtual communities across borders, over which governments have little control, ICTs introduce new possibilities for interaction with actors based abroad. Social media plays a pivotal role in connecting labor migrants in Russia with friends and family in Kyrgyzstan. The most popular are the Russian sites V Kontakte (In Contact), Odnoklassniki (Classmates), and Moi Mir (My World). These are used less for political debate than for social networking, self-promotion, and lifestyle. There is also Russia's mobile chat facility mail.ru.agent, which is used by young people to send messages to groups of subscribers.[43] Facebook

[41] Skype interview with Kimairis Leah Toogood-Luehrs, Senior Peacebuilding Trainer and Facilitator at International Alert, Bishkek, September 2012.

[42] Interview with Toogood-Luehrs.

[43] Its site says that "Mobile Agent is a free application to communicate with friends and family. Communicate at the same time in the Agent, ICQ, Odnoklassniki, VKontakte and other services. Use Mail Mail.Ru: receive and write letters, send attachments. Send free SMS. Share your impressions in microblogs. Upload photos, videos and other files. Use geo maps, traffic jams, routes," available at: http://agent.mail.ru/mobile .

is more often used for sociopolitical issues, albeit mostly by users outside the former Soviet countries. It also acts as a proxy for accessing content from websites banned in the region, such as *Ferghana*.

The voice of the Uzbek minority is largely absent from public discussion inside the country. Even the donor-supported *Kloop* publication reported that Uzbek journalists do not approach them with their materials, and bloggers do not participate in online debates. Still, the Internet is almost the only information resource available for the "losers" in the interethnic conflict. Exiled Uzbek political leaders use it to present their side of the story to the external world, to demonstrate to their supporters in Kyrgyzstan that they have not given up on the cause, and to appeal to the international community. Video statements on YouTube by the main protagonist Kadyrjan Batyrov, now exiled in Sweden, were the most embarrassing for the government in Bishkek, as they claimed a different version of interaction between Uzbek politicians and the provisional government. The authorities were powerless to act: Batyrov remained in Europe while his statements continued to appear.

Uzbek diaspora groups with a public face include the Alisher Navoi Institute[44] and Osh Initiative run by Uzbeks in Uzbekistan, the West, and Russia. These groups serve as a bastion of hope for the Uzbek minority, for whom this is one of the few sources of alternative information and support for their aspirations. The groups' sites are suppressed in Kyrgyzstan, and they have to rely on Facebook and online news agencies in Russia to publish their content. *Ferghana* occasionally takes their material because it views them as a distant voice but potential participant in conflict negotiations in future.[45]

Diaspora activity is a big irritant for the Kyrgyz majority and the government. Two books *Философия жестокости. Час шакала* (Philosophy of Atrocity) and *Философия жестокости. Геноцид продолжается… Шакалы еще не ушли* (Jackal's Hour and Genocide Continues. Jackals Have Not Yet Left) by diaspora Uzbeks present a developed victimization narrative. They were released in April 2011, and featured photos and videos of atrocities downloaded from the Internet without buying the copyright. The books and accompanying CDs were produced in Finland. Some copies found their way into Kyrgyzstan, where the publication was quickly banned and a criminal investigation opened.[46] Kyrgyz community activists organized public burnings of the books.

GOVERNMENT: AWARE AND ACTIVE

The authorities are well aware of the destructive potential of ICTs and take a range of measures to control the field, such as banning websites. Successive Kyrgyzstan governments felt that *Ferghana* worked against them and promoted the "wrong version" of the key political events. The site was banned by ex-President Bakiyev, as it published critical information on his family's affiliation with corrupt businessmen and on unrest in Naryn in March 2010. After the "second revolution" the ban on the site was lifted, but it was imposed again on June 16, 2011 by the Kyrgyz parliament for publishing "subjective information" on the June 2010 clashes.[47] The agency started a court action against the ban. *Kloop* had been harassed under Bakiyev when the agency launched a journalistic investigation into privatization of Kyrgyz Telecom in favor of the president's favorite son, Maxim. The editors were summoned to the State Committee on National Security and advised to steer clear of the presidential family. *Belyi Parus* was banned under Bakiyev but unblocked as the April power change got underway and while there was still fighting in the streets.

The lesson the government learned from the June events was that when tensions break out, the first action should be to block cell phone communication. Officials switch off their phones so as not to be asked questions by the public and the press, and so as not to be held responsible for giving away information without permission from their seniors. The regional neighbors do the same—for example, Tajikistan's government blocked the cell phone connection for weeks during security escalations in

[44] See http://alishernavoi.net .

[45] Interview with Kislov.

[46] "Книги «Час шакала-1, 2» признаны в Кыргызстане вне закона; возбуждено уголовное дело – генпрокуратура," *KyrTAG Newagency*, Bishkek, April 21, 2011, available at www.kyrtag.kg/?q=ru/news/5565 .

[47] Abdulfazal, "Ferghana.ru's website has been banned in Kyrgyzstan," *New Eurasia*, June 17, 2011, available at www.neweurasia.net/media-and-Internet/kyrgyz-parliament-bans-ferganaru .

Gharm (2011) and Badakhshan (2012). In Kazakhstan an ethnic Uzbek activist was arrested for inciting ethnic hatred after posting a video of the Osh events on the Internet.[48]

The government also fears the propagation of religious extremism and terrorism when young people get radicalized through the Internet. It bans websites suspected of Islamist propaganda. The state has a legitimate concern since the country hosts a US military base at Manas airport and has been a target of jihadists from the Islamic Movement of Uzbekistan in the past. Liberal media and the international community, critical of the government in other areas, sympathize with its anti-extremist agenda. One website editor admitted publishing apparently state-planted but good quality content prepared by what is believed to be the security services of Kyrgyzstan and other countries acting in disguise. The editor saw the fight against radicalism and narcotics as legitimate.

ICT is proactively used by the State Committee on National Security and law-enforcement agencies to eavesdrop on conversations of anybody of interest—for example, rival politicians and business leaders using their mobile phones and wi-fi routers as reception devices. Politicians routinely take batteries out of their phones and disconnect the Internet when having confidential meetings.[49] Intercepted conversations on plotting a coup, conspiring to embezzle state funds, and selling jobs have been published on the Internet and featured prominent politicians, including the current president Almazbek Atambayev.[50] Equipment is now available capable of blocking such interceptions and was reportedly used by the US in their meeting with Uzbek journalists in Osh in June 2010.[51]

State secret services penetrate online discussions by registering under various aliases. There is a persistent perception among "liberals" in the online community that security agents seek to shape the debate. Examples were given where information available only to the government appeared in online discussions. One blogger remarked, "I feel that half of the time I correspond with an agent. It is distracting a lot of the time. But I cannot ignore such commentators because the convention is that a blogger has to answer comments." At the same time, the *Belyi Parus* editor reported that even during the Bakiyev period she turned to the State Committee on National Security for help to track a user who was bombarding the site with nationalist propaganda under different aliases. The *Kloop* editor noted that the State Committee on National Security approaches them offering their well-produced video material.

There was one proven case of ICT use for conflict prevention by state officials in 2010. In May, after the first escalation in Jalalabad, the surrounding areas were full of rumors of exaggerated casualties and non-existent political claims. Prompted by the Foundation for Tolerance International, a Kyrgyzstani NGO, the deputy minister of interior requested that the main mobile operator in Jalalabad province distribute official data signed by the ministry on the true state of affairs to all of its subscribers. The information was sent out, but as monitoring was not conducted, it is not known if this measure achieved its aim. Recently, the Ministry of Youth Affairs approached UN Women for help in developing an interactive website to engage with a young audience.[52]

In the aftermath of the conflict, the government apparently became more open to the use of ICTs for prevention, as it expressed more interest in international expertise in dealing with conflict.[53]

INTERNATIONAL COMMUNITY

The main early-warning systems active for at least a decade in Kyrgyzstan are those affiliated with the Organization for Security and Co-operation in Europe (OSCE), United Nations Development Programme (UNDP), and Foundation for Tolerance International (FTI). Given that the two regime changes and the outbreak of ethnic conflict took the international community by total surprise, these early-warning systems appear to have been

[48] According to an interview with Igor Savin, KIC expert, Osh, November 2010, in person.

[49] Witnessed by the author during interviews with officials conducted for the KIC. For example, for the meeting with Jalalabad governor in a hotel suite, everybody took batteries out of their mobile phones, and the handsets and the batteries were separately put into a freezer, Jalalabad, November 2010.

[50] For a detailed story see "Kyrgyzstan: A Hollow Regime Collapses," Asia Briefing No. 102, Bishkek/ Brussels: International Crisis Group, Apr 27, 2010.

[51] KIC interview with Maksuda Aitieva, head of Osh Media Resource Center, Osh, October 2010.

[52] Skype interview with Sabine Mahl, UN Women representative in Kyrgyzstan, Bishkek, September 2012.

[53] Phone interview with Ainura Umetalieva, former UNDP program manager, Bishkek, September 2012.

fairly ineffective. Rather, they played a role as local information and analysis systems in support of international development policies.

The OSCE high commissioner on national minorities has conflict prevention as part of his mandate. In 1993, an early-warning system was established in southern Kyrgyzstan as it had been the scene of clashes in 1990. The function of the system is to inform the high commissioner about developing conflicts, so that he can respond. Initially covering interethnic relations, it has since expanded to religious issues. The early-warning system is based on qualitative methods: quarterly reports are compiled by field monitors, synthesized into a single narrative by an analyst in Kyrgyzstan, and processed by the high commissioner's office in The Hague.

The OSCE system does not rely much on technology, other than email. ICT is mostly used in "spot reports" on potential escalations. The information should first appear on mainstream news agencies' websites for The Hague office, which has better Internet access, to have it checked. The adviser at the high commissioner's office gets the information and feeds it back to the local monitors in Kyrgyzstan. If deemed relevant, the adviser asks a field monitor or a team of mediators to travel to the site to investigate.

Experience suggests that the system works well in peacetime to identify evolving trends but is inefficient in a conflict situation. The view is that "the early warning project is long term, maybe medium term, but it is too slow to be able to prevent conflict in real time if a situation escalates."[54] During the 2010 conflict, the high commissioner's office issued an "Early Warning to the Permanent Council" on June 14th, when violence was drying out and most of the killings had already taken place.[55] In the run-up to and during the conflict, the high commissioner's voice was not heard in Kyrgyzstan and no warnings were available for the affected communities. After the outbreak of violence, the OSCE office in Bishkek issued daily situation reports summarizing the previous day's developments, which were distributed among the international players. After five days the practice stopped, as the responsible officer went on holiday.[56]

Since the early 2000s, UNDP had run its own early-warning system within its Preventive Development Program. At first this was based on population surveys and then on qualitative data collected by UNDP staff and partners in the field. After the 2005 "revolution," however, the early-warning system was outsourced to FTI, which by then had its own system. FTI's early-warning system after the "revolution" was funded by UNDP, the OSCE, and the Swiss Development Cooperation Office, but the donors could only offer short-term funding, and FTI had to look for alternative donors. Depending on the available funding, the system was expanding or shrinking, losing analysts and technical capacities when cash was tight. In early 2010, prior to the April and June events, FTI finally ran out of funds and the early-warning system had to close. Thus, the UN had no functioning system in the run-up to the crises, although a national representative of the UN Regional Centre for Preventive Diplomacy compiled reports for the center's headquarters in Ashgabat.

Case Study: Making a Leopard Change Its Spots

In 2011 UNDP and UN Women funded the FTI to revive the early-warning system in southern Kyrgyzstan. The new project differed from the previous system at FTI, which used to rely on a network of its own monitors in each problem area. This time, FTI acted in partnership with the Women's Peacemaking Network (WPN), which involved women activists throughout the south who were to collect data for FTI to prepare the early-warning reports.

The new system attempted to make use of mobile technology. The design was that the WPN activists report on escalating tensions in real time by text messaging FTI in Bishkek, which would in turn compile the information and produce analysis. This was also meant as a cost-cutting option. However,

[54] Personal interview with an adviser at the OSCE HCNM Office, The Hague, September 2012.

[55] Statement by Knut Vollebaek, OSCE High Commissioner on National Minorities, "Early Warning to the (Special) Permanent Council on 14 June 2010," Vienna, June 2010, available at www.osce.org/hcnm/68539 .

[56] Personal experience when working as a political analyst at the OSCE Referendum Observation Mission, Bishkek, June 2010.

the design did not work. Rural women, most of them elderly and semi-literate, could not use text messaging and were unwilling to be trained. They could call FTI to report events, such as the outbreak of fighting or a protest rally, but they were capable only of conveying facts as they witnessed them, not of analysis. The information submitted still needed to be verified. FTI had to send their own staff from its Osh or Bishkek offices to investigate on site, which was a slower and a more expensive option than to maintain local analysts as they had previously.

