Mob Violence, Mobile Phones
Private Messaging and the Future of Peacekeeping
Mob Violence, Mobile Phones
Private Messaging and the Future of Peacekeeping

APRIL 2019

Elizabeth Sutterlin
**Mob Violence, Mobile Phones:**
Private Messaging and the Future of Peacekeeping

*Peer-to-peer mobile communications are a blind spot for peacekeeping operations in conflict-prone areas. Increased access to cheap mobile phones has allowed misinformation to spread quickly via direct messaging platforms. People are prone to believe private messages from their peers that contain sensational rumors. The more widely these messages spread, however, the greater their risk of inciting violence. Without a strategy to monitor inflammatory rumors on peer-to-peer digital platforms, future peacekeepers will be hampered in their ability to prevent conflict and protect civilians. To address this challenge, the UN should expand the responsibilities of locals acting as community liaison assistants (CLAs) to include gathering information from digital peer-to-peer networks. By expanding this role, rumors on digital platforms will be identified and shared with peacekeepers by CLAs before messages incite violence.*

**Introduction**

Mobile phones have dramatically reduced the cost of interconnectivity over the past 15 years. Cell phone ownership is now a possibility for millions in the developing world because of lower cost and more capable mobile communications technology. While many scholars, policymakers, and aid workers are optimistic about the promise of cell phones to improve the lives of impoverished people around the world, the security concerns that accompany this technology have been largely ignored.

Messages shared over short messaging services (SMS), like WhatsApp and other private channels, may act as a powerful catalyst for violence. By decreasing the costs of communication and increasing the frequency and reach of contact, instant messaging intensifies a community’s existing rumor dynamics and can deepen wedges between social groups. High speed communications reduce the coordination costs of actors who aim to punish minorities for perceived social injustices. The newfound frequency with which rumors circulate make them more believable to the wider public, providing a motive to carry out attacks and further fueling community divisions.¹

This problem will be particularly challenging for peacekeepers. Under-resourced UN forces already operate in environments where reliable information can be hard to collect and share. These forces will struggle to ensure peace and protect civilians when faced with violence driven by misinformation on private, often encrypted networks.
Mobile Technology and the Future of Peacekeeping

Since the inception of UN peacekeeping operations, new threats from non-state actors have prompted a gradual shift towards more expansive and robust mandates. Today’s peacekeeping operations encompass far more than just security support through the peacebuilding process. They now take on a variety of complicated tasks to assist countries as they transition into post-conflict reconstruction. Peacekeepers work to facilitate a fair political process, organize elections, protect civilians, promote human rights, restore rule of law, and disarm, demobilize, and reintegrate former combatants after conflicts.

These new, more expansive mandates require more resources and support from UN member states. This need is only intensified by technological changes that have produced new challenges in conflict and post-conflict environments. Violence spread via mobile phone messaging is one such challenge.

Inflammatory cell phone messages that lead to more widespread ethnic violence are not a critical threat to U.S. national security on their own. However, outbreaks of violence resulting from these messages have the potential to reignite conflicts that will fuel refugee flows in strategic regions for the United States. This dynamic was in evidence in Myanmar in 2017, when Facebook and other digital platforms played a significant role in ethnic cleansing against the Rohingya minority. Online rumor-mongering and the rapid sharing of information were used to endorse and encourage physical violence, which has caused nearly 700,000 of the Rohingya to flee Myanmar for neighboring Bangladesh. Such violence also can promote extremism that will have long-term security implications for the United States. Multilateral peacekeeping missions will be required to address the threat of low-level conflicts and creeping instability. Maintaining the ability of peacekeepers to respond effectively to mob violence incited by rumors on mobile phones, therefore, should be a priority for the international community.

The Spread of Mobile Technology and Ethnic Mob Violence

*Rumor, the swiftest of all evils. Speed lends her strength [...] She affrights great cities, clinging to the false and wrong, yet heralding truth.*

--The Aeneid, Book 4, Line 173

Mobile phones have made it easier than ever before to spread rumors that incite and encourage violence. In India in 2015, villagers dragged a man out of his home and lynched him in the street after a rumor circulated on WhatsApp that he had killed a cow and eaten beef. In 2017, rumors of a gang of child kidnappers spread quickly across rural Indian states, turning frightened villagers into mobs. Outsiders were quickly identified by their ethnolinguistic backgrounds and severely beaten and burned on suspicion of kidnapping. The rumor left seven dead in two separate mob incidents within hours.
How Mobile Phones Incite Ethnic Violence

This phenomenon is not limited to any one country or region. Mobile-based rumors led to violence in at least eight countries over the last eleven years. There are many factors that make mobile communications a potent tool for fostering ethnic violence and unrest. This analysis focuses on three factors: (1) the speed and frequency of mobile communications, (2) mass forwarding on platforms and the power of direct messaging, and (3) the social structure of peer-to-peer platforms.

