STABILITY Mancini, F and O'Reilly, M 2013 New Technology and the Prevention of Violence and Conflict. *Stability: International Journal of Security & Development,* 2(3): 55, pp. 1-9, DOI: http://dx.doi.org/10.5334/sta.cp

RESEARCH ARTICLE

New Technology and the Prevention of Violence and Conflict

Francesco Mancini* and Marie O'Reilly†

Amid unprecedented growth in access to information communication technologies (ICTs), particularly in the developing world, how can international actors, governments, and civil society organizations leverage ICTs and the data they generate to more effectively prevent violence and conflict? New research shows that there is huge potential for innovative technologies to inform conflict prevention efforts, particularly when technology is used to help information flow horizontally between citizens and when it is integrated into existing civil society initiatives.[1] However, new technologies are not a panacea for preventing and reducing violence and conflict. In fact, failure to consider the possible knock-on effects of applying a specific technology can lead to fatal outcomes in violent settings. In addition, 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.

Introduction

There are now 6 billion cell phone subscriptions in the world, and one third of the world's population is online (ITU 2012). These numbers are growing rapidly, particularly in the developing world, and they demonstrate an unparalleled level of global interconnectivity. 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.

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 (ITU 2010), the amount and variety of data produced is a phenomenon of historical significance. It is estimated that we now produce more data every year than in all previous years combined (O'Reilly 2012).

It is with these trends in mind—the increasingly rapid global interconnectivity, the growing access to mobile devices globally, and the generation of an unprecedented quantity of

* Senior Director of Research, International Peace Institute, New York, United States
mancini@ipinst.org

† Associate Editor, International Peace Institute, New York, United States
oreilly@ipinst.org

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 Conflict Management and Mitigation, launched a project to investigate the potential role of new ICTs in conflict prevention. The project benefited from the inputs and insights of a small group of experts from academia, think tanks, the private sector, and the field.

The resulting report, *New Technology and the Prevention of Violence and Conflict*, whose findings we are sharing in this article, explored 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.[2] It examined 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 by independent experts assessed 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).

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 significantly, as is the nature of conflict and violence. The number of interstate and civil wars has declined worldwide, and these conflicts produce fewer battle-related deaths. On the other hand, violence linked to local disputes, organized crime, and political repression is far more pronounced (World Bank 2011). Overall, the case studies demonstrated 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 Different Contexts

Before identifying cross-cutting recommendations for the more effective use of new ICTs in conflict prevention, it is worth highlighting the lessons learned from different contexts and tools.

Criminal violence. 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 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.

Election-related violence. As the richest country in East Africa and one with recent outbreaks of election-related violence, Kenya is an interesting example of a country where national institutions have pioneered the use

of innovative ICT for conflict prevention as technology penetration rates increase. Yet, despite many innovative applications of new technologies to early-warning initiatives in particular, there is a persistent gap between warning and response in Kenya. Kenya's national conflict early-warning system connects to the regional system known as CEWARN. This tool allows information collected partly using digital devices to make its way up from the local to the state and regional levels. But when response is not forthcoming, nonstate actors at the community level cannot access the information to close the warning-response gap. In addition, top-down approaches in Kenya have sometimes lacked transparency and accountability. This has led to suspicion on the part of those giving over their information, reducing the credibility of the data and the effectiveness of the undertaking. At the same time, the choice of technology used for prevention activities sometimes appears to be supply-driven as opposed to demand-driven. One conflict-prevention initiative in Kenya 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.

Violent crisis. A gloomier assessment emerged from the analysis of new technology's role in violent riots that broke out in Kyrgyzstan in 2010. In a context where the government restricted the use of new technology, ICTs appeared to do little to facilitate a response from local authorities or 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.

Armed conflict. 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.

Big data. In a variety of contexts, much has been made of the potential for big data analytics to inform development strategies, but it also has significant potential for preventing violence and conflict. 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. It could serve descriptive, predictive, and diagnostic functions for conflict prevention. 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 (Croll 2012). 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.