In a related initiative, FTI tried to use mobile technology to combat rumors, but this did not work for similar reasons. The US embassy sponsored training on ICT use. A trained FTI moderator was to circulate reliable information by text messaging the women—community leaders in conflict hot spots—for them to act quickly to dispel rumors. FTI had been compiling information from reliable, mostly state sources in a user-friendly format for this purpose. However, it emerged that most community leaders did not know how to use the short message service (SMS). Some of those who did manage to read the messages did not know how to reply to confirm receipt. Text messaging is a surer way to prevent data manipulation, as the written word can serve as more reliable evidence than the spoken word, but the age and education levels of the recipients worked against the initiative. They preferred to have conversations over cell phones, but this introduced the risk that the community leaders would misinterpret or deliberately distort information and spread it as reliable, because it came from a trusted NGO source. Young people are more technologically savvy, but using them to dispel rumors would not work because they have no authority in their communities.[57]

UNDP also invested in ICT use for the prevention of election-related violence. It supported a mobile-technology project during the 2011 presidential election by a network of NGOs led by Civil Initiative Internet. This project sought to dispel various provocative rumors that proliferated at the time by providing official information, but the number of users reporting violations of the Electoral Code of Conduct was not high. In practice, many text messages were voting-related inquiries.[58] The experiment raised two questions: If user identity could not be verified and the information could have been planted for electoral manipulation, how reliable could this method be? And if messages needed to be filtered before going on the website, how timely and relevant could it be? The second and more successful attempt occurred during local government elections in 2012, when the circle of users was confined to partner NGOs. This time, information collected through mobile technologies raised the interest of the prosecutor general and the Ministry of Interior.[59] Questions of verification and the use of the UNDP logo (how should such a platform be labeled, and would a disclaimer be sufficient for distancing if needed?) would have to be addressed in future planning.

Another UNDP project that used ICT for conflict prevention involved police training on how to develop a community liaison platform and how to interact with the public using modern technologies. The idea was that people could address messages to the police online, allowing it to react quickly to an escalation of conflict.

In 2011 the United States Agency for International Development's (USAID) Office of Transition Initiatives, the European Commission, and the UN Refugee Agency (UNHCR) sponsored the Agency for Technical Cooperation and Development (ACTED) to develop an online interactive map to identify socioeconomic issues and potential points of conflict in the Ferghana Valley, which crosses Uzbekistan, Kyrgyzstan, and Tajikistan (http://reach-initiative.kg). USAID's website states that "in the four months since it released the map, ACTED estimates that it has helped mobilize more than $10 million in donor funds into more effective programming."[60] According to this, the map's impact is in acting as a fundraising mechanism.

Empirical investigation brought the following

[57] Interview with Kadyrova.

[58] Interview with Umetalieva.

[59] Joerg Stahlhut, UNDP Peace and Development Adviser, Kyrgyzstan, January 2013.

[60] See "USAID/OTI Kyrgystan Quarterly Report: January–March 2012," USAID Office of Transition Initiatives, available at http://transition.usaid.gov/our_work/cross-cutting_programs/transition_initiatives/country/kyrgyzstan/rpt0312.html .

insights. The author could not make the map work.[61] If the site in English does not work, it is hard to see how the donors use it.[62] The site in Russian does work, although it is not complete and is likely to be too complicated for a non-specialist audience (and for the author).[63] It offers data on local economic problems, jobs, and infrastructure in about 120 villages, mostly from public sources. ACTED staff traveled to each municipality to verify and gather additional data. Microlevel assessment of disputes, mostly about water sharing, infrastructure, and public services was done via focus groups with elders, women, and youth.

The data on the map is not unique, as similar assessments were carried out by development practitioners in the past, and some are available on their websites. The distinction is that it is put on the map to "create map awareness and shape the world the audience sees."[64] If the purpose of the tool is information management for the aid and donor community—to make it open, accessible, and visual on the map—then the coverage is not complete. While ICTs do need to be used more effectively for donor coordination in conflict prevention and the ACTED map was meant to do just that, there is little evidence that this is taking place. A thorough donor evaluation is needed to determine its level of success or failure.

Moreover, the village assessments avoid all the causes of conflict that were central to the two power changes and the June 2010 violence, such as the distribution of macroeconomic assets, majority-minority relations, security, justice, and crime. For example, the conflict history of one village in Jalalabad *oblast* talks about poor public services, but does not mention the mobilization of men from that village for fighting in Jalalabad in 2010, where they engaged in mass murder, gang rape, arson and looting, and harassment of vulnerable people in their own village thereafter.[65] The subject of Uzbeks is not mentioned at all, and the map does not appear to include the Uzbek villages where resistance and fighting were the most ferocious.

It would be difficult for ACTED to present any controversial issues on its website and at the same time continue with its rural development operation. As a result, it has to be careful to avoid a real conflict agenda. The logos of USAID, the European Commission, and UNHCR are also on the site, making it more likely that the site would have to avoid anything politically sensitive. It is unclear how the donors envisaged publicizing any conflict-related data on Uzbekistan, if the map was indeed to cover the Ferghana Valley rather than the south of Kyrgyzstan.

ACTED seeks to involve local people in "map awareness," although it is difficult to find evidence of online interaction. The organization does the local government outreach offline, as Internet is barely accessible in the target areas and rural administrators typically do not use it. ACTED accepted that the map is not a tool intended for an immediate conflict-prevention effect.[66]

Another ACTED ICT project involves SMS surveys across southern Kyrgyzstan through random sampling based on proximity to transmission towers. So far, it has brought a high volume of information but not very high quality; it is a "low risk, low reward way to gather baseline information."[67] There are 1,600 respondents per district. It is also termed as early warning. One respondent noted that the initial intention was to gather data rapidly through mobile phones. She expressed a concern that live data on conflict collected in this way and launched into the public domain can potentially do more harm than good. However, in its present shape the system only gathers views on basic socioeconomic indicators, such as performance of public utilities, and appears quite harmless.

Sponsorship of ACTED's map and SMS-based early-warning system may well be an indicator that the international donors are unwilling to seriously challenge the government, but wish to be seen doing "something with an edge" for conflict prevention. This substitutes action on difficult issues with

[61] ACTED has been very helpful, but the author's inquiry addressed to USAID remained unanswered.

[62] The site was not working in October 2012 and in January 2013.

[63] However, it was difficult to make the map work even in London, despite good connection and equipment. The author had to ask ACTED staff in Kyrgyzstan for assistance, who navigated her through every step by Skype.

[64] Skype interview with Evangeline McGlynn, GIS Manager at ACTED, Osh, September 2012.

[65] KIC Report.

[66] Interview with McGlynn.

[67] Ibid.

miniscule measures to deal with microlevel tensions. As the target actors and social groups involved in such microdisputes in villages are not sufficiently ICT-savvy, whether because of age, rural location, or the limited availability of technology, the project may not represent the most efficient use of funds. Perhaps a program on interethnic relations among university students in the south could have accomplished more with less.

To sum up, ICT data in internationally sponsored projects tended not to be relevant when it came to the quality of early warning, and the numbers of people reached using this technology were low. ICT has the potential to contribute to conflict prevention, but it is still in its infancy in this respect. The problem is that the use of ICTs by local actors in relation to conflict is in one place, while international efforts are in another. The ICT projects did not pay sufficient attention to the way ICTs and other communication flows were already playing out in the local context during crises. Furthermore, important lessons about the use of ICT were not learned by donors and implementers; the lack of coordination between the different donor-driven projects exacerbated this situation.

Conclusion

There is no evidence that ICT expedited the response to the June 2010 conflict by the government or the international community. However, mobile phones and interaction on popular websites played a role on the community level in fostering group action toward fight or flight.

Although technology is likely to make gains in contributing to conflict prevention in the future, given the current context in Kyrgyzstan in terms of development and ICT use, expectations have to be adjusted accordingly. ICT is relevant for conflict prevention when it comes to cell phones, but the Internet is less relevant due to fluctuations in electricity services, bad Internet connections, and limited awareness among rural populations. The Internet only reaches the elites and urban youth, so using this tool for prevention is not that relevant for the country as a whole. In general, mobile technology is more prominent in poor countries, and donors could focus their attention on what can be done with SMS and cell phones instead of the Internet. The Internet can be used to target the elites as agents of change—pushing for democracy, advocating for a change of leadership, contributing to the struggle against corruption, and the like. This is important work, but it must be acknowledged as what it is—working with elites to change elites rather than working to reach the masses through ICTs that are alien to them.

The use of ICTs is not universal and can be differentiated in terms of demographics and geography. While planning interventions involving the use of ICTs, detailed attention needs to be paid to the following:

1. Internet and phone coverage: acknowledge physical barriers inside the country, while recognizing that ICTs facilitate interaction with abroad.
2. Online demographics: Who uses ICTs (or not), and how? What is their status or position in society in terms of culture, age, and ethnic group? How are they positioned in relation to the conflict?
3. Types of ICT: Consider the differences between cell phones and the Internet—both have specific uses and user groups, as well as limitations. Videos, if they hit a nerve, are often capable of creating more public resonance than the written word and are accessible to a less literate population.
4. User capacity: How able is the user to apply the available technology and how willing is she or he to learn? This can be estimated from the user's demographic profile described above. Technology has to be adapted to the user level, otherwise people may react negatively to ICTs they do not understand.

The most valuable element of ICTs does not lie in the creation of data but in the way that this technology can make data that is already somewhere in the public domain accessible to a wider audience in real time. Thus, the use of ICT needs to be considered in a broader sense in relation to communication flows. ICT does not function in isolation. It is closely related to face-to-face, conventional social interactions in a heavily networked and small country such as Kyrgyzstan, where distances between people are not that huge. Communication flows play out differently across different groups in a crisis situation. Minority and opposition groups are more likely to rely on information and communication coming from outside the country or to seek external verification of government-distributed information. The existing online fora are used for interaction and for shaping perceptions by a variety of actors simultaneously. These actors include the government, nationalists, the intelligentsia, and business lobbies, who all manipulate data according to their values and interests.

The role and use of ICTs in connecting individuals and groups with people abroad is pivotal if communication flows inside the country are restricted and if the diaspora has the will and means to uphold the flag. Diasporas are known to play a critical role in both conflict perpetuation and in reconciliation. The use of new ICTs is ever more relevant in this respect, since it is more difficult for the diaspora to rely on face-to-face interaction. The international community has not yet recognized actors based abroad as an important group for conflict prevention.

The significance of risk assessments cannot be stressed enough in this context because of a potential for "spoilers" to use ICTs to exacerbate conflict. More attention needs to be paid to the use of ICTs to heighten nationalism and preach ethnic, regional, and religious hatred. Preventing the negative use of ICTs in this manner should be considered an integral part of conflict-mitigation strategies and an important outcome in its own right—for example, by influencing online debate and preventing social media from becoming a harmful force. For this to be effective, online interventions aimed at conflict prevention have to be carried out in the virtual spaces used by the general public—that is, mainstream websites rather than only at donor-funded ones. Working with editors and bloggers of popular online outlets and monitoring potentially destructive ICT use are therefore essential. Technology for blocking out or filtering SMS containing hate content should be made available, and the responsible agencies should know how to use it in an accountable manner.

ICT should not be mistaken for an "early warning" cure, because it is only a means to an end. This paper has demonstrated that ICT-driven early-warning systems in Kyrgyzstan did not work in times of crisis: although plenty of warning existed, neither the government nor the international community took any decisive action. June events showed that if early-warning information goes against the interests and priorities of those who hold power at the state level, it is likely to be ignored. "Early warning is good only if action follows."[68] While an early-warning mantra continues to dominate thinking on conflict prevention, a glaring gap between warning and response persists. ICT is unable to substitute the lack of will that is the main obstacle to bridging the gap between "warners" and "responders." Therefore, expectations have to be adjusted according to the existing capacities at the international community's disposal. There is a need to consider specific requirements, political dynamics, and risks when using ICTs for prevention in situations of escalating conflict.

The donor agenda, and that of the international community, is also a factor shaping the trend described above. Projects that include new ICTs appear more attractive to funders, creating a risk of overstating the role of ICT because of donors' interests. This hype can translate into inefficient use of funding, such as investment in projects that may not be sufficiently targeted, shaped, or relevant for local people affected by conflict. The relevance of a project to the ultimate aim of preventing violence can get lost in the process of project development when there is an apparent necessity to include the use of ICTs, even if such use is artificial. Experimentation is valuable, since it fosters innovation, but it is meaningless without rigorous evaluation and extraction of lessons of what works and what does not.

[68] Interview with Mahl.

New Technologies and Conflict Prevention in Sudan and South Sudan

Helena Puig Larrauri[1]

Introduction

The advent of new technologies is changing the way we learn about events and respond to them. In particular, technologies that focus on collecting, processing, and disseminating information about a conflict have the potential to change the way all actors involved in a conflict learn about and respond to it.[2] These developments raise a critical question for conflict prevention practitioners: how can new information and communications technologies (ICTs) aid international actors, governments, and civil society organizations to strengthen their voice and action, in order to more effectively and directly prevent violent conflict?

This paper explores answers to this question based on experiences involving the use of new technologies in Sudan and South Sudan. Following a brief description of the conflict and development context in Sudan and South Sudan, the paper describes three case studies of projects that use new technologies. The case studies serve to provide an assessment of the use of ICTs for conflict prevention in Sudan and South Sudan and lessons learned from these experiences. Based on this assessment, the paper draws out key recommendations on how the use of technology can further strengthen efforts to prevent violence and conflict, specifically for international actors, governments, and civil society.

Conflict and Development Background[3]

In 1956, Sudan gained independence from the United Kingdom, inheriting the structures and boundaries of the British Colony of Anglo-Egyptian Sudan. Sudan has witnessed armed conflict in some part of its territory for most of its existence. Shortly after independence, the new Khartoum government reneged on promises to southern Sudan to grant it some autonomy through a federal system. This led to the First Sudanese Civil War (1955–1972). During this war, Sudan had two brief periods of democratic rule and two longer periods of military rule imposed by coup d'état. The second of these coup leaders, General Gaafar Nimeiry, negotiated the Addis Ababa Agreement that ended the First Sudanese Civil War.

The government's introduction of Islamic Law in 1983 triggered the Second Sudanese Civil War (1983–2005). In 1986, the newly elected president, Sadiq al-Mahdi, formed a coalition government that attempted to resolve differences by drafting a penal code that provided an alternative to *sharia*. Its failure to do so, and a coup d'etat shortly thereafter in 1989 by military leader Omar al-Bashir, ended attempts at reconciliation.