- **Frequency and Speed of Mobile Communications.** As mobile phones become cheaper, communication costs fall and the frequency with which communities can share information among themselves and with others rises. According to the international development literature, greater access to communication generally has positive outcomes; for instance, many farmers have benefited from better knowledge of weather and market conditions.9 But the increase in communication frequency also boosts the speed and ease with which groups can garner support or mobilize against a scapegoat.10 Instant messages and group chat functions decentralize group structures and make group coordination easier.11 Further, the popular forwarding functions for SMS and instant messages increase the size of audiences who receive a rumor.12

- **Mass Forwarding and the Power of Direct Messaging.** The forwarding function of these private, peer-to-peer communication channels presents a different dynamic than that of social media platforms. Posts made on social media platforms are directed at a wide audience of friends and followers, rather than sent directly to individuals.

When it comes to mobilizing people, or activism on a local level, researchers have shown that direct text messaging often can far outpace other methods of outreach in effectiveness.13 Yale University’s Institution for Social and Policy Studies has analyzed get out the vote (GOTV) field experiments and found significant evidence that personalized messages are more effective than wider messages.14 When making the choice about how to best reach people with political messaging, many American campaign organizers have returned to direct messages or SMS texts rather than advertisements on social media since 2016. Political strategists have referred to sites like Facebook and Twitter as “crowded,” and consider text messages a promising alternative due to their high read rate.15 Some consider peer-to-peer communications to be “the best tool right now for getting out the vote.”16

A natural extension of this finding is that direct text messaging may be a more effective method for inciting violence.17 Although there have been many cases of public social media sites stoking discontent, fostering ethno-nationalism, and encouraging violent action, the less visible but equally if not more insidious network of peer-to-peer communications has its own potential to sow distrust between divided groups in a society, ultimately pushing individuals towards violence.
• **Obscured Authorship.** Another important difference between social networks and peer-to-peer communications is that even when posts are shared among individuals or small groups, social media platforms preserve the identity of the original post author. Forwarded texts or WhatsApp messages instead appear as though the forwarder is the original author. This poses an accountability problem, as the original authors of inflammatory messages can be difficult to identify.¹⁸ Rather than seeing that one’s family member or friend is sharing a message written by a stranger, recipients believe that the friend or family member wrote the message themselves.

The ability to forward WhatsApp messages without a record of their original authors is of major significance. Research in the field of psychology has shown that individuals are more likely to trust those who are like them or close to them.¹⁹ Research has shown that the identity of who shares a post with friends and family influences how believable and trusted the message is—a forwarder matters. Forwarded messages from a family member, close friend, or community member will evoke more of a response than one from a stranger.²⁰ Peer-to-peer communications thus nurture tendencies for intra-group trust and inter-group distrust.

• **Social Structures on Peer-to-Peer Platforms.** Proponents of using technology for greater social interconnectedness have viewed mobile phones with optimism—with the dawn of the internet, the opportunities for cross-cultural, transboundary communication, whether social or geographic, seemed more numerous than ever. In practice, however, private messaging channels are often used to reinforce tribalistic trust dynamics in divided societies.²¹ This system cultivates relationships within existing social groups and does not forge new ties across different groups.

Private messaging platforms further strengthen bonds among like-minded people in their own social groups, and actors who wish to spread rumors can capitalize on these ties. Misinformation that confirms one group’s worldview goes unquestioned and escalates tensions as it is forwarded rapidly across a messaging platform. The dynamics of intragroup trust and the way information is shared across these peer-to-peer platforms promote ethno-nationalism and intolerance as they enforce existing social circles. While drastic decreases in communication costs have provided people with the ability to mobilize and pursue collective action much more easily than in the past, it is the dangerous dynamics of these messaging channels that funnel mobilization efforts toward mob violence and vigilante attacks on minority groups.

As information and communication technologies like mobile phones become more widely available, the phenomenon of mobile phone-based, rumor-driven violence will only grow in scale. This emerging trend has already become more pronounced over the past ten years, since the introduction of cheap cell phones to the market in the mid-2000s.
Evidence of Growing Rumor-based Violence

To analyze the growth of rumors linked to violence spread via cell phone, this analysis provides a count of violent incidents linked to both rumors and cell phones. It also points to eight high-profile cases where widespread violence can be directly attributed to rumors or misinformation spread on peer-to-peer messaging platforms.

Event Count Data

A review of news articles in the LexisNexis database from 2013 to 2019 found a clear increase in reports of violence fueled by messages on mobile phones. In 2013, one instance of mobile phone fueled violence was reported in the news media. In 2016, instances of mobile phone fueled violence began to increase. This trend continued into 2017 and 2018, with the number of instances rapidly growing from 2 to 5 in 2017 and then from 5 to 28 in 2018.