How-To Guide: Leveraging New Technology for the Prevention of Violence and Conflict

The diversity and changing nature of conflict settings 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, such as Kenya, may have limited impact in an environment where governments act precisely to restrict such information flows, as happened in Kyrgyzstan. 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.'[3] 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 settings 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.

That said, the lessons emerging from these case studies, the insights of the experts involved in the project, and the analyses of the authors suggest a number of steps that those using innovative ICTs 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 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.[4] 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. Today, citizens with mobile phones, cameras, videos, and Internet access can contribute greatly to early warning by 'getting the word out' to a larger audience. International civil society groups and advocacy groups also draw on this digital deluge—along with other data-driven evidence and satellite images—to pressure international actors and Western governments to respond.

However, this technology-driven information overload does not always facilitate timely or appropriate action. In fact, political decision-making processes at the international level remain largely disconnected from early warning and conflict-prevention mechanisms. Reams of digital evidence can contribute greatly to postconflict justice and accountability mechanisms. But when it comes to prevention, the international warning-response gap persists even if information about violence and mass atrocities abounds (O'Reilly 2013).

To close the gap, citizens in conflict settings can use digital technologies to more easily inform themselves and those who are better placed to respond more quickly at the local level. This information, spread horizontally, can be used to put pressure on local decision makers much more effectively than it can at the international level. 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. Over the long term, citizens can also use digital tools and platforms to incentivize positive change in their communities and societies. In other words, it seems that new technologies have greater potential neither in 'top-down' nor 'bottom-up' mechanisms, but for 'bottom-bottom' approaches.

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 individu-

als 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 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 delegitimize 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.

Conclusion

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 a localized level, and to link decision-making processes with early-warning and conflict-prevention mechanisms. And given the huge pools of data 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.

Notes

[1] This article is based on the following report: Mancini, F (ed.) 2013. *New Technology and the Prevention of Violence and Conflict*. New York: International Peace Institute.

[2] The present article is a condensed version of the introduction and conclusion of this report (Mancini 2013).

[3] For an explanation of the 'generational' approach to technology in early warning and response, see the chapter on big data in Mancini 2013. See also Meier 2009.

[4] For more on assessment tools for donors and international organizations, and the necessity of integrating a culture of analysis and contextualization, see Slotin et al 2010.

References

Croll, A 2012 Big Data is Our Generation's Civil Rights Issue, and We Don't Know It. In: *Big Data Now*. Sebastopol, CA: O'Reilly Media.

International Telecommunication Union 2010 *The World in 2010: ICT Facts and Figures.* Available at www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

International Telecommunication Union 2012 *ITU World Telecommunication/ICT Indicators Database 2012.* Available at www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf.

Mancini, F (ed.) 2013 *New Technology and the Prevention of Violence and Conflict*. New York, NY: International Peace Institute.

Meier, P 2009 Fourth- Generation Early Warning Systems. *Conflict Early Warning and Response.* March 6. Available at http://earlywarning.wordpress.com/2009/03/06/fourth-generation-early-warning-systems/.

O'Reilly, M 2013 In Syria, to End Mass Atrocities, World Watching Is Not Enough. *The Global Observatory*. August 12. Available at http://theglobalobservatory.org/analysis/557-syria-end-mass-atrocities-world-watching-not-enough.html.

O'Reilly, M 2012 Robert Kirkpatrick, Director of UN Global Pulse, on the Value of Big Data. *The Global Observatory*. November 5. Available at www.theglobalobserva-

tory.org/interviews/377-robert-kirkpatrick-director-of-un-global-pulse-on-the-value-of-big-data.html.

Slotin, J, Wyeth, V, and **Romita, P** 2010 *Power, Politics, and Change: How International Actors Assess Local Context.* New York: International Peace Institute.

World Bank 2011 *World Development Report 2011: Conflict, Security, and Development.* Washington, DC: The World Bank.

How to cite this article: Mancini, F and O'Reilly, M 2013 New Technology and the Prevention of Violence and Conflict. *Stability: International Journal of Security & Development,* 2(3): 55, pp. 1-9, DOI: http://dx.doi.org/10.5334/sta.cp

Published: 29 October 2013