The Second Civil War ended with the signing of the Comprehensive Peace Agreement (CPA) in Nairobi on January 9, 2005. The agreement granted autonomy to the south for six years and the right to a referendum on secession at the end of this interim period. It also stipulated the division of jobs in the administration between northern and southern officials, that oil revenues should be shared (thought not by what formula), and that the implementation of Islamic law would be decided by the respective assemblies of north and south.

The agreement also contained special protocols on three areas—Abyei, South Kordofan, and Blue Nile—that had been heavily contested during the war and were considered critical to the stability of both north and south. The protocols made a number of provisions for the interim period, including joint governance arrangements between northern and southern officials, a "popular consul-

[1] Helena Puig Larrauri is a freelance peacebuilding practitioner. Her work focuses on the use of technology for conflict transformation. She is currently working on projects in Sudan, Iraq, Libya, Cyprus, Macedonia, and Romania. She blogs at http://letthemtalk.org .

[2] Anne Kahl, Christy McConnell, and William Tsuma, "Crowdsourcing as a Tool in Conflict Prevention," *Conflict Trends*, No. 1 (January 2012): 27.

[3] Development indicators for the newly independent South Sudan have not yet been collected. Some data on Sudan contains information on both north and south; where this is the case, it is clearly stated.

tation" on governance issues to be held in South Kordofan and Blue Nile (both states would remain in north Sudan should there be a secession), and a referendum to be held in the Abyei Area on whether it should remain with the north or with the south should there be a secession.

During the CPA interim period, general elections were held in all of Sudan, between April 11 and 15, 2010. President Omal al-Bashir was re-elected with 68 percent of the vote. Salva Kiir was elected president of southern Sudan with 93 percent of the vote. International election observers, including the European Union and the Carter Center, said the election did not meet international standards, but also made it clear that the results would be recognized by the international community. The CPA interim period culminated in a referendum on secession in southern Sudan, which was held on schedule in January 2011 and declared successful. Thus, the Republic of South Sudan came into existence on July 9, 2011.

Despite the peaceful elections and referendum, there is some debate as to the success of the CPA. In order to attain the consensus needed for it to be signed, the drafters of the CPA deliberately left out a number of key issues of contention between the north and the south. In fact, following the end of the CPA interim period and the secession of South Sudan, three disputes relating to these unresolved issues have emerged. First, conflict in two northern states bordering South Sudan (South Kordofan and Blue Nile) re-started in 2011 due to grievances that remained unaddressed after the CPA interim period. On June 6, 2011, fighting broke out between the Sudan People's Liberation Army–North (SPLA-N) and the Sudanese Armed Forces in South Kordofan. Fighting quickly spread to many parts of the state. In September 2011, fighting spread to Blue Nile State, where then governor Malik Agar (of the Sudan People's Liberation Movement) sided with the SPLA-N in fighting against the Sudanese Armed Forces. Since fighting broke out, no international observers have been allowed into the two states, so information on the conflict remains patchy. The Sudanese Armed Forces have bombed both states extensively, and there are reports of many civilian casualties. The African Union (AU) reported that fighting was escalating in early 2013.[4] Sudan accuses South Sudan of supporting rebels in these two states.

Second, a dispute over the oil-rich Abyei Area (on the border between Sudan and South Sudan) was scheduled to be resolved via a referendum that would allow Abyei Area residents to choose whether to join Sudan or South Sudan. A disagreement over who qualifies as a resident resulted in the cancellation of the referendum, and the status of the area remains unresolved. Over the past decades, the Abyei Area has seen many armed clashes, often between the nomadic Misseriya and the Dinka Ngok. In 2009, fighting erupted in Abyei town and displaced all of its population. Many had returned since then, but on May 19, 2011, fighting re-started in the area. The area continues to be heavily militarized, with military tensions kept at bay by an AU peacekeeping force.

These two border conflicts fall within the third, broader dispute between Sudan and South Sudan, which centers on provisions for oil payments (South Sudan ships its oil via Sudan) and for border demarcation and security. Over the past months, the two states have on several occasions seemed to be on the brink of war. AU-sponsored negotiations in Addis Ababa are ongoing, led by the African Union High-Level Implementation Panel for Sudan and South Sudan (AUHIP). The most significant breakthrough in these negotiations came on Septemer 27, 2012, with the signing of "The Cooperation Agreement" and the "Agreement on Oil and Related Economic Matters." The second of these agreements allowed for the resumption of oil production in mid-October. However, the broader Cooperation Agreement, which deals with security and border arrangements, has yet to be implemented. The settlement of the Abyei Area and the conflict in South Kordofan and Blue Nile continue to be the major sticking points. An AUHIP proposal on the final status of the Abyei Area presented in September was accepted by South Sudan, but rejected by Sudan, whose government claims the proposal reflects only the South Sudanese position. The proposal called for a referendum to be held in Abyei in October 2013. On October 23, 2012, the AUHIP asked for negotiations to be

[4] African Union Peace and Security Council, *Report of the African Union High-Level Implementation Panel for Sudan and South Sudan*, AU Doc. PSC/PR/COMM.1 (CCCLIII), February 13, 2013, p. 3.

extended for a further six weeks. This extension has not resulted in any agreement, as reported by the AUHIP in December 2012.[5] The Sudanese government is now making the Agreement on Oil and Related Economic Matters conditional on full implementation of security arrangements.[6] The two governments have agreed to meet in January in Addis Ababa to resume negotiations.[7]

As well as these ongoing north-south tensions, both countries continue to face serious internal disputes. In Darfur (western Sudan), an ongoing conflict between rebels and the central government has displaced two million people and killed more than 200,000.[8] The conflict has led to the indictment of a number of officials by the International Criminal Court, including the current president, Omar al-Bashir. In July 2011, the Darfur Peace Agreement was signed by the government of Sudan and the Liberation and Justice Movement in Doha. The agreement makes provisions for the establishment of a Darfur Regional Authority to oversee Darfur until a referendum is held to finalize its status. Progress on implementation of this agreement has been slow. In Jonglei State (South Sudan), a dispute between rival tribes has left hundreds of people dead and displaced about 100,000. The conflict, mainly between the Murle and Lou Nuer tribes, was most intense in 2011, and has since been limited to smaller cattle raids and clashes. Finally, the widespread availability of arms in both countries, together with years of political manipulation of tribal alliances, has resulted in a volatile environment in many areas, especially where nomadic and sedentary tribes coexist. Armed clashes between tribes—whether over the use of resources or to settle past grievances—are not uncommon.

The north-south wars, ongoing internal conflicts, and widespread insecurity have left a legacy of underdevelopment and unequal distribution of resources in both countries. In 2012, gross domestic product (GDP) per capita for Sudan was $1,500, and UNDP reports it has one of the highest growth rates among sub-Saharan African countries.[9] Although agriculture continues to be the sector employing most of the labor force, the development of this sector has been neglected since oil was discovered in Sudan in 2000. The resulting imbalanced growth process has produced a concentration of manufacturing and irrigated land at the center, and a huge disparity in development indicators across regions. In 2012, 47 percent of the Sudanese population lived below the poverty line. The incidence of poverty varies widely: only 25 percent of the Khartoum population lives in poverty versus 66 percent of the population of northern Darfur.[10] According to the World Bank and the International Monetary Fund (IMF), the external debt of Sudan (which reached $38 billion in 2010) is unsustainable.[11] Sudan did not fare well on the Millennium Development Goals in 2012: 32 percent of children under the age of five are moderately or severely underweight; primary and secondary school enrollment stand at 67 percent and 22 percent, respectively, with rates dropping to below 10 percent in some regions; access to improved water sources varies from 5 percent to 73 percent by state; and malaria is a leading cause of mortality and morbidity.[12]

Throughout both wars, the Khartoum government invested very little in the development of southern Sudan. This shows in much higher levels poverty in South Sudan relative to Sudan in terms of income, health, and education. GDP per capita in 2010 was $1,546, with approximately 80 percent of the population living on less than $1 per day.[13] South Sudan has the highest maternal mortality rate in the world, and 60 percent of people have no access to health care at all.[14] Primary school enrollment was 46 percent in 2010, 67 percent of the

[5] Ibid.

[6] Ibid.

[7] “Bashir & Salva Kiir to Meet in January to Boost Talks on Rebels’ Issue,” *Sudan Tribune*, December 20, 2012, available at www.sudantribune.com/spip.php?article44924 .

[8] “Sudan Country Profile,” BBC News, May 1, 2012, available at www.bbc.co.uk/news/world-africa-14094995 .

[9] United Nations Development Programme (UNDP), “Status of MDGs in Sudan in 2012,” available at www.sd.undp.org/mdg_fact.htm .

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Thomas Danielewitz, “South Sudan Launches its First GDP Estimate,” *Africa Can…End Poverty*, World Bank, August 23, 2011. Available at http://blogs.worldbank.org/africacan/south-sudan-launches-its-first-gdp-estimate .

[14] UK House of Commons International Development Committee, South Sudan: Prospects for Peace and Development, Fifteenth Report of Session 2010–12, April 12, 2012.

population had access to safe water, and malaria was hyper-epidemic.[15]

Access to new technologies in both Sudan and South Sudan is growing fast. In 2009, 8 percent of the population of both Sudan and South Sudan were Internet users; by 2010 this rose to more than 10 percent.[16] By 2012, in northern Sudan alone, there were 6.5 million Internet users or approximately 19 percent of the population.[17] This places Sudan above the average for African countries (15 percent). There are no Internet usage figures available for South Sudan, but numbers of cybercafés in Juba and other state capitals are rapidly increasing.

In 2005, cell phone subscriptions in Sudan and South Sudan were 9 percent, by 2009 this had risen to 28 percent and there were 17.6 million cell phone handsets.[18] As with many other African countries, Sudan and South Sudan never had well developed landline networks (less than 1 percent of the population had access to landlines in 2009), making the adoption of mobile networks, which have an easier infrastructure to install and maintain, all the more rapid. In fact, investors in South Sudan believe they will triple cell phone subscribers by 2014.[19] Cell phone companies in both countries are also quickly becoming providers of banking and payment services, making adoption rates even faster.

Government censorship and control of cell phone and Internet services is present in Sudan, under the National Telecommunication Corporation (NTC). Media censorship was officially lifted in July 2005 but reinstated in 2008. Since then, a number of media outlets have been closed down for publishing content contrary to the views of the government. The 2001 National Strategy for Building the Information Industry says that the Internet will be filtered for content that is “morally offensive and in violation of public ethics and order.”[20] Filtering is handled by a special unit of the NTC, which screens Internet media before it reaches users in Sudan. The NTC has an email address on its website where users can request to add or remove websites from this blacklist. Sites that facilitate anonymous browsing or circumventing Internet filters are blocked, as are sites with content related to hacking and a few translation sites.[21] In 2012, following protests over a YouTube video depicting the Prophet Mohamed, YouTube.com was blocked. The government also reportedly monitors Internet communications, including reading email messages between private citizens and reviewing content on Facebook, Twitter, and the blogosphere. Some blogs have been occasionally, temporarily blocked. A number of downloadable software products, including some Google products, are not available in Sudan as a result of US sanctions. Finally, the government also requires that telecom networks disconnect any mobile prepaid subscribers who do not provide personal information, for security reasons. The government also occasionally requests mobile network providers to cut off connections in certain areas for matters of national security, as it has done recently in South Kordofan and Blue Nile when fighting has intensified.

There are few analyses of control and censorship of the Internet and mobile networks in South Sudan, but there appears to be greater freedom. Reportedly, the Media Bill of South Sudan largely conforms with international standards of freedom of expression.[22]

Case Studies

CRISIS AND RECOVERY MAPPING AND ANALYSIS

Since 2007, UNDP Sudan’s Crisis and Recovery Mapping and Analysis project (CRMA) has carried out community-level mapping of threats and risks affecting communities in six states of Sudan and ten states of South Sudan, in collaboration with the respective state governments. In this process,

[15] Ibid.

[16] “Sudan Millennium Development Goals Progress Report 2010," The Republic of Sudan Ministry of Welfare & Social Security National Population Council General Secretariat, available at www.sd.undp.org/doc/Sudan%20MDGs%20Report%202010.pdf ; UNDP, “Status of MDGs in Sudan in 2012.”

[17] Internet World Stats, “Internet Usage Statistics for Africa,” available at www.Internetworldstats.com/stats1.htm .

[18] UNDP, “Status of MDGs in Sudan in 2012”; CIA, “Sudan Profile,” The World Factbook, August 29, 2012, available at www.cia.gov/library/publications/the-world-factbook/geos/su.html .

[19] Aaron Maasho, “South Sudan’s Vivacell Aims to Triple Subscribers,” *Reuters*, April 8, 2011.

[20] “Sudan Country Profile,” OpenNet Initiative, August 7, 2009, available at http://opennet.net/research/profiles/sudan .

[21] Ibid.

[22] Ibid.

CRMA has developed a participatory mapping and analysis methodology to enhance evidence-based strategic planning in conflict and postconflict settings. The methodology relies on a GIS-enabled, desktop database tool developed by UNDP for the project (the CRMA tool, see box 6 for details). Through its work, CRMA supports government and civil society actors to jointly identify priorities for intervention and response. The process has fostered an open dialogue, strengthening the capacities of local actors to respond to emerging priorities and potential conflicts in a timely and appropriate manner. Participatory, technology-enabled mapping has thus become a key tool in UNDP's support to peacebuilding and recovery in Sudan and South Sudan.