Figure 1: New Media Reference to Mobile Phone Fueled Violence

<table>
<thead>
<tr>
<th>Year</th>
<th>Violent Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>1</td>
</tr>
<tr>
<td>2014</td>
<td>0</td>
</tr>
<tr>
<td>2015</td>
<td>0</td>
</tr>
<tr>
<td>2016</td>
<td>2</td>
</tr>
<tr>
<td>2017</td>
<td>5</td>
</tr>
<tr>
<td>2018</td>
<td>28</td>
</tr>
</tbody>
</table>

High-Profile Incidents

Eleven heavily reported instances of mobile peer-to-peer platforms inciting widespread violence have occurred in the past eleven years. In addition to the eight cases discussed below, peer-to-peer rumor mongering has also occurred in Bangladesh, Nigeria, and the Central African Republic.

- Kenya, December 2007 - February 2008: After a highly contested presidential election between President Mwai Kibaki and opposition leader Raila Odinga, both candidates declared themselves the winner. Odinga, a member of the Luo ethnic group, announced his victory first in a public briefing, but shortly afterwards the Electoral Commission released results that put Kibaki, an ethnic Kikuyu, ahead by 200,000 votes. Odinga accused the Commission of fraud and doctoring the results of the election, but Kenya’s internal security minister announced a five-day ban on live broadcasts shortly after the updated election results were released.
During the ban, Kenyans moved to SMS messaging to keep up with the news about the election outcome. Mass text messages aimed at inciting ethnic violence against the Kikuyu began to spread throughout the country. Another mass message encouraged the Kikuyu to slaughter others in Nairobi. The two months of ethnic violence that passed before Kibaki and Odinga signed a power-sharing agreement left over 1,500 people dead and 500,000 displaced. This case highlights the effect of a mass media blackout on misinformation, rumors, and ultimately, violence.

- **Kyrgyzstan, March - June 2010**: Due to high government control of mass media, citizens opposed to the government moved to the internet to escape censorship. The reach, anonymity, and ease of use that mobile phones offered made them a key tool for the opposition in the Second Kyrgyz Revolution. Over SMS messages and platforms like Twitter, the opposition organized protests and coordinated support. New media shared and accessed on mobile phones was a space for citizen journalism in March and April.

After the removal of President Bakiyev (a shared enemy) in April, however, the online community began to splinter along preexisting societal cleavages. Throughout the months of May and June, new media became polarized as online platforms were used to spread opposing narratives and undermine other groups. This polarization led to violence when ethnic Kyrgyz and Uzbek populations in the southern part of the country clashed in the wake of the revolution. The months of violence resulted in the deaths of between 893 and 2,000 people and the displacement of 400,000 people.

- **India, 2017 - 2018**: The first reports of an online rumor-driven mob lynching in India appeared in 2017, but it was not until the summer of 2018 that the phenomenon became a widespread problem and perhaps the most internationally well-known case of online rumors fueling ethnic mob violence. One WhatsApp message circulated in Madhya Pradesh claimed that people disguised as beggars were roaming the countryside to kill people for their organs. Another message in Tamil Nadu warned of child kidnappers on the prowl, which led a mob to attack a tourist who was seen distributing chocolate to local children. As of June 2018, a dozen people had been beaten by mobs for accusations spread on WhatsApp and other messaging platforms. India’s mob attacks target those who are identifiable others—including tourists, migrant workers, and Muslims in predominantly Hindu areas.

Police efforts to counter rumors with public announcements and information were largely unsuccessful. The government blamed the design of social media platforms, especially WhatsApp, for the outbreak of violence. Several WhatsApp groups were deleted after the attacks, and the company began an advertising campaign to help users distinguish between real and false information on its site. The company has also beta tested a change that would flag all forwarded messages, but it does not intend to make any changes to its data encryption methods.
• **Mexico, September 2018:** Mob violence has long existed in Mexico, due to high levels of crime, ineffective policing, and the sense that lawbreakers escape punishment. Mexican law enforcement officials are concerned that rumors spread on messaging platforms are exacerbating the problem. There have been at least 142 recorded mob lynchings in Mexico since 2017, which have been responsible for the deaths of 25 people and the injuries of many others.

A particularly egregious case occurred in September in Puebla state, when two men traveling to a nearby village were lynched, beaten, and burned to death on accusations of kidnapping. Rumors had been circulating that a pair of kidnappers (robachicos) were removing organs from children to sell on the black market. Six states had issued public announcements before the mob attack, warning that the fast-spreading, countrywide stories of kidnapping rings were false, but action was not swift enough to prevent the violence. The two innocent men were burned alive in front of a local police station. A representative from WhatsApp, where the kidnapping rumors went viral, announced the company’s plans for a Spanish-language advertising campaign designed to teach tips for spotting misinformation on its platform, similar to the one it conducted in India.

