Today’s Digital Witnesses Can Prevent Tomorrow’s War Crimes Robert Muggah OpenCanada.org

21 April 2014

War crimes and mass atrocities are reported not just by journalists, aid workers, and survivors on the frontlines, but also by thousands of advocates around the world. The twenty first century is giving rise to collaborative conflict prevention and digital witnessing. Concerned citizens are using satellite maps, (big) data scraping systems, and crowd sourcing technologies to report on war crimes and mass atrocities in real time. A growing cadre of scholars, practitioners, and hobbyists are leveraging new tools to disrupt genocidal violence. While such technologies on their own are no panacea, they offer a means to prevent gross violations of human rights and holding perpetrators to account after heinous crimes are committed.

Arguably one of the most revolutionary societal transformations of the past two decades is the advent of mobile technology and increased Internet connectivity worldwide. More than 6 billion people now have access to mobile phones and 2.5 billion are connected to the Web resulting in previously unthinkable expressions of empowerment. These and other information communication technologies (ICTs) are literally redefining the space in which authoritarian regimes, rebel groups, and criminal organizations can act with impunity. Virtual tools such as remote sensing systems and spatial mapping are exposing mass violence where physical access was previously limited. Many of these innovations emphasize decentralized collaboration and open source software, allowing for constant improvement, adaptation, and replication. Although questions over the management and curation of sensitive data remain, the emergence of these ICTs is re-shaping the landscape of conflict prevention.

There is growing appetite among governments and United Nations agencies to improve their ability to predict, prevent, and punish war crimes and mass atrocities. A **first generation** of early-warning systems designed to protect civilians from extreme violence emerged after the failure to prevent the Rwandan genocide of 1994. Many early innovations were taken up by inter-governmental, multilateral and bilateral agencies. A **second generation** of crisis mapping and prevention tools was spawned a decade later owing to widespread improvements in digital connectivity, cloud computing, and the proliferation of ICTs. The most prominent of these are Ushahidi, Frontline SMS, and other crisis mapping platforms. Both grassroots organizations and individuals are deploying these new tools in conflicts and humanitarian crises around the world. There is also a **third generation** of emerging digital systems that are providing 24/7 surveillance in the world's hotspots through a combination of earlier methods together with Big Data analysis and drone surveillance.

The most widely recognized wave of early warning systems emerged in the wake of explosive election violence in Kenya in 2008. The aforementioned Ushahidi system was novel in that it was developed not by governments, international agencies, or the private sector but by a collaborative team of activists and programmers. Their primary innovation is the integration of standard SMS/text messaging, social media platforms, crowd-source mapping, and other tools to spatially and temporally map violence. Since 2008 there has been a proliferation of conflict prevention tools fusing multiple data sources—from sentinel surveillance, crowd-sourced information, and interactive maps—into a "firehose" that allows analysis to be rapidly developed and disseminated. The Harvard Humanitarian Initiative, for example, has pioneered the development of data fusion centers that can monitor troop movements and anticipate likely attacks by drawing upon satellite imagery and remote sensing.

At the same time, contemporary early warning systems are harnessing the power of cloud computing, masses of raw unfiltered data, and new mobile surveillance systems. Computer scientists working with multinational firms such as Google Ideas and Microsoft are learning how to use Big Data to predict political and criminal violence, including the tracking millions of data points in social media and search engines. Universities and research groups, including Canadian entities such as the SecDev Foundation and the Digital Mass Atrocity Prevention Lab are developing platforms to track security and censorship from Colombia to Syria. At the vanguard of these efforts are initiatives such as GDELT, a global data set that includes hundreds of millions of variables harvested from over 300 (micro) news outlets spanning four decades.

While still largely the preserve of governments and private corporations, a new class of technologies—including unmanned areal vehicles (UAVs)—promises to dramatically restructure approaches to early warning. For example, UAVs are being equipped with high-resolution cameras to track movements of “enemy combatants” around the world. But there is also enormous potential to use them in humanitarian contexts. There is some evidence of this already taking place, with drones used in peace support operations in Bosnia in the early 1990s and more recently deployed in the Central African Republic, the Democratic Republic of the Congo , and Haiti . Rather than distributing messages and warnings through radio and pamphlets, peacekeepers, and relief workers are turning to social media and directed targeting through telecommunications systems instead.

So what is really new about the advent of these new technologies? Across all three generations of the technology, specialists are still fundamentally preoccupied with improving their predictive capacities and protecting civilians. Yet something is changing. The explosion of data and ICTs is offering improvements in the accuracy, scale, timing, and diffusion of real time analysis. The last decade has generated an unfathomable array of data sources —from satellite images and social media to stock market indexes and search engines. The sample size for analysis has expanded from a representative cross-section of a given population to its entirety. Whereas early warning tools from the 1990s could generate predictions two to four weeks ahead, today’s platforms offer real-time geo-tagged information in seconds. What is more, the nearly ubiquitous use of mobile phones means that unfiltered information can also be disseminated directly to end users. Furthermore, data can be encrypted and sent anonymously to protect individuals on the ground.

The conflict prevention and early warning sectors are actively reflecting not just on the breathtaking potential of these new technologies, but the ethos that gave rise to them in the first place. A signature feature of new technologies is their “openness,” a characteristic acknowledged by specialists in the aid world. Many of these new tools were developed on the basis of a collaborative approach and partnerships and not in secret by private firms or government agencies. Those responsible for developing and applying them are more comfortable working in horizontal networks than vertical hierarchies. They also purposefully draw from a range of disciplines to improve their products, pulling in the required expertise on demand. And they prefer rapid iteration in testing out their products rather than long, drawn-out pilots. Importantly, they embrace the possibility of failure and are incentivized to take risks.

Those involved in tracking mass atrocities and war crimes have an extraordinary opportunity to become early adopters of these new tools and techniques. Yet technology is not a solution in and of itself. Indeed, new technologies can themselves be used to perpetrate organized violence. Researchers have already found that cell phone coverage can also generate negative externalities, including facilitating violent collective action. Governments and non-state groups are also reliant on communications to coordinate and monitor potential targets. Security forces, rebel groups and militia can and do intercept messages, underlining the importance of encryption and anonymity in today's war zones. There is also the risk of some involved in the early warning business of fetishizing new technology and unintentionally expanding the distance between observers and victims. Nevertheless, its effective use can play an important enabling function and improve the pace and precision of prevention.

Technology cannot be treated as an "add-on" and relegated to peripheral departments of human rights organizations and advocacy groups. Obviously, some organizations will do better than others in taking up this challenge. Indeed, there is no blueprint for how best to take advantage of these new high-tech tools. Part of the reason for this is that the pace of change is taking place at breakneck speed. Some organizations may continue successfully using first- and second-generation approaches owing to weak Internet connectivity, while others may combine elements of all three to useful effect. But with so much innovation bubbling up, identifying and scaling-up the most promising technologies is hugely important and impactful. To innovate successfully will require a change in mindset but also an upgrading of capacities. It will also demand a greater tolerance of risk and uncertainty. Most of all, it will demand bridging the gap between technology-enabled early warning and political will to do something about the rapidly revealed facts on the ground.

See the original article here.