Box 1. CRMA Methodology

The CRMA methodology builds on existing tools such as Rapid Rural Appraisals, Conflict Analysis Frameworks, Vulnerability Assessments, and Community-Based Risk Assessments to provide an evidence base generated at the grassroots. Community workshops are run by the CRMA team in partnership with government officials to gather perceptions on threats and risks to livelihoods. Each workshop gathers about thirty participants, from mixed backgrounds representing the community, over the course of two days. The workshops run a variety of exercises, including plenary fora, participatory mapping, mind mapping, and focus groups. Community perceptions gathered at these workshops are then assigned a category and a geographic location, to allow for both thematic and geographic analysis. In locations where a local peace agreement has just been signed, the Joint Conflict Reduction Programme (another UNDP Sudan project) has adapted the CRMA methodology to take communities through a participatory intervention-design process. Mixed groups of participants from either side of the conflict brainstorm specific interventions (with beneficiaries and geographic locations identified) that would address the risks they have agreed affect the entire community and are at the root of the conflict.

At its inception, the CRMA project had three key aims: (i) to address the planning needs of a country with a weak evidence base; (ii) to support good governance by providing a transparent methodology for the identification of priorities, and (iii) to rebuild community ties by operationalizing participatory planning methods.[23] There has been a fourth, unexpected outcome to CRMA. The introduction of an innovative desktop software (the CRMA tool) to state governments has opened the door to further innovation in the use of mobile and Internet-based technologies for conflict prevention, specifically two pilot early-warning systems in Sudan and South Sudan.

In 2011, UNDP Sudan identified that the work of the CRMA project provided an entry point for setting up a state-level conflict-early-warning system that drew on grassroots information and utilized new technologies. Such an early-warning system would use the community-level mapping exercise as a baseline, and would then update in real time a set of minimum indicators drawn from this baseline. UNDP Sudan has plans for a pilot state-level conflict-early-warning system in South Kordofan State. Here, UNDP Sudan had carried out its community-level mapping exercise in collaboration with the state's Reconciliation and Peaceful Coexistence Mechanism (RPCM). The RPCM is the state's conflict-early-response mechanism, and is supported by UNDP's JCRP. JCRP and CRMA supported the RPCM to analyse data from the community level mapping exercise, and produce a conflict situation analysis report that informed the RPCM's priorities for action.

Based on this experience, the Joint Conflict Reduction Programme convened a number of discussions and an initial design workshop with technical staff at the RPCM, which resulted in a draft design for the early-warning system (see box 1). All data collected would be entered into the CRMA tool. RPCM technical staff members are trained in and familiar with this tool, having used it to process and analyze data collected in the community mapping process carried out by CRMA. Using this data and based on their previous experience with analyzing geolocated community perceptions of conflict, the technical secretariat for the early-warning system would produce regular, actionable reports to identify priority areas, priority

[23] Margunn Indreboe Alshaikh and Helena Puig Larrauri, "Building Resilience Through Crisis Mapping, Community Engagement and Recovery Planning in Sudan," Proceedings of the Ninth International ISCRAM Conference, April 2012.

Box 2. Sudan Early-Warning System Design

The conflict-early-warning system would be run by two structures: (i) a six-member state-level steering committee, with high-level representatives from state government, the UN, and Dilling University (in South Kordofan); (ii) a technical secretariat, with technical staff from the same organizations. The technical secretariat would coordinate the collection of data on a minimum set of indicators pertinent to conflict early warning, drawn from the existing community mapping data collected by CRMA and the RPCM. These indicators would be both incidents and perceptions of conflict.

The system would use a combination of participatory mapping and bounded crowdsourcing to collect data. Specifically, three reporting mechanisms would be used:

- An annual community mapping exercise: the technical secretariat would run a series of local workshops based on the CRMA methodology (participatory mapping workshops). Locations for these workshops would be identified to ensure geographic spread as well as focused coverage of known flashpoints.
- Monthly situation updates: at the location of each mapping workshop, a local peace committee would be set up (or identified where one already exists). This local peace committee would be asked to fill out a survey on a quarterly basis, to be processed by the technical secretariat.
- Real-time updates from the public and from a network: a short message service (SMS) shortcode would be made available for free SMS reports to the conflict-early-warning system. This shortcode would be publicized to communities at the mapping workshops. A network of trusted informants identified by the technical secretariat would be provided with scratch cards and encouraged to report using the shortcode.

issues, emerging areas, and emerging issues.

This draft design was presented to the chairman of the RPCM, who in turn presented it to the governor of South Kordofan State in early 2012. The governor replied that the conditions are not right to implement a conflict-early-warning system. This response is hardly surprising given the recent developments in South Kordofan, which since June 2011 has witnessed armed conflict between the Sudan Armed Forces and the Sudan People's Liberation Army. As of December 2012, the pilot is still pending implementation.

The early-warning-system pilot in South Sudan also builds on an interested government institution. On May 5, 2012, South Sudan launched its national Conflict Early Warning and Response Unit (CEWERU).[24] CEWERU is chaired by the South Sudan Peace and Reconciliation Commission and is directly linked to the Inter-Governmental Authority on Development's (IGAD) Conflict Early Warning and Response Mechanism (CEWARN). CEWERU was established as a result of the government's adoption of a seven-year conflict-reduction strategy (2012–2019).[25] In fact, the national Conflict Early Warning and Early Response System (CEWERS) has been operational in four states since 2009, under the leadership of the South Sudan Peace and Reconciliation Commission with the

Box 3. South Sudan Early-Warning System Pilot

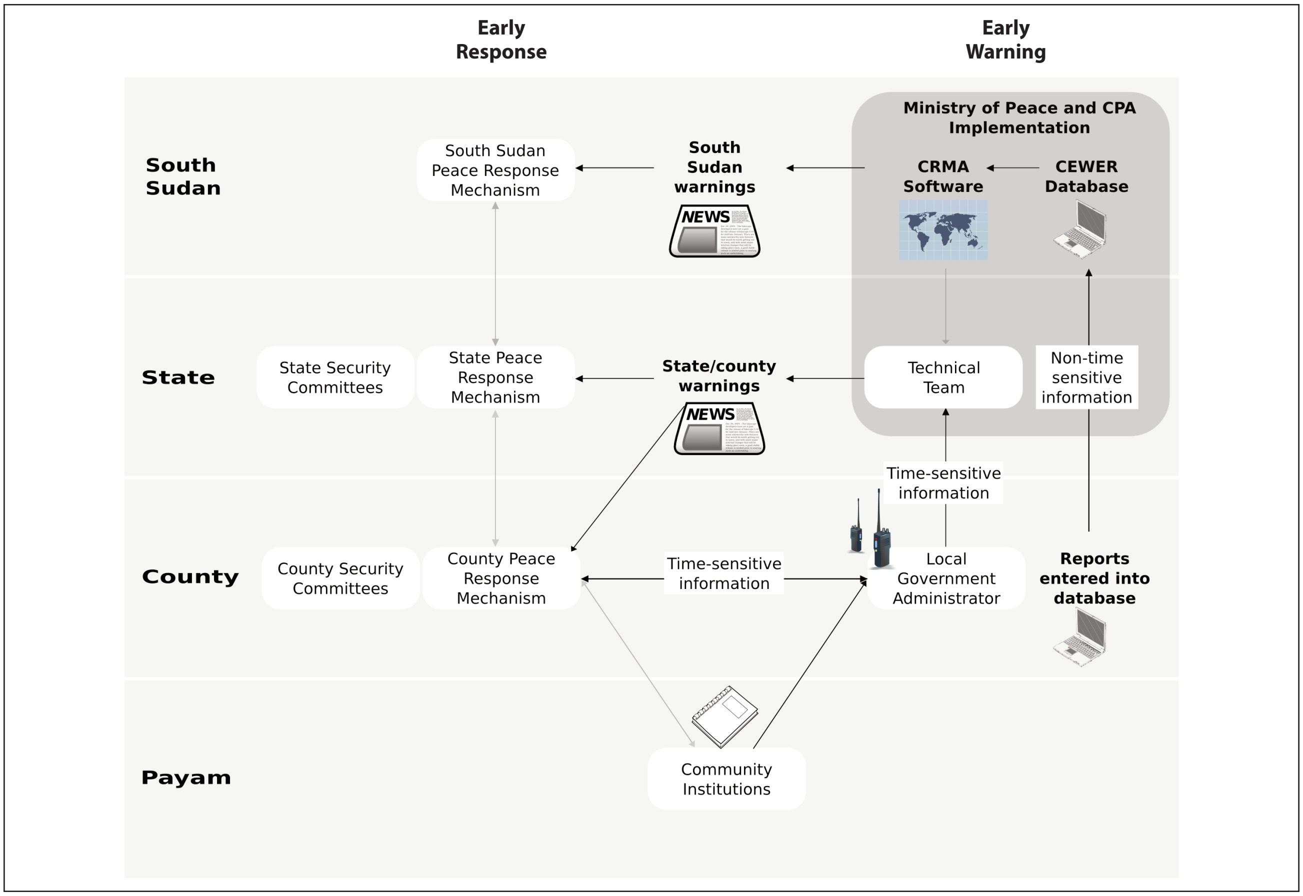
CEWERS operates a database that collects georeferenced conflict-incident reports at various levels.

- Local: reports are collected at the local level from early warning officers, including staff of the South Sudan Relief and Rehabilitation Commission, staff of community organizations, and IGAD field monitors.
- County: reports come in to an early-warning-and-response structure managed by the South Sudan Peace and Reconciliation Commission at the county level via email, radio, cell phone, radio link, and handwritten reports. All reports follow a standard incident-report format.
- State: reports collected at the county level are then aggregated up to the state level and relayed to the SSPRC-managed state early-warning-and-response structure.
- National: all data from the states is fed in to the SSPRC-managed database at the national level. This data is also fed into the UNDP-managed Crisis and Recovery Mapping and Analysis (CRMA) digital atlas database.

[24] "Launch of South Sudan Early Warning and Response Unit," *Sudan Tribune*, May 9, 2012, available at www.sudantribune.com/spip.php?article42544 .

[25] Julius N. Uma, "S. Sudan to Develop Conflict Early Warning and Response Strategy," *Sudan Tribune*, June 15, 2012, available at www.sudantribune.com/S-Sudan-to-develop-conflict-early,42928 .

Figure 1: Conflict Early Warning and Early Response System for South Sudan[26]


Early Response
Early Warning
South Sudan
State
County
Payam
Ministry of Peace and CPA Implementation
South Sudan Peace Response Mechanism
South Sudan warnings
NEWS
CRMA Software
CEWER Database
State Security Committees
State Peace Response Mechanism
State/county warnings
NEWS
Technical Team
Non-time sensitive information
Time-sensitive information
County Security Committees
County Peace Response Mechanism
Time-sensitive information
Local Government Administrator
Reports entered into database
Community Institutions

support of Catholic Relief Services as its lead implementing partner.[27] The establishment of CEWERU in 2012 signals the proposed expansion of the system to nine states and transfers ownership of the system to a high-level committee of government, UN, and NGO officials who are tasked with responding to alerts in the system.

CEWERS has started using SMS on a trial basis, both to receive early-warning information and to send out early-response information. Already SMS enables community members to report directly on incidents to the county-level structures (circumventing field monitors), although the process is ad hoc and has not been made systematic through the use of a tool or shortcode. Soon, county, state, and national structures will start using SMS to send out alerts on incidents to relevant responders. To further expand the use of SMS, CEWERS has obtained a toll-free number and is negotiating access to the servers for cell phone service providers like Zain and MTN. Most of the incident data collected to date relates to cattle raids, one of the most prevalent forms of conflict in South Sudan. The database is available to the public upon request from the CEWERU, but it is not available on the Internet.

The development of early-warning-system pilots that utilize mobile and web-based technologies has also had a feedback effect into the original CRMA project. The latest version of the CRMA tool (currently in testing with UNDP and users affiliated with the UN Office for the Coordination of Humanitarian Affairs) incorporates two web-enabled functions: (i) a simple and efficient export-import function to share map layers and table data; (ii) a function to export and display any selection of data to Google Maps, Open Street Map, and Ushahidi automatically. Although there is as yet no

[26] Diagram courtesy of Catholic Relief Services South Sudan.

[27] CEWERS has been fully operational in eastern Equatoria and Upper Nile and partly operational in northern Bahr ElGhazal and western Equatoria.

way to incorporate SMS data, the CRMA team are considering developing a specific "early-warning mapper" component to the tool.

SUDAN VOTE MONITOR

The Sudan Vote Monitor was an initiative of the Sudan Institute for Policy Research[28] in partnership with the Asmaa Society for Development. It sought to use communication technologies to support independent monitoring of the Sudanese presidential elections in 2010 and the South Sudan referendum on independence in 2011 by local civil society organizations, local media, and the general public.[29] Specifically, the initiative aimed to support these groups by deploying a live map.