• **Sierra Leone, March 2018:** Rumors played an important role in the lead-up to Sierra Leone’s elections, despite the country’s low internet and messaging app penetration. After the first round of the 2018 elections, the two lead candidates were separated by less than 1 percent after the National Electoral Commission (NEC) had reported 75 percent of the votes. The tight race meant there would likely be a second-round runoff, but a falsified report circulated on WhatsApp claimed that the opposition candidate Maada Bio had received 56.3 percent of the vote, just above the 55 percent threshold for victory. While the message contained several inaccuracies, including a listed date six months in the future, the rumor still circulated widely and was spread via word of mouth to those with no phone or Internet access. Another rumor spread while the last 25 percent of the ballots were being counted that each candidate had received identical numbers (249,000 each) from the final portion. Even party officials were susceptible to the rumor and accused the NEC of fraud.

• **South Sudan, 2018:** Only about 20 percent of South Sudan has access to the internet, but that access is almost entirely though mobile phones. Because of the country’s near total media blackout and the reliance on mobile phones for information, the diaspora has a large influence on the news heard by those in the country. Hate speech spreads rapidly through personal and family networks, from the diaspora to the South Sudanese population.

An organization analyzing hate speech on social media in the country found digital bigotry to be closely associated with targeted ethnic rapes and killings. In one high-profile incident, after the president removed the head of the army, Facebook users began spreading rumors that the president had been assassinated and that a militia loyal to the former army chief was assembling in the city of Aweil. As the rumors spread unchecked, messages on online platforms caused mass panic about the likelihood of an ethnic military coup.
• Sri Lanka, March 2018: Rumors spread on mobile phones have brought existing tensions between the Sinhalese Buddhist majority and Muslim minority to a boil in Sri Lanka. In the village of Mullegama, a Buddhist mob attacked Muslim residents, accusing them of stealing from temple donation boxes, and burned down twenty Muslim homes. The situation quickly devolved after subsequent rumors that a group of Muslim men had killed a Sinhalese man. In the first state of emergency since the civil war, riots broke out in which 150 houses and vehicles were destroyed. As ethnic attacks multiplied, the government tried to shut down access to social media services, claiming that the platforms were amplifying hate speech.

• Sudan, 2018: The Sudanese government has significantly restricted mainstream and mass media. Many of the television companies are state owned, and harassment of journalists and newspapers is common. Reports about anti-regime protests that began in 2018 were silenced. In response, protesters and disaffected citizens moved to communicate and coordinate online. Additionally, as the government began to clamp down on social media access and digital communication platforms, Sudanese citizens moved to VPNs to circumnavigate government censorship. Protesters preferred to move further away from mass media rather than back to what sources known to be misrepresenting the truth.

This case demonstrates the lengths to which people will go for information in an opaque, conflict-prone environment. It also reveals that the turn to peer-to-peer communications does not lead to mass ethnic violence in every circumstance. If an unpopular regime becomes the scapegoat for social problems, mobile phones enable groups to push back against the government rather than attack other ethnic groups.

The analysis above demonstrates that instances of mobile phone fueled violence targeted at minorities or other ethnic groups have jumped in recent years. Given this trend, it is likely that as mobile phone penetration increases around the world, rumor-driven violence will also rise.

Peacekeeping in the Age of Mobile Phones and Rumor-Driven Violence

“Peacekeeping is no longer about the blue berets sitting between two sides, but rather a much more complex, multidimensional challenge that involves the UN in counterinsurgency, policing, intelligence gathering and nation building.”

-- Walter Dorn, 2011

Rumors spread on mobile, peer-to-peer communication networks will be particularly significant for peacekeeping forces. Peacekeeping operations have historically suffered from a lack of information about local dynamics and events, limiting their ability to fulfill their missions. In the future, peacekeeping forces will need to address threats to stability in the information domain, such as rumors spread through digital peer-to-peer networks.
Increased access to mobile phones and the acceleration of rumor dynamics on peer-to-peer communication networks threatens the ability of peacekeepers to maintain peace and stability by impeding three major tasks necessary for effective peacekeeping. With local citizens moving communication to digital platforms rather than traditional, more easily monitored media, peacekeeping forces will have a harder time understanding the dynamic social environment in which they operate. As rumors spread at faster speeds, rapidly inciting mob violence, peacekeeping forces will need to respond more rapidly in the physical realm.

- **Understanding the local population.** Peacekeeping forces face a host of challenges when trying to acclimate to the environment of their mission. The international nature of peacekeeping forces means there are frequently language and cultural barriers between peacekeepers and those they are protecting. Local knowledge, as well as the trust and cooperation of local residents, can be critical for the success of a mission.

Obstacles to dialogue between peacekeepers and the communities they are tasked with protecting will amplify as cell phone ownership increases discussions on peer-to-peer networks. Unlike open social media, one must be a member of a peer-to-peer network to be aware of that community’s social dynamics. Future peacekeeping missions that do not account for these messaging platforms will be ignorant of rumors and concerns transmitted through the digital streets of these communities that have the potential to spark violence.

- **Responding effectively to violence.** As rising mobile phone ownership increases the frequency of digital peer-to-peer communication within communities, groups of like-minded people will be able to share information and mobilize rapidly. The increasing speed at which messages spread will require peacekeeping forces to respond more quickly to the spread of rumors and mob attacks.

Peacekeepers already struggle to quickly respond to calls for help. Peacekeeping forces often operate in complex environments, and frequently lack both the resources on the ground and the situational awareness that would allow them to respond in a timely fashion.\(^5^5\) One especially egregious example of this reality occurred in the Democratic Republic of the Congo (MONUSCO) in 2008, when 150 villagers were slaughtered overnight one mile from a peacekeeping base that had no intelligence of what was happening nearby.\(^5^6\)

- **Building trust and reconciliation between groups.** Successful peace-building requires that UN officials and forces interact with multiple institutional actors and societal groups to influence post-conflict outcomes.\(^5^7\) The UN’s New Deal for Peace identifies two overarching goals for peace-building: building social cohesion and inclusive (legitimate) politics.\(^5^8\) The UN seeks to enhance social cohesion by building trust between social groups, through initiatives such as reconciliation processes. To improve the legitimacy and accountability of governments, the New Deal emphasizes the importance of building trust in governments through political dialogue.\(^5^9\)
Reconciliation processes and political dialogues are crucial for creating peace, but they require intergroup cooperation and a mutual willingness to trust other groups. In many cases, peacekeeping forces play a significant role in establishing and maintaining these interactions. Peacekeepers often represent a force dedicated to monitoring and ensuring adherence to ceasefires, demobilization of combatants, and other elements of peace agreements, all of which provide evidence of growing society-society and state-society trust.

The decentralization of communications brought about by increased access to mobile phones will make fulfilling this peacekeeping role vastly more difficult in the future. As more people have access to mobile phones the spread of rumors and associated violence will accelerate. Mobile phones will enable and empower vigilantes and mobs. In the past, preventing mass propaganda and misinformation required the capture and shutdown of a single radio tower. Future peacekeepers, however, will have to grapple with a new reality in which an equally powerful tool for communicating misinformation is available to those with bad intentions.

The rumors that are spread on mobile-based, peer-to-peer communication networks will pose special challenges for peacekeepers. The speed at which rumors are transmitted on peer-to-peer networks will make it difficult for UN forces to be proactive, and it will result in forces being largely unaware of dynamics an increasingly important social domain.

**Shortcomings of Existing Policy Responses**

Policymakers concerned with peace and stability operations have generally overlooked the potential of mobile phone ownership to drive ethnic conflict. Where thought has been given to addressing this growing threat, it has mainly focused on one of two approaches: (1) legal action to ban certain apps and limit mass forwarding of peer-to-peer messages, and (2) technology-based monitoring of private peer-to-peer networks. Both approaches are problematic and likely would prove to be unfeasible, unsafe, and ineffective in the peacekeeping context.

**Limiting Mass Messaging**

Efforts to restrict or eliminate peer-to-peer messaging platforms will likely be ineffective for three reasons: the decentralization of modern communications, technologically sophisticated users, and the importance of mobile phones for social communication and economic growth.

- **Decentralization of modern communications.** As earlier cases of mobile phone-enabled violence show, rumors and misinformation are most likely to take hold where authorities already restrict free speech and freedom of the press. Extending bans and censorship further to include messaging platforms and other forms of peer-to-peer communication will simply
push populations to newer and less well-regulated platforms. As discussed in the Sudan case above, protesters who knew they could not trust the state-owned media moved to VPNs and more underground forms of communication when the government cracked down on the internet.\textsuperscript{62} Bans on well-known messaging platforms will likely push actors to use other peer-to-peer technologies, while having limited effect on the speed at which rumors spread. As rumors continue to spread and people lose trust in highly restricted mass media, they will be more susceptible to believing inflammatory messages sent to them by family and friends.

- \textit{Limited impact due to tech-savvy users.} Initiatives that aim to limit the number of people to whom a message can be forwarded will likely be ineffective.\textsuperscript{63} Forwarding limits are a politically convenient way to respond to mob violence seen in countries like India. While such a policy may slow the acceleration of rumor dynamics on targeted platforms, these limits are also easy to subvert by savvy users.\textsuperscript{64} Users have already found ways around these limits by using group messages to boost the number of message recipients to many times the size of the audience intended by the ban.\textsuperscript{65}

- \textit{The centrality of mobile communication to society.} Access to mobile phones and the internet are increasingly important for economic and social life. Although several South Asian nations have attempted to cut internet access or cell service to stop ethnic violence during states of emergency, this tactic is unrealistic in the long term because of the associated economic and social costs.\textsuperscript{66} Any policy option that attempts to deal with the spread of rumors by shutting down mobile networks must take into account the increasingly central role that mobile technology has in economic exchange and the effect on the ability of citizens to carry on with the basic aspects of their daily lives.\textsuperscript{67}

\textit{Using Technology to Monitor Peer-to-Peer Networks}

While some states have begun to investigate technological solutions for monitoring peer-to-peer networks, this policy is unrealistic for peacekeeping missions. Several factors limit the feasibility of technological monitoring, including: (1) the principle of consent in UN peacekeeping, (2) international laws regarding data privacy, and (3) the hesitance of member states to share surveillance technology with international forces.