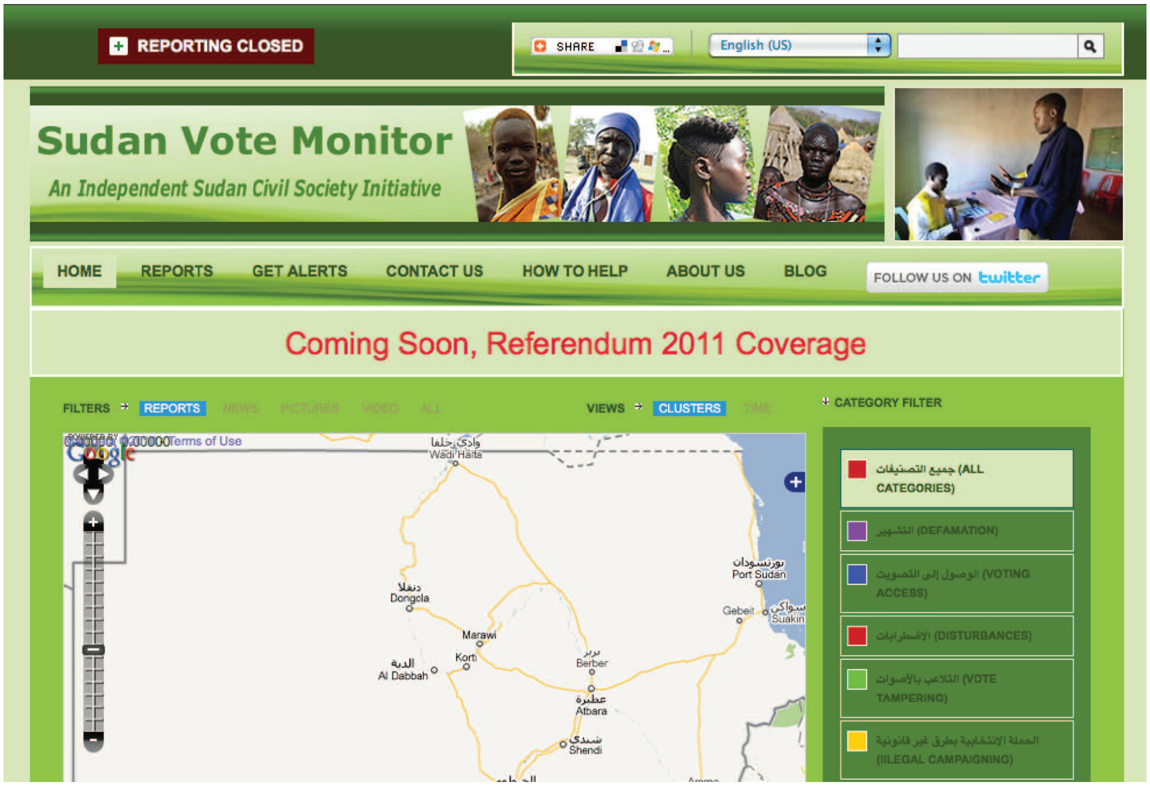
Box 4. Sudan Vote Monitor: System Details

The Sudan Vote Monitor system used an Ushahidi platform (see box 6 for details) that received reports via email, SMS, and web. The system had three sources for reports:

1. Independent local observers working for participating civil society organizations, who reported back using standard reporting forms and/or text messages. When texting, observers used coded categories to relay information (e.g., 1 = election fraud).
2. The general public could send reports via SMS (using a shortcode in the 2010 elections and a longcode in the 2011 referendum) or via the Ushahidi web platform. These crowdsourced reports were verified by trained volunteers.
3. Selected press media and social media reports were monitored for the 2011 referendum by online volunteers from the Standby Task Force, an online network of volunteers.

Reports received in the platform were mapped and posted to the Sudan Vote Monitor website in real time by its staff and volunteers. Reports included information on people voting without IDs, lack of voter registration lists, polling centers opening very late or closing very early (or both),

Figure 2: The Sudan Vote Monitor Website[30]



[28] Sudan Institute for Research and Policy (SIRP) is an independent, nonpartisan, nonprofit research organization based in the United States, dedicated to the promotion of knowledge about Sudan. For more information, see www.sudaninstitute.org .

[29] The initiative also received technical support from Ushahidi (see www.ushahidi.com) and eMoshka (see www.emoshka.org).

[30] A screenshot from the Sudan Vote Monitor website, www.sudanvotemonitor.com. The website is no longer available.

observers being denied access to polling centers, ballot boxes going missing, and different versions of ballots. The initiative also produced summary blog posts of reports received.

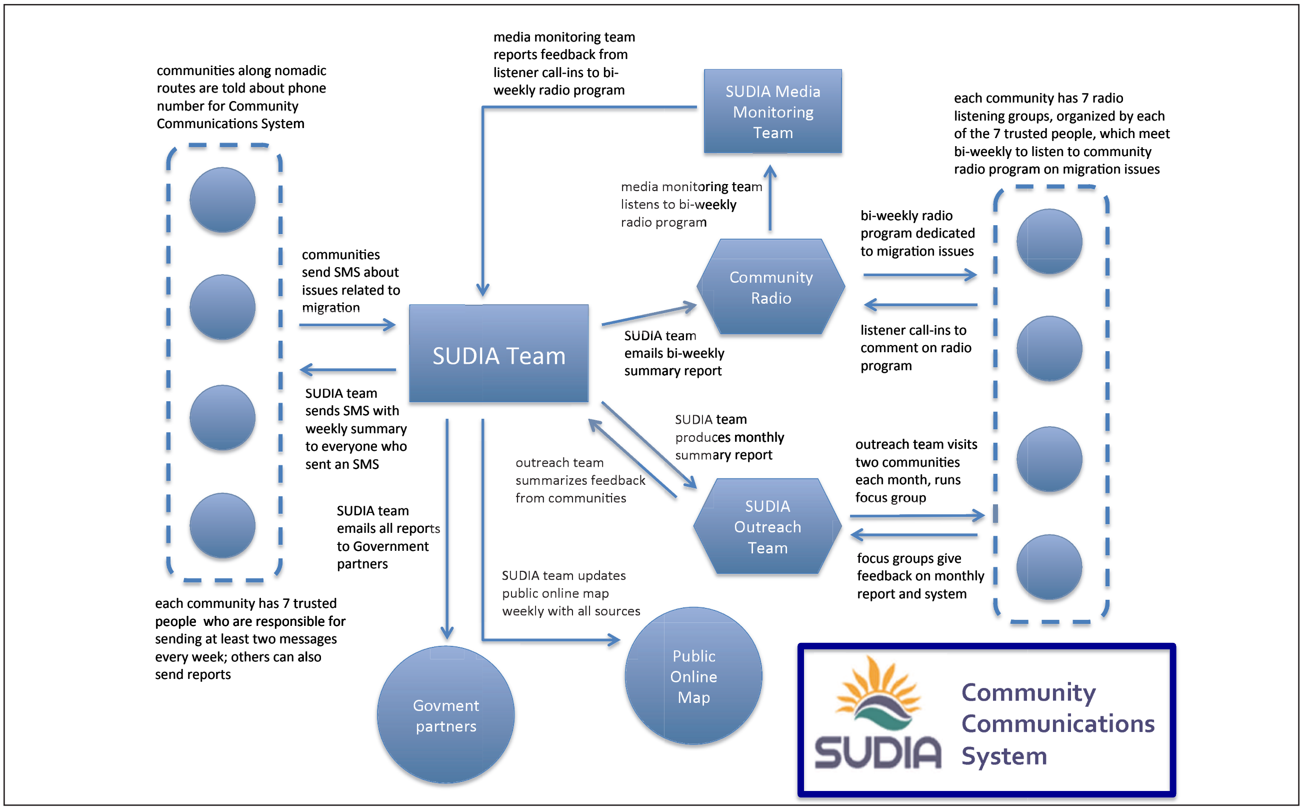
The Sudan Vote Monitor ended after the 2011 referendum was conducted, and was mostly a failure. The initiative suffered from the pitfalls of a conflict-early-warning system that is technology driven and short term. Its one clear success was to demonstrate to local civil society groups that it was possible to leverage crowdsourcing and technology to monitor elections, or other possible causes of conflict. In his study of various tech-enabled, crowdsourced election monitoring projects, Max Grömping makes a remark that also applies to the situation with the Sudan Vote Monitor:

> The added value of crowdsourcing lies mainly in the strengthening of civil society via a widened public sphere and the accumulation of social capital with less clear effects on vertical and horizontal accountability.[31]

BLUE NILE PARTICIPATORY DIGITAL MAPPING

The Participatory Digital Mapping project is an initiative of the Sudanese Development Association (SUDIA), funded by the United States Institute for Peace.[32] SUDIA has been working on a number of peacebuilding projects in Blue Nile State and has identified that communication is typically poor along the migratory routes. Located in the southeast of Sudan, bordering Ethiopia and South Sudan, Blue Nile State is home to many tribes that migrated there from across Sudan and across the Sahel in previous centuries. Most of the population engages in either sedentary farming or nomadic pastoralism. Over the past few years, conflict between farmers and pastoralists in Blue Nile State has become more acute as a result of increasing

Figure 3: Map of the Communications System in the Participatory Digital Mapping Project[33]


communities along nomadic routes are told about phone number for Community Communications System
media monitoring team reports feedback from listener call-ins to bi-weekly radio program
SUDIA Media Monitoring Team
each community has 7 radio listening groups, organized by each of the 7 trusted people, which meet bi-weekly to listen to community radio program on migration issues
media monitoring team listens to bi-weekly radio program
bi-weekly radio program dedicated to migration issues
communities send SMS about issues related to migration
Community Radio
SUDIA Team
SUDIA team emails bi-weekly summary report
listener call-ins to comment on radio program
SUDIA team sends SMS with weekly summary to everyone who sent an SMS
SUDIA team produces monthly summary report
outreach team summarizes feedback from communities
outreach team visits two communities each month, runs focus group
SUDIA team emails all reports to Government partners
SUDIA Outreach Team
focus groups give feedback on monthly report and system
SUDIA team updates public online map weekly with all sources
each community has 7 trusted people who are responsible for sending at least two messages every week; others can also send reports
Public Online Map
Govment partners
SUDIA
Community Communications System

[31] Max Grömping, "Many Eyes of Any Kind? Comparing Traditional and Crowdsourced Election Monitoring and Their Contribution to Democracy," Presented at ICIRD, Chiang Mai, July 26-27, 2012.

[32] The Sudanese Development Initiative (SUDIA) is a nongovernmental not-for-profit organization committed to playing an active and lead role in advancing peace, development, and social justice within the African continent (see www.sudia.org). The United States Institute of Peace (USIP) is an independent, nonpartisan conflict-management center created by the United States Congress to prevent and mitigate international conflict without resorting to violence (see www.usip.org).

[33] Diagram courtesy of SUDIA.

demands on the land available for both grazing and farming. The expansion of rain-fed mechanized schemes, the increment in numbers of cattle, and the expansion of a national park have all contributed to this growing demand. In 2011, the situation was aggravated further by blockages at the borders with South Sudan following independence (which have caused some pastoralists to remain in Blue Nile State at times when they would normally be in South Sudan) and by the eruption of conflict between the government of Sudan and the Sudan People's Liberation Army–North (which has rendered the general security situation unstable).

Local people rely on community leaders, cell phones, and community radio to access information, but the flow of information from these sources is patchy, and there are rarely opportunities for people to contribute information themselves. SUDIA believes that enhancing information flows along the migratory routes can help prevent conflict in two ways. First, misinformation about the timing of migrations or the availability of water can be a direct cause of conflict. With accurate and up-to-date livelihoods information, communities can understand, influence, and adapt to the fluid situation in the state. Second, there are many local initiatives to foster better understanding and coexistence between farmers and pastoralists. And this work needs to be publicized to create a discourse of peace. SUDIA believes that the participatory dissemination of information on peace activities can become a locally owned early-response mechanism.

With this in mind, SUDIA is implementing a pilot participatory-digital-mapping process along three migratory routes in Blue Nile State. Workshops with local stakeholders began in October 2012. SUDIA staff members have developed a data-collection protocol, standard analysis report, and public online map. The organization is seeking final approval from the authorities to begin collecting data via SMS from communities.

Box 5. Participatory Digital Mapping: System Details

The system will use a combination of crowdseeding and crowdsourcing, receiving reports from four sources: SMS from the public, SMS from selected trusted reporters, call-ins to a biweekly community radio program, and feedback from monthly outreach meetings run by the SUDIA team. All reports coming in will be tagged by source, location, date, topic, and verification status. There are twenty topics in the system, grouped under four broad categories: livelihoods, herding and farming, disagreements, and peace. Verification of reports will follow a standard protocol, whereby a report is verified if the following conditions are met: (i) report from a trusted source is supported by two or more reports from any source; or (ii) a report from a public source (SMS, radio call-in, or outreach meeting) is supported by four or more reports from two or more different sources.

Everyone who sends an SMS to the system will receive in return three weekly SMSs summarizing important information on livelihoods, herding and farming, and peace. Every two weeks, the Blue Nile Community Radio will broadcast a one-hour program about issues related to migration. The program will be based on a biweekly summary prepared by the SUDIA team using information from the system. The radio broadcast will invite listeners to call in and comment on the summary. SUDIA's media monitoring team will listen to these calls and record relevant information that will then be entered into the system. SUDIA's trusted reporters in each community will organize radio listening groups, which will not only encourage call-ins but also provide a forum for discussion of community responses to challenges identified in the radio program.

Every month, the SUDIA outreach team will visit two of the communities participating in the system. During this visit, they will present a summary monthly report to a focus group and then facilitate a discussion on possible community responses to emerging livelihood and conflict challenges. The meeting will also provide an opportunity for the community to give feedback on reports (verifying or denying information) and on how the system can be made more useful to them.

Lessons Learned from Sudan and South Sudan

SHORT-TERM PREVENTION AND CRISIS RESPONSE

Has the use of information communication technology strengthened efforts to prevent violence and conflict in the context of crises in Sudan and South Sudan? Assessing the three case studies, it becomes clear that **success in the short term depends on whether technology facilitates the creation of actionable data**. Technologies make collection and analysis of information in crisis settings easier, but this does not always result in early-response programming in the short term.