- \textit{Surveillance as a threat to state sovereignty.} Respect for state sovereignty is at the heart of the UN Charter. Peacekeeping missions, therefore, require the consent of the main parties to the conflict.\textsuperscript{68} Because of sovereignty and the probable domestic political concerns about an international body conducting surveillance at home, it is unlikely that local governments and key actors would consent to foreign forces establishing a digital surveillance system that monitors all civilian messaging on peer-to-peer platforms in their country.
Violations of international data privacy laws. International law regarding data privacy also will limit the ability of UN Peacekeeping forces to monitor or surveil peer-to-peer communication platforms. Article 12 of the Universal Declaration of Human Rights establishes an individual’s right to legal protection against “arbitrary interference with his privacy, family, home, or correspondence,” and Article 19 establishes the right to freedom of expression and the freedom “to seek, receive, and impart information and ideas through any media and regardless of frontiers.” In 2013, the UN general assembly passed a resolution affirming the right to privacy in the digital realm.

Hesitance of UN member states to share surveillance technology. Walter Dorn, training advisor for the UN Department of Peacekeeping Operations, has pointed to the growing “monitoring technology gap” between UN and contributing countries and between the UN and the factions it deals with on the ground. Despite the potential for new surveillance technology to assist peacekeeping forces in carrying out their mandates, the permanent members of the Security Council are wary of sharing surveillance technology for fear of revealing their methods to rivals. This concern makes it unlikely that technological improvements in the ability to monitor peer-to-peer networks will reach the hands of peacekeepers.

Any viable policy option for addressing the threat of rumors spread over digital peer-to-peer networks should recognize the increasingly important role that access to mobile phones and the internet plays in the daily lives of many across the globe. A viable policy also must be able to garner the support of local actors and UN member states, while also accounting for international and local concerns about digital privacy.

Policy Recommendation: Walking the Digital Block

The link between community engagement and improved protection of civilians is well established in peacekeeping literature. The local population can help peacekeepers identify threats to peace, leading to better protection of both civilians and mission personnel. Community engagement is a cornerstone of the peacebuilding and reconciliation process by facilitating awareness, by helping maintain a mission’s legitimacy and enabling peacekeepers to better understand the impact of their own interventions.

To prevent and counter violence incited by rumors on peer-to-peer messaging platforms, future peacekeeping forces will need to not only monitor developments on the ground where they serve but will also need to walk the “digital block”. Better monitoring of inflammatory rumors spread online will allow peacekeepers to respond more effectively to mob violence in real time. The ideal actors for this task are community liaison assistants (CLAs), who already assist UN missions with collecting and interpreting information about conflict developments and cultural context.
**Digital Community Liaison Assistants**

The role of the community liaison assistant (CLA) was created in 2010 during the UN mission in the Democratic Republic of the Congo (DRC) “as a tool to link the Mission to communities and increase its situational awareness.” Individuals from the local community take on the role of CLA to bridge the divide between the community and the mission. They provide UN personnel with information regarding the situational context and build relationships between locals and the foreigners who serve in peacekeeping bases.

CLAs bring skills to peacekeeping missions that can be extended to the digital realm to effectively prevent violence. CLAs’ existing social capital and their knowledge of the local language and cultural context make them an effective partner for collecting information about rumors spreading on peer-to-peer networks.

- *Existing social capital.* UN personnel may struggle to gain access to social groups both on and offline. Meanwhile, individuals who take on the role of CLAs are likely to already be established within the peer-to-peer communication networks where rumors spread. By coordinating with CLAs who belong to pre-existing social networks, UN missions will be able to better build capacity for tracking and analyzing online rumors than they otherwise could.

- *Knowledge of language and cultural context.* CLAs do not face the language barriers that challenge foreign UN personnel on missions. UN personnel are also frequently unaware of the cultural context necessary to understand messages translated literally. CLAs will likely be more sensitive to the subtle meaning and implications of rumors spread on peer-to-peer networks. CLAs, therefore, are better-equipped than UN personnel to collect accurate information.

Although CLAs can improve the ability of a peacekeeping mission to identify and respond to the needs of the local population, their inclusion in UN operations presents unique challenges. Missions rely on the pre-existing social connections between CLAs and other community members to both collect information and establish legitimacy. However, as they work closely and openly with UN personnel, they can be “othered” by their communities, especially in contexts where there is widespread distrust of UN peacekeepers or questions about the mission’s legitimacy. CLAs struggle to maintain connections to their community the more they work with peacekeepers, making them both a less effective asset for the mission and a target for anti-UN violence. CLAs are often threatened, attacked, or detained for performing their duties. Peacekeepers often are tasked with preventing violence across ethnic lines. If the UN has overdeveloped its contacts with one ethnic group, it may create the image of a peacekeeping operation favoring one group over another.

Digital CLAs monitoring peer-to-peer networks for rumors will likely face fewer obstacles than regular CLAs and are a more viable option for conducting surveillance for two reasons:
• **Operating in the digital domain.** The relationship between digital CLAs and UN peacekeepers is easier to conceal because they will primarily be responsible for reporting rumors or information of interest to peacekeepers found on peer-to-peer networks. In contrast to regular CLAs who work alongside peacekeepers in the physical spaces of their communities, digital CLAs do not need to have extensive public contact with peacekeepers. This increased anonymity allows digital CLAs to maintain their status and safety within their communities both on and offline.

• **Maintaining digital privacy.** Although the platforms where rumors are spread are closed to outsiders, including peacekeeping forces, digital CLA monitoring of these networks will lessen concerns about invasion of privacy. CLAs are already members of these peer-to-peer networks, and the rumors they report are being widely shared within these digital communities. As such, these rumors and messages are not truly private. Further, in contrast to technological surveillance, UN forces will not collect and analyze every message transmitted on peer-to-peer networks, raising concerns about state sovereignty and citizens’ privacy. Digital CLAs alternatively will only report rumors and messages that are widely disseminated in the digital streets of their communities and could lead to violence.

**Conclusion**

The global rise in mobile phone technology is accelerating the spread of rumors on peer-to-peer messaging platforms that will increase the likelihood of rumor-based violence. This phenomenon will pose a special challenge to peacekeeping forces as it undermines UN efforts to respond quickly to violence and improve social cohesion. Technological solutions to the challenge of peer-to-peer networks are politically and economically problematic because of concerns for state sovereignty, digital privacy, and the unwillingness of members states to share surveillance technology.

By expanding the purview of community liaison assistants to include digital communications, peacekeepers can better monitor the rumors flowing through the digital streets of communities, while limiting concerns about sovereignty and privacy. Given the growing social and economic importance of digital communication and peer-to-peer networks, UN peacekeeping forces will need the cooperation of local citizens to help the walk the “digital blocks” of their communities.

In the age of the mobile phone, showing support for a group does not require one to leave their home and demonstrate with them. Simply liking, following, or otherwise connecting and engaging with a group’s accounts on a digital platform gives the impression of backing or support. As Clay Shirky writes, “Now the highly motivated people can create a context more easily in which the barely motivated people can be effective without having to become activists themselves.” See: Clay Shirky, Here Comes Everyday: The Power of Organizing without Organizations, London: Allen Lane (2008): p. 182.

Now the organization of group effort can be invisible, but the results can be immediately visible. Because the cost of sharing and coordinating has collapsed, new methods of organization are available to ordinary citizens, methods that allow events to be arranged without much advance planning.” See: Ibid, pp. 168-169.


13 It is important to note that while the United States is dissimilar from most of the countries I discuss in my case studies, it is significant that a country with some of the most advanced information and communications technology in the world and abundant capital to use it is defaulting to lower tech organizing because it’s more powerful. If social media and more advanced tech is less powerful even where it would theoretically work best, then states and societies with fewer resources available for such technology and mobilization will likely do the same. See: Kevin Roose, "Campaigns Enter Texting Era With a Plea: Will U Vote 4 Me?,” The New York Times, (August 1, 2018), https://www.nytimes.com/2018/08/01/technology/campaign-text-messages.html.

14 Ibid; Use of peer-to-peer networks is also growing in the developing world as well. “Launch Facebook's mobile app, and the first thing you'll see will be a flurry of wall posts from people you barely know and a big juicy ad. It's annoying, and it's something you don't find on WhatsApp. That's why WhatsApp is becoming a new kind of social network in these countries – one that connects people more immediately and intimately than Facebook.” See: Robert McMillan, “You May Not Use WhatsApp, but the Rest of The World Sure Does,” Wired, (February 20, 2014), https://www.wired.com/2014/02/whatsapp-rules-rest-world/.


16 In Kenya in 2017, the government was able to identify 21 groups on WhatsApp’s platform that were spreading large amounts of misinformation and inflammatory messages. Even then, the government warned that it was the responsibility of moderators and moderators of these groups to police hate speech and did not identify consequences for those who were found to be the original authors of such posts. It was also unclear at the time of the report how the government planned to get data from WhatsApp to monitor for hate speech and disinformation. See: Jula Namlola, “21 WhatsApp groups spreading hate identified,” Daily Nation, (July 27, 2017), https://www.nation.co.ke/news/21-WhatsApp-groups-spreading-hate-identified/1056-4018322-ix7vff/index.html.