Sudan Vote Monitor provides a lesson learned on the failure to create actionable data. The potential for a citizen-reporting initiative to warn about election-related conflict in Sudan is strong. In a country with large distances, a system that allows local monitors and the general public to get their story out can be very powerful. And yet, as polls closed for the 2010 presidential elections, only 218 reports had been mapped by the Sudan Vote Monitor. The results for the 2011 referendum were even lower, with only 96 reports mapped. The limited number of reports received by the system call into question the usability of any resulting analysis, since it seems unlikely that the initiative could present a comprehensive picture of any tension or conflict during the election periods. More importantly, the information collected by the system did not effectively flow back out to anyone who could act on it. The initiative was best known and respected by local civil society groups, and these groups could have been in a position to respond to reports of violence. However, most Sudanese civil society groups are not online and do not regularly use the web to organize or communicate, so they were unlikely to check an online platform for information. Thus, in the case of Sudan Vote Monitor, the added value of a tech-enabled platform was at best marginal.

Box 6. Software Tools Used in Sudan and South Sudan

CRMA

The CRMA tool is a desktop application with four modules, each for different data collection needs: (i) the 4Ws for project activity information; (ii) the Crisis and Recovery Mapper for perceptions of threats and risks; (iii) the Incident and Event Mapper for violent incidents data; and (iv) the Basic Service Mapper for information on health, education, and water services. Each module has a data-entry component, a dynamic visualization tool, a reporting and statistical function, and an import-export function via the Internet. The tool is license free (available from UNDP Sudan) but not open source.

Frontline SMS

Frontline SMS is a desktop application that enables users to send, receive, and manage SMSs over a mobile network. The application is free and open source; users only pay the standard text-messaging charges through their regular cell provider. The application can be downloaded here: www.frontlinesms.com.

Ushahidi

Ushahidi is a web-based application for data management and mapping. The platform allows data to be filtered and visualized by location, by category, and over time, and other map layers can be superimposed on the initial one. The platform also allows for easy integration of data streams from SMS, email, Twitter, and web forms. The application is free and open source, and can be downloaded here: www.ushahidi.com. Ushahidi also offers a hosted version of their platform called Crowdmap: www.crowdmap.com.

For the other projects, there is no evidence that the collection of crowdsourced data for early warning is likely to encourage governments to respond more quickly and effectively to drivers of violence. However, the projects do indicate **great potential for the use of tech-enabled crowdsourcing and crowdfeeding to help governments and communities better respond to ongoing localized disputes**. Both early-warning-system pilots connected to the Crisis and Recovery Mapping and Analysis project (CRMA) illustrate this potential.

In the conditions prior to the current conflict, it seems likely that an ICT-enabled conflict-early-warning system would have expedited the response to conflict in South Kordofan. The system proposed by UNDP was designed to fit the RPCM, an existing early-response mechanism that had already proven its ability to effectively prevent conflict and resolve existing disputes.[34] Furthermore, the RPCM had already begun to adopt data-driven decision making and started using geospatial technology (the CRMA tool). The system thus builds on a government institution with both the credibility and capacity to adequately manage a technology-enabled early-warning system.

Although a full assessment of South Sudan's CEWERS is still premature, the decision to scale up the system from four to nine states suggests that it has, to date, been somewhat effective at triggering early responses to prevent conflict.[35] The system is designed to link frequently to dedicated conflict-early-response mechanisms. Each state's technical team meets monthly to review and analyze early-warning reports and produces a situation-analysis report with recommendations. These recommendations are then relayed to county and state "peace response meetings," which bring together stakeholders with the ability to intervene in local conflicts. Where action is required at a higher level, Catholic Relief Services contacts the Peace Commission, which then contacts CEWARN and/or convenes CEWERU for immediate action. Action taken by CEWERU or at peace response meetings to respond to a conflict incident is also recorded in the system. Finally, all CEWERS data is entered in the UNDP CRMA database, which supports conflict-prevention and -recovery planning for the UN in Sudan.

Despite this positive assessment, there is one key drawback to all initiatives examined when it comes to crisis response. A fast response requires near real-time information, which in all the cases is dependent on either physical access to or Internet or cell phone coverage in all areas. Both the conflict situation and the infrastructure of Sudan and South Sudan make this unlikely. There is limited information on Internet and cell phone usage, making it harder to assess how critical ICT is to crisis response. Both Catholic Relief Services and CRMA report that, although their current databases are desktop applications not web platforms, email is critical for data sharing between different levels. Even if the Internet is not available to all government officials the two projects work with, it is accessible to many. Catholic Relief Services further reports that some information is relayed over the phone or delivered physically on paper. Given the wider availability of cell phones, the organization also reports that the addition of SMS data collection can improve and expand the network of reporters, but there is no assessment at present of this feature. That said, while cell phone services reach all locality capitals in the state, coverage in more remote rural areas is patchy. In more remote areas, mobile-enabled real-time reporting would require reporters to physically travel to an area with coverage before sending out messages. This would work most of the time, but physical access to many parts of Sudan and South Sudan is impossible during the rainy season. In the current context, restrictions on physical access and reductions in cell phone service as a result of security concerns are likely to reduce the effectiveness of crisis-response initiatives that are reliant on the Internet or cell phone networks.

LONG-TERM PREVENTION AND CAPACITY BUILDING

How can these same uses of new technology prevent conflict in the long term? New technologies for conflict prevention are more likely to be adopted when capacity building includes training in the use of technology. Given the importance of government buy-in demonstrated in the case studies, **international actors should invest in building government capacities to use new technology**. The success of investing in training as a path to sustainable use of new technologies for conflict prevention is demonstrated by the CRMA case. With capacity-building support through CRMA, state departments of planning across Sudan have gathered an evidence base using novel technologies and participatory methodologies to engage communities in recovery planning. Building on this work, UNDP's Conflict Reduction Program has used state peacebuilding mechanisms in Blue Nile and South Kordofan to engage communities in the use of the evidence base, identify priorities for peace, and design interventions that would support recovery and reconciliation. This history of engagement, support, and training was evident in the

[34] According to UNDP, the RPCM has a strong track record in convening and accompanying local peace conferences. With the exception of areas affected by the current state-level conflict, all peace agreements supported by the RPCM still hold.

[35] Catholic Relief Services shared (in phone conversation and over email) a number of success stories of rapid response to a specific conflict incident, including one case where cooperation through CEWARN enabled Kenyan police to stop a cross-border cattle raid using information in an alert issued by CEWERS.

quick understanding and acceptance of the early-warning system by staff in the state Reconciliation and Peaceful Coexistence Mechanism. Staff members see the benefits of a tech-enabled early-warning system because they have already been trained to use a geodatabase to analyze conflict and plan based on this analysis.

In South Sudan, CRMA has not been present as long, and lower capacity levels are likely to be an obstacle to CEWERS. Local capacities to manage CEWERS are reportedly mixed.[36] Catholic Relief Services have carried out extensive training at the state and county levels, and reports indicate that local capacities at those levels are generally strong, particularly in counties where local authorities are strongly involved and have come to see value in the system. However, capacity at the national level is weaker, with the Peace and Reconciliation Commission requiring ongoing support to maintain the database. This does not bode well for the rollout of tech-enabled features, since most of the tech (specifically SMS alerts) would be managed at the national level.

The case studies also indicate that governments can use new technologies to build the capacities of their institutions. Specifically, **governments should be advised that new technologies are effective at connecting different levels of conflict prevention** and bridging the gap between "warners" and responders. The CRMA case illustrates how a technology-enabled process can show government institutions the value of sharing information on the conflict context in order to plan ahead together to prevent conflict. First, the CRMA process has helped government officials identify priority areas for intervention. For example, where an actor is interested in areas that are prone to conflict and have a lack of water services, CRMA data can identify locations where communities report tensions between groups and problems with access to water. Second, since all inputs are geolocated at the village level, it has provided contextual information about specific locations of interest, in greater depth than sectoral reports. Finally, it has provided a way to check how the objective situation on the ground compares to the subjective perceptions of communities. Where these two differ, policy solutions often required cooperation between several institutions.

In addition to lessons learned from CRMA in this respect, the South Sudan CEWERS case illustrates the benefits of two-way communication and of expanding reports to cover responses (not just warnings). It also shows how SMS technology can make the links between different levels of government faster and wider in reach.

There are also long-term prevention and capacity-building lessons for civil society in these case studies. **Civil society organizations can learn from these case studies that new technology does not create local capacities for peace, but can increase existing local capacities.** Specifically, the Participatory Digital Mapping project suggests that new technology in areas with a history of violent conflict can be an effective tool in bolstering community capacity for conflict prevention by building on existing mechanisms and combining analog and digital technology. SUDIA's initiative has the potential to demonstrate how technology-enabled conflict-prevention initiatives can be put to work in remote environments, enhancing existing local networks for peace. The key strength of this project is that it augments an existing analog early-warning system with a digital component. The initiative will likely gain legitimacy from the strong institutional relationships enjoyed by SUDIA. SUDIA is considered an independent actor by local civil society organizations and at the same time has strong links with government bodies at both the national and state levels. Most relevant, it has an existing relationship with the Blue Nile State Peace Council, the main peacebuilding (and early-response) mechanism in the state.

On the other hand, the Sudan Vote Monitor case demonstrates that where civil society responders are not already using digital means, new technologies that are not connected to existing (non-digital) methods are likely to fail. The small number of reports received by the Sudan Vote Monitor is to some extent a reflection of calm polling with little to report, but that is not the whole story. Two other Sudanese civil society organizations conducting

[36] According to Catholic Relief Services, the potential for effective early warning already exists in South Sudan. Communities consistently warn of violence before it occurs through local mechanisms, and seasonal livelihoods patterns reliably predict inter-community violence. However, assessments undertaken by Catholic Relief Services reveal a number of capacity challenges (inconsistent and reactive reporting, uncoordinated responses, and inadequate infrastructure) that have made early-warning and -response mechanisms in practice less effective than they could be.

paper-based monitoring received thousands of reports. There were a number of difficulties specific to the deployment of SMS and Internet technology that affected the performance of this particular monitor. Lack of coordination with civil society on the ground was a big problem. The Sudan Institute for Policy Research did not have a continued presence on the ground in Sudan. As a result, the local civil society organizations and local media whose monitoring work the Sudan Vote Monitor planned to support were not contacted until very close to polling time. Local civil society organizations had an established workflow by this point, and integrating the Sudan Vote Monitor's support at such a late stage proved difficult. Likewise, the local media already had a full program for coverage and was not given enough time to plan coverage of this initiative's message. Finally, SMS reporting numbers were on both occasions only made available and publicized a few days prior to polling. Equally problematic was the limited capacity to process reports demonstrated by participating civil society organizations. For the presidential elections, the Sudan Institute for Policy Research stated that over 500 reports were received, but only 200 made it onto the web platform. This might in part be due to insufficient training, but more likely was a result of insufficient human resources to cope with various reporting activities. Adding reports to the web platform was not top priority.

HORIZONTAL AND HIERARCHICAL INFORMATION FLOWS

A lesson learned from all case studies is that **horizontal information flows are more likely to elicit rapid responses**. This is one limitation of the pilot early-warning-system design for north Sudan: it caters only for hierarchical information flows. In other words, information comes from the ground up to the technical secretariat (and possibly back down), but the system does not envisage enabling information flows between communities (e.g., from one peace committee to another or between trusted informants). The South Sudan early-warning system has remedied this by introducing SMS alerts. Catholic Relief Services is positive about the potential of SMS alerts to support faster response to conflict incidences or potential conflict-risk situations. Unlike the current hierarchical information flow for warnings, SMS alerts can go out to more people simultaneously, and thus enable a faster grassroots response. That said, Catholic Relief Services again recognized that many places are not currently covered by cell phone service and the system will need to continue to rely on radio links for local alerts.

Uneven cell phone coverage is the reason SUDIA's Participatory Digital Mapping project mixes radio and SMS. SUDIA is focusing on communicating early-warning information back to communities on the ground and facilitating discussions to respond early and peacefully to any emerging tensions. This **emphasis on non-hierarchical information flows guarantees the credibility of the initiative**, since communities directly understand what the information is used for. Furthermore, discussions will take place at community meetings facilitated by the SUDIA outreach team. These meetings are the key to linking the information collection (early warning) to local capacities for peace (early response). Meetings will focus on helping communities think through necessary responses to emerging resource-based issues, such as timing of arrival of herds or early signs of water scarcity. They will also discuss the culture of peace that is emerging along the routes, in an effort to change any existing conflict discourses. SUDIA hopes that through these meetings, it will be able to facilitate direct contact between communities and stakeholders, and thus support local early responses to prevent conflict.

CONFLICT-SENSITIVE USE OF TECHNOLOGY IN CRISIS SETTINGS

Governments, international actors, and civil society organizations should all be aware of the potential negative uses of crowdsourcing. Crowdsourcing is most open to misuse by spoilers, who can over-report certain incidents to bias data collection or simply spread misinformation. In the Sudan Vote Monitor initiative, which used crowdsourcing more extensively than any of the other cases studied, the staff involved believes that some of the reports were constructed.[37] All the case studies, except CEWERS, have a triangulation process to verify reports, as a way of mitigating any

[37] Patrick Philippe Meier, "Do 'Liberation Technologies' Change the Balance of Power Between Repressive States and Civil Society?" TUFTS University Fletcher School of Law and Diplomacy Dissertation, April 2012, available at http://irevolution.net/dissertation .

potential for manipulation of crowdsourced information.

In all projects, implementing teams have considered whether the **information collected via crowdsourcing could be used to target violent acts** by providing information to spoilers that they did not have previously. Most staff members involved in these case studies agreed that it is unlikely a crowdsourced conflict-prevention mechanism would uncover information that spoilers didn't already have. A graver concern is the potential targeting of reporters whose identity cannot be fully protected. The Participatory Digital Mapping project gets around this by encouraging (less controversial) reports of migration issues and peace activities, rather than reports on incidents of conflict. Given the potential of SMS alerts demonstrated by both CEWERS and Participatory Digital Mapping project, it is also important to consider the potential harm spoilers can cause by using crowdfeeding to disseminate messages to instigate conflict rather than peace. SUDIA manages this concern by providing training in conflict-sensitive reporting techniques to its community partners, with a focus on community radio stations, which have the widest reach.

Governments and civil society should bear in mind the expectations they raise by requesting information on conflicts. Managing expectations of early response is a problem common to all early-warning systems. However, systems that use new technologies increase participation in information collection and dissemination, and this greater exposure also increases expectations of response to conflict warnings. The Sudan Vote Monitor project suffered most from this problem, and dashed expectations of response may to some extent explain low levels of reporting.

Finally, **all actors introducing new technologies to a conflict-prevention program should carry out a "do no harm" assessment** to ensure they are operating in a conflict-sensitive manner. A simple analysis identifying the effect of new technology on dividers and connectors present in the conflict context would help identify the issues presented in this section. For example, the system design for the north Sudan early-warning system goes some way to addressing concerns around conflict sensitivity. The steering committee and technical secretariat structures ensure shared ownership between the government (for legitimacy), the UN (for neutrality), and a respected civil society organization (for credibility)—including shared ownership of all information received in the system. Publication of a detailed codebook and verification strategy would ensure impartiality of information management within the system. Publication of at least some of the information received in the system would help avoid information control by any party to the system. Despite these measures, in the current context some sections of society question the legitimacy of any government organization as a supporter of peace and dispute resolution, since it is also engaged in active conflict.

LEGITIMACY AND THE RISKS OF PARTICIPATION

The use of new technologies for conflict prevention increase participation in early-warning and early-response activities. All participants in the case studies agreed that greater participation in collection and dissemination of information about conflict increases the legitimacy and thus the efficacy of conflict-prevention work. However, more participation is also harder to control, so legitimacy comes at the expense of greater dispersion of power. In Sudan and South Sudan, the conflict context can make participation politically sensitive.

Civil society organizations should work closely with government counterparts to ensure participation is not seen as a counter-government threat, as the Participatory Digital Mapping and CEWERS projects have done. It is also helpful to ensure the project is well connected locally and has the support of formal or informal local structures of authority. The Participatory Digital Mapping and CEWERS projects both emphasize their local connections, and participation of communities is linked to increasing the reach and efficiency of these local structures. On the other hand, the Sudan Vote Monitor project did not reach out to government counterparts and as a result the government attempted to shut down the system. During the presidential elections, the Sudan Vote Monitor website was blocked for two days before it was reportedly unblocked following pressure from US

Special Envoy to Sudan General Scott Gration.[38] The interrupted service may have accounted for a drop in reporting.

International actors should equally be aware of the effect of their support to tech-enabled conflict-prevention initiatives on the political context. A stumbling block for SVM was that it was seen as an outside intervention, increasing participation without being part of the local networks. One of the difficulties for the north Sudan early-warning system pilot is obtaining approval to form a joint UN-government technical team at a time when the government does not allow the UN full access to conflict areas. The Participatory Digital Mapping and CEWERS projects are more locally owned initiatives, so fewer questions are raised about their motives for increasing participation through the use of new technologies.

Recommendations: Suggestions for Investment

International actors and governments are advised to continue to invest in pilot projects that use new technologies. These projects have the potential to significantly impact conflict prevention in a positive manner. Furthermore, assessing the impacts of fully implemented pilots will provide clearer insights. Based on the lessons learned from Sudan and South Sudan, below are some suggestions on where to focus investment.

1. Investment should focus on mobile technology. The case studies show that mobile works best because it supports non-hierarchical information flows and can easily build on analog technologies such as radio. Furthermore, mobile technology has a very rapid adoption rate, and the increases globally are being driven by Africa[39] and will in turn shape development in the continent.[40]
2. Using technology to make an early-warning system reflect real time is not necessary; near-real time is sufficient. Where early response cannot be immediate, early warning need not be immediate. The marginal utility of immediacy decreases, and time is best spent on ensuring quality of information.
3. Tech-enabled conflict-prevention initiatives work best when they enhance traditional conflict-prevention, early-warning, and early-response mechanisms, working with existing structures rather than creating new ones.
4. Initiatives should focus on using technology to support early response to local conflicts rather than investing in identifying drivers of conflict. Although addressing drivers of conflict is crucial to conflict prevention, new technology does not seem to improve identification of drivers. Greater emphasis should be placed on how technology enables communities to act to prevent conflict by allowing information to surface while incentivizing positive behavioral change.
5. Pilot projects should not focus excessively on getting the specific technology tool right the first time. As the CRMA case shows, what matters is introducing the notion of tech-enabled work and creating a robust methodology. After that, one technology innovation can lead to another.

[38] Meier, "Do 'Liberation Technologies' Change the Balance of Power Between Repressive States and Civil Society?" The election period was scheduled from April 11th to 13th but was extended through to April 15th due to logistical challenges. The Sudan Vote Monitor website was blocked on April 12th and 13th.

[39] Ibid., 11.

[40] Clayton Powell III, "Bigger Cities, Smaller Screens: Urbanization, Mobile Phones, and Digital Media Trends in Africa," Washington, DC: Center for International Media Assistance, September 18, 2012, available at http://cima.ned.org/sites/default/files/CIMA-Africa%20Digital%20Media%20-%2009-18-12.pdf .

Conclusion: New Technology in Conflict Prevention

Francesco Mancini and Marie O'Reilly[1]

The cases presented in this report have addressed conflict prevention from diverse perspectives, covering different regions of the world (Africa, Asia, Latin America), different types of violence (criminal violence, election-related violence, armed conflict, violent riots), different political contexts (restrictive and collaborative governments), and different technological tools and methodologies (big data, cell phones, crowdsourcing, crisis mapping, blogging, social media). The authors sought to cover as many contexts as possible with a limited number of case studies, with a view to examining the use of innovative technology in different settings of violence and conflict.

This approach may be particularly useful for informing policy in light of the dramatic changes underway in the landscapes of violence. At a global level, the contexts in which armed conflict and collective violence take place are changing dramatically. The number of interstate and civil wars has declined significantly worldwide, and these conflicts produce fewer battle-related deaths. On the contrary, violence linked to local disputes, organized crime, and political repression is far more pronounced.[2] The cases demonstrate clearly that employing new technologies for conflict prevention can produce very different results depending on the context in which they are applied, and whether or not those using the technology take that context into account.

Learning from the Cases

Before identifying cross-cutting recommendations for the more effective use of new information and communication technologies (ICTs) in conflict prevention, it is worth highlighting the lessons from each case.

The first paper showed how big data could serve descriptive, predictive, and diagnostic functions for conflict prevention. Big data can be used to identify patterns and signatures associated with conflict—and those associated with peace—presenting huge opportunities for better-informed efforts to prevent violence and conflict. Indeed, law-enforcement agencies are already searching for patterns in data from 911 calls, closed-circuit cameras, and crime reports in an attempt to stop crime before it happens. And academics and civil society actors are predicting social unrest and riots by tracking food prices and correlating their patterns with previous events. Nonetheless, there are significant hurdles to overcome before big data can begin to systematically and reliably inform conflict prevention. Privacy, access, and use remain key concerns for all actors looking to leverage big data for different ends.[3] But in conflict settings—where individuals face higher risks to their personal security—getting the balance right in terms of who has access to what data for what purpose is critical. Conflict settings also produce unique analytical challenges for big data. For example, if unequal access to technology in a society mirrors the conflict cleavages, problems with the representativeness of the data take on a whole new dimension, which could serve to exacerbate the situation.

In the context of criminal violence and citizen insecurity in Latin America—a region with significant Internet and mobile technology use—government agencies and police forces are successfully using digital platforms to help reduce homicidal violence through improved surveillance and intelligence. In Brazil, for example, the online Infocrim system that collects crime data in a central database and generates real-time maps is credited with helping to reduce homicide rates from 12,800 in 1999 to 7,200 in 2005. The use of innovative technologies for violence prevention among civil society actors is also widespread, largely in the form of horizontal citizen-to-citizen interventions. In light of self-censored reporting on violence in the mainstream press in Colombia and Mexico, for example, citizen-reporting systems and popular blogs now publish information on the drug wars

[1] Francesco Mancini is Senior Director of Research at the International Peace Institute. Marie O'Reilly is Associate Editor at the International Peace Institute.

[2] See, for example, World Bank, *World Development Report 2011: Conflict, Security, and Development* (Washington, DC, 2011).

[3] Alistair Croll, "Big Data is Our Generation's Civil Rights Issue, and We Don't Know It," in *Big Data Now: 2012 Edition* (Sebastopol, CA: O'Reilly Media, 2012), pp. 59-63.

that is not available elsewhere. Some also advocate pro-peace messages and sustain networks among activists. However, many of these engaged citizens are doing so at considerable risk and personal cost. Drug cartels have also proven adept at infiltrating networks and using individuals' personal information to exact retribution, which can be fatal. Thus, while a rapid growth in ICT use for violence prevention is apparent in Latin America, it is partly due to these risks that its use remains mixed at both governmental and societal levels.

Despite many innovative applications of new technologies to early-warning initiatives in Kenya, examples relating to the regional system known as CEWARN indicated a persistent gap between warning and response. Information collected partly using digital devices made its way up from the local to the state and regional levels, but if response was not forthcoming, nonstate actors at the community level could not access the information to close the warning-response gap. In addition, top-down approaches that lacked transparency and accountability sometimes led to suspicion on the part of those giving over their information, and ultimately reduced the credibility of the data and the effectiveness of the undertaking. At the same time, the choice of technology sometimes appeared to be supply-driven as opposed to demand-driven. One conflict-prevention initiative introduced outdated technology (high-frequency radios) to a population that could not make use of it and in a way that led to biased reporting. Yet many web- and SMS-based platforms in Kenya are making valuable contributions to early warning using crowdsourcing and GIS mapping. It appears the most successful have strong local input, effective partnerships, and horizontal sharing of information.

A gloomier assessment emerged from the analysis of the violent riots that broke out in Kyrgyzstan in 2010. In a context where the government restricted, rather than facilitated, the use of new technology, ICTs appeared to do little to facilitate a response by both local authorities and international actors. On the contrary, the government elected to shut down some mobile networks. At the community level, actors using mobile phones and Internet websites did foster group action, but these technologies were predominantly used to help mobilize violent mobs, issue threats to the opposing community, and propagate conflict narratives. The Kyrgyz case also highlighted the diaspora's use of ICTs in an otherwise restrictive context—an audience that is mostly ignored by donor initiatives. While the government was able to block some websites and communication flows, it was largely unable to censor the voices of the diaspora abroad, whose message was carried to the domestic population over the Internet. Thus, using ICTs, the diaspora was able to provide the Uzbek minority with information about the conflict that the Kyrgyz-dominated government and media would not make public. The Kyrgyz case was illustrative of both pernicious uses of ICTs during conflict, particularly in a situation where government accountability is lacking, and avenues for ICT to empower outside actors to influence the situation. Once again, understanding the local context in which violence is taking place appeared to be paramount for effective employment of new technologies for conflict prevention.

In the crisis context of Sudan and South Sudan, it was clear that innovative technologies could only enhance crisis response if they produced actionable data. While there was little evidence that technology contributed to short-term conflict prevention in the projects reviewed, there were indications that ICT could play a valuable role in preventing conflict emerging from ongoing localized disputes. However, Sudan and South Sudan's positions as least developed countries demonstrated that it is not just the type of technology used in a conflict-prevention intervention that matters, it is also the user's familiarity with the technology introduced. In a context with very little ICT infrastructure, paper-based monitoring of elections proved far more fruitful than the SMS-based Sudan Vote Monitor, for example. Adding ICT elements to prevention efforts worked best when bolstering existing local capacities, or when combining digital technologies with analog technologies, like radio, that were already widely in use.

How-To Guide: Leveraging New Technology for the Prevention of Violence and Conflict

The diversity and changing nature of the conflict settings explored in this report strongly suggest that those seeking to prevent conflict and save lives need to adapt their strategies to the context at hand. For example, the types of technology that link civil, governmental, and regional early-warning efforts in a relatively stable setting—as shown in the Kenya study—may have limited impact in an environment where governments act precisely to restrict such information flows—as shown in the Kyrgyzstan case. Similarly, the tools and approaches used in a context of entrenched criminal violence, in which anonymity seems critical for incentivizing citizen use of ICT for violence prevention, are unlikely to have the same effect in a situation of election-related violence, in which the vetting of the information is essential to avoid politicization and false reporting.

For policy purposes, when applying new technologies to violence- and conflict-prevention efforts, it may therefore be more helpful to think in terms of the conflict context rather than frameworks suggesting that responses are "generational."[4] Such ambitious theories may lead policymakers astray rather than inform them about how to operate in different socioeconomic, demographic, and political contexts. In reality, actors in conflict contexts rarely move linearly from one generation of tools to another. "Older" proprietary technology is often used in conjunction with "new" open-source technologies. Top-down tools cohabit with bottom-up approaches. Ultimately, the context should inform what kind of technology is needed and what kind of approach will work best.

That said, the lessons emerging from these cases, the insights of the experts involved in the project, and the analyses of the authors suggest a number of steps that those using innovative information and communication technologies can take to strengthen their voice and action in order to more effectively prevent violence and conflict. Together they can be taken as a how-to guide for international organizations, governments, and civil society actors embarking on prevention initiatives that seek to leverage new technologies.

1. EVEN IF YOU CROWDSOURCE YOUR HAMMER, NOT EVERY PROBLEM IS A NAIL.

Assuming there is a technical fix for what is an inherently political problem is a dangerous path, no matter what technology is at hand. New technologies have the potential to make huge contributions to violence- and conflict-prevention efforts, but they are no panacea for holistic solutions. In particular, when trying to integrate operational prevention (targeting a crisis at hand) and structural prevention (addressing root causes of conflict), new technologies should be accompanied by more traditional tools, such as preventive diplomacy, governance reforms, and economic initiatives. They may complement these other elements of prevention—for example, by increasing citizen participation in governance reforms—but should not replace them.

In other words, new technologies make up one more tool in the toolbox of preventive action. As such, international organizations and governments should examine all the tools at their disposal when designing prevention initiatives, not just technological tools. Civil society organizations should also not be blinkered by their particular thematic focus or pet projects. Sometimes applying new technologies simply may not work. All actors should think politically as well as technically.

2. CONSIDER THE CONTEXT.

Before embarking on any prevention initiative that seeks to apply innovative technologies, actors should step back and assess whether their investment will generate the desired results. First, the socioeconomic setting—from technology penetration and use to literacy levels—should be thoroughly examined to see whether technology can have a positive impact and to select the technology that will be appropriate. Users in one community may be well equipped to adopt a new technology and integrate it into their existing initiatives, while others may not have the means, know-how, or inclination to do so. Keep in mind that not

[4] For an explanation of the "generational" approach to technology in early warning and response, see the chapter on big data above. See also Patrick Meier, "Fourth-Generation Early Warning Systems," *Conflict Early Warning and Response*, available at http://earlywarning.wordpress.com/2009/03/06/fourth-generation-early-warning-systems/ .

every culture or group will have the same enthusiasm for embracing new technologies. Demographics, rural versus urban contexts, gender considerations, and generational factors will also play an important role. In addition, sometimes "old" technologies (or no technology) may be more appropriate and effective. In fact, many local-level projects appeared to work best when they combined old and new technologies—for example, by augmenting existing analog early-warning systems with digital components—and accompanied them with training and capacity building.

With this in mind, international organizations and governments should make needs assessments and feasibility studies standard practice to prevent the supply of technology from outstripping the demand.[5] Civil society organizations are generally closer to the ground and should have a better understanding of the context. However, very often they have no tools or resources for thorough assessments. They should include needs assessments or conflict and peace assessments that incorporate technological tools in their proposals when seeking funding from donors.

3. DO NO HARM.

Failure to consider the possible knock-on effects of applying a specific technology can lead to fatal outcomes in violent settings. Spoilers—whether in criminal gangs, rebel groups, or government agencies—can also leverage new technologies and the information they provide to incite violence, promote conflict, and perpetrate crimes. As the case studies demonstrated, restrictive governments can use information and communication technologies to prevent information from getting to one group in society and identify members of a dissenting group. Criminals and drug lords can use personal information obtained from websites to eliminate individuals that present a threat to their activities.

As such, human input, political awareness, and a conflict-sensitive approach remain vital from the conception of an initiative until long after its completion. Identifying the possible spoilers, conducting a cost-benefit analysis that incorporates levels of risk, developing mechanisms to mitigate risks, and creating contingency plans should be fundamental components of project design and implementation. Every actor seeking to apply new technologies to prevention initiatives should apply conflict-sensitive approaches and be aware of possible negative and knock-on effects emerging from their use of specific technologies.

4. INTEGRATE LOCAL INPUT THROUGHOUT, AND DON'T REINVENT THE WHEEL.

Once a project is underway, continual input from the local beneficiaries is vital to any attempt to use technology to support prevention efforts. The case studies show that interventions designed almost exclusively in a top-down manner are set up to fail. Examples abound where an absence of consultation with and involvement of the affected communities meant there was a lack of buy-in from those who were supposed to benefit, project financing was unsustainable, or the credibility of the information collected was questionable. In addition, insufficient awareness of or collaboration with existing initiatives can lead to a multiplicity of technological platforms and initiatives, as seen in Kenya. This can undermine the impact of prevention efforts, particularly when it means information does not get to the actors with the greatest ability to respond. In general, the application of new technological tools to prevention efforts at the local level works best when integrated into existing civil society initiatives.

5. USE TECHNOLOGY TO HELP INFORMATION FLOW HORIZONTALLY MORE THAN VERTICALLY.

Perhaps the most significant innovation created by advances in technology is the empowerment of individuals to participate in conflict-prevention initiatives in their own communities and societies. Governments and international actors have been collecting data and using technological tools to inform and implement policy and action for a long time. But since these tended to be large-scale, complex, and expensive endeavors, they remained the reserve of those in power. In addition, political decision-making processes remain largely disconnected from early warning and conflict-prevention

[5] For more on assessment tools for donors and international organizations, and the necessity of integrating a culture of analysis and contextualization, see Jenna Slotin, Vanessa Wyeth, and Paul Romita, "Power, Politics, and Change: How International Actors Assess Local Context," New York, International Peace Institute, June 2010.

mechanisms at the international level. Now, citizens can use digital technologies to more easily inform themselves and others, and to incentivize positive change in their communities and societies.

This information, spread horizontally, can be used to put pressure on local decision makers much more effectively than it can at the international level. In other words, it seems that new technologies have greater potential neither in "top-down" nor "bottom-up" mechanisms, but for "bottom-bottom" approaches. For the prevention of violent crime, the example of Latin America showed how horizontal citizen-to-citizen ICT initiatives are the most dynamic and promising.

Ultimately, facilitating the horizontal spread of ICT use for conflict prevention can help to connect more "warners" and "responders" more quickly, and contribute to communities' resilience in the long term. As such, international organizations should consider supporting the emergence of spontaneous micro-initiatives, provide funding to develop local capacity, improve connectivity among different initiatives, and help the sharing of best practices. Civil society organizations should identify and reward skilled individuals and groups in local communities who can adopt new technologies for preventing violence and conflict.

6. ESTABLISH CONSENSUS REGARDING OWNERSHIP, USE, AND SHARING OF INFORMATION.

Community participation alone may not always be enough to prevent a conflict, particularly when it comes to large-scale collective violence and war. New technologies make it possible for international organizations and government agencies to acquire more information and more granular information to inform prevention efforts—whether this data is voluntarily given in the form of citizen reporting, harvested from the data deluge online, or collected using new surveillance technologies.

But much more work is needed to identify the levels of trust, transparency, and control that individuals, businesses, and governments are willing to accept when it comes to sharing data via digital technologies in a context of violence and conflict. As evidenced in Kenya, suspicion and distrust of national police and security establishments may have contributed to communities' reluctance to share information for early warning with the National Steering Committee. In the Latin America case, it was clear that citizens were more likely to report crime if they felt confident they could do so anonymously. And in Sudan, there were indications that when communities understand what their information is going to be used for, they may be more willing to participate.

International organizations, governments, and civil society actors should establish consensus around questions of around privacy, access, and use of digital data in any given initiative. This will make prevention efforts more legitimate in the eyes of affected communities, and ultimately more effective.

7. FOSTER PARTNERSHIPS FOR BETTER RESULTS.

Partnerships will be essential for the effective application of new technologies for preventive ends. There are indications that prevention initiatives that drew on the complementary strengths of international donors, governments, the private sector, and civil society proved more effective. Indeed, in some contexts donors may need to sacrifice visibility for the sake of effectiveness. This is particularly true when the use of new technologies to gather data in a politically charged context is seen as external meddling or even spying, which can de-legitimize and undermine the endeavor, if not kill the initiative completely. The need for partnership in the realm of big data is particularly acute given the array of actors involved in extracting actionable information from the data deluge—private companies that hold the data, academics and technical experts who can analyze it, civil society actors who can put it in context, and governments and international bodies that can regulate its use and incentivize cooperation. International organizations and governments are well placed to foster such partnerships and should invest in doing so for more promising results.

***

At this early stage in the consideration of new technology's role in preventing violence and conflict, it is only possible to sketch out very tentative conclusions. The application of new technologies to conflict-prevention efforts has yet to show robust results. Most of the analysis points to the potential rather than the current reality, although there have been some significant, positive indicators at the local level in particular. Continued, extensive research and systematic evaluation are needed for a deeper understanding of the realities as well as the possibilities.

Yet, many "traditional" conflict-prevention initiatives also aren't producing the outcomes desired. With or without new technology, this is particularly true when it comes to bridging the gulf between warning and response. Beyond examining the provision of warning or identification of conflict drivers, further research into technology's impact on response could be the most helpful for the field of prevention as a whole. This could include assessing how ICT can be used to generate incentives for action, which seems to be more promising at localized level, and to link decision-making processes with early-warning and conflict-prevention mechanisms. And given the huge pools of information that now need to be analyzed for actionable information, governments and international actors also need to invest heavily in analytical capabilities at local, national, and international levels.

There is a real risk that applying new tools to a system that already struggles to meet its goals may not get much further than a Band-Aid effect. But the increased horizontal spread of new technologies across societies has the potential to revolutionize these traditional systems by making more information available to more people. This not only makes it harder *not* to do something when violence or conflict appears imminent, it also makes response more likely because it empowers local actors—who are closer to the crisis—and creates incentives to take action. Given the frequent paralysis at national and international levels when it comes to taking action to prevent conflict, this "bottom-bottom" approach may be even more important in the short term than the "bottom-up" tactic of raising voices to national and international levels.

In the long run, however, the most effective approach to using new technologies for conflict prevention may well be the approach needed in prevention more broadly: one that successfully balances both grassroots, decentralized efforts and the more rationalized and coordinated activities of governments and international organizations.

Annex
Members of the Expert Reference Group

Jenny Aulin
Program Manager, Preventive Action and Human Security Global Partnership for the Prevention of Armed Conflict

Rob Baker
Senior Program Developer, External Projects Team, Ushahidi

Brendan Ballou
Google Ideas

Michael L. Best
Associate Professor and Program Director, Information and Communication Technology for Development, Sam Nunn School of International Affairs, School of Interactive Computing, George Institute of Technology

George Chamales
Rogue Genius LLC

Alexa Courtney
Executive Vice President, Caerus Associates

Gustavo Diniz
Research Associate, Igarapé Institute

Scott Edwards
Managing Director, Tactical Response, Advocacy, Policy, and Research Department, Amnesty International, USA

Simone Eymann
Intranet Project Manager, Policy and Mediation Division, United Nations Department of Political Affairs

Lt. Colonel David Foster
Plans and Operations Officer, United States Army

Christina Goodness
Acting Chief, Peacekeeping Information Management Unit, Office of the Chief of Staff, United Nations Department of Peacekeeping Operations/Department of Field Support

Bernard Harborne
Lead, Violence Prevention Team, The World Bank Group

Travis Heneveld
Account Director United Nations, Motorola Solutions

Joe Hewitt
Team Lead, Technical Leadership Team, US Agency for International Development

Anne Kahl
Program Specialist, Conflict Prevention, Bureau for Crisis Prevention and Recovery, United Nations Development Programme

Tim Kelly
Lead ICT Policy Specialist, infoDev, The World Bank Group

Nirina Kiplagat
Program Officer, Peacebuilding and Conflict Prevention Unit, United Nations Development Programme, Kenya

Robert Kirkpatrick
Director, Global Pulse

Helena Puig Larrauri
Consultant, United Nations Development Programme

Emmanuel Letouzé
Consultant, United Nations Office for the Coordination of Humanitarian Affairs; Consultant, Organisation for Economic Co-operation and Development

Matthew Levinger
Director, National Security Program, Elliot School of International Affairs, The George Washington University

Rachel Locke
Conflict Adviser, Office of Conflict Management and Mitigation, USAID

Francesco Mancini
Senior Director of Research, International Peace Institute

Anna Matveeva
Senior Visiting Research Fellow, Department of War Studies, King's College London

Patrick Meier
Director of Social Innovation, Qatar Foundation, Computing Research Institute (QCRI)

Robert Muggah
Research Director and Program Coordinator for Violence Reduction, Igarapé Institute

Godfrey Musila
Consultant and Director, African Center for International Legal and Policy Research (CILPRA), Nairobi; Visiting Lecturer, LLM in International Criminal Justice, Open University of Tanzania

Ozonnia Ojielo
Coordinator, Conflict Prevention Team, Bureau for Crisis Prevention and Recovery, United Nations Development Programme

Jorge A. Restrepo
Associate Professor of Economics, Pontificia Universidad Javeriana; Director, Centro de Recursos para el Análisis de Conflictos, Colombia

Nigel Snoad
Product Manager, Crisis Response, Google

William Tsuma
Dialogue Financing Facility Adviser and Programme Specialist, United Nations Development Programme, Zimbabwe

Katrin Verclas
Co-founder and Editor, MobileActive.org

Zab Vilayil
Conflict Early Warning Systems Consultant

Patrick Vinck
Director, Program for Vulnerable Populations, Harvard Humanitarian Initiative

Raúl Zambrano
Global Lead/Senior Policy Adviser, ICTD and e-Governance, Bureau for Development Policy, Democratic Governance Group, United Nations Development Programme

The **INTERNATIONAL PEACE INSTITUTE** (IPI) is an independent, international not-for-profit think tank with a staff representing more than twenty nationalities, with offices in New York, facing United Nations headquarters, and in Vienna. IPI is dedicated to promoting the prevention and settlement of conflicts between and within states by strengthening international peace and security institutions. To achieve its purpose, IPI employs a mix of policy research, convening, publishing, and outreach.

IPI

INTERNATIONAL
PEACE
INSTITUTE

777 United Nations Plaza
New York, NY 10017–3521
USA
TEL +1-212 687-4300
FAX +1-212 983-8246

Freyung 3, 1010
Vienna, Austria
TEL +43-1-533-8881
FAX +43-1-533-8881-11

www.ipinst.org