17 Homophily theory is the tendency of individuals to associate and bond with similar others, and is expressed through the proverbial “Birds of a feather flock together.” See: James M. Cook et al., “Birds of a Feather: Homophily in Social Networks,” Annual Review of Sociology 27, (2001); pp. 415-444; For more literature on the theory as it applies to online behavior, see: “Homophily in social networks,” FutureLearn, https://www.futurelearn.com/courses/social-media/steps/16055.

18 A study by the American Press Institute found that whether subjects trusted the person who shared a news article on social media mattered more than whether they trusted the original post author or news source. See: 'Who Shared It? How Americans Decide What News to Trust on Social Media," American Press Institute, (May 24, 2017), https://www.americanpressinstitute.org/publications/reports/survey-research/trust-social-media/.


20 This search included articles that used the search terms “mobile phones AND ethnic violence.”

21 Bangladesh, 2015: Bangladesh’s prime minister was quoted as saying that criminals were using services like WhatsApp and Viber to carry out crimes. At the time, government officials in the country were considering a national ban on these messaging platforms and working to track down the perpetrators. See: “WhatsApp, Viber to be blocked, when needed: PM,” The Daily Star, (November 11, 2015), https://www.thedailystar.net/country/whatsapp-viber-be-blocked-pm-170767. (Similar to WhatsApp, Viber is an end-to-end encrypted phone call and private messaging service. See: “About Viber,” Viber, https://www.viber.com/about/.)


28 One such message read “The Kikuyus have stolen our children’s future. Hope of removing them through the ballot has been stolen. We must deal with them the way they understand, violence.” See: Ofiebea Quist-Arcton, “Text Messages Used to Incite Violence in Kenya,” NPR, (February 20, 2008), https://www.npr.org/templates/story/story.php?storyId=19188853.

29 A number was provided and recipients of the message were instructed to send lists of names of Luo people they knew, as well as where and how Luo children went to school. See: Ibid.


31 “As individuals, notably from the south, began to join new media sites, these disputes were magnified, and the online community itself became part of the battleground connected to the growing ethnic polarization in the country. Once the June violence began, polarization accelerated rapidly as members of the different groups sought to use new media to present their stories and to undermine the other versions.” See: Neil Melvin and Tolkun Umaraliev, “New Social Media and Conflict in Kyrgyzstan,” SIPRI Insights on Peace and Security 2011, no. 1, (August 2011), https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1101.pdf.

32 Ibid.


It is important to note here that part of what makes Sudan an unusual case is the relatively widespread access to
VPNs and other advanced technology. This is not the case in most unstable areas where peacekeepers would
be
regrets
for rebellion in the post-conflict country itself. Further, diasporas do not
themselves suffer any of the costs of conflict, and so have a greater incentive to purchase vengeance than the
problem which besets fund
societies. In the CH model, the reason why diasporas are predicted to affect
the risk of conflict is financial. Diasporas are much wealthier than resident populations in the countries which they
have left, and so are much better able to finance conflict. Further, being themselves small minorities in their host
societies, they have a strong incentive to organize for collective action, for example, to preserve their cultural
heritage for their children. The same organizations which preserve culture can be used to overcome the free-rider
problem which besets fund-raising for rebellion in the post-conflict country itself. Further, diasporas do not
themselves suffer any of the costs of conflict, and so have a greater incentive to purchase vengeance than the
resident population.” See: Paul Collier, “Policy for Post-conflict Societies: Reducing the Risks of Renewed

PeaceTechLab Africa is a group working in South Sudan to catalogue a lexicon of hate speech online. See:
“Social Media and Conflict in South Sudan: A Lexicon of Hate Speech Terms,” PeaceTech Lab,
https://static1.squarespace.com/static/54257189e4b0ac0d56ca1566/t/5851c213725e25e531901330/1481753114460/
PeaceTech+Lab+_SouthSudanLexicon.pdf.

For a history of tensions between Sinhalese Buddhists and Muslims in Sri Lanka, see: James John Stewart,
10.1177/0262728014549134.

Michael Safi and Amantha Perera, “Sri Lanka blocks social media as deadly violence continues,” The Guardian,

It is important to note here that part of what makes Sudan an unusual case is the relatively widespread access to
VPNs and other advanced technology. This is not the case in most unstable areas where peacekeepers would
be deployed.

Mark Piesing, “Why are UN Peacekeepers so badly equipped for modern conflict?,” The Independent, (August 9,
2011), https://www.independent.co.uk/news/world/politics/why-are-un-peacekeepers-so-badly-equipped-for-
modern-conflict-2334052.html.

Peter Jones et al., “Head of U.N. Congo peacekeepers regrets failing to stop massacre,” Reuters World News,
(July 3, 2014), https://www.reuters.com/article/us-congodemocratic-massacre-head-of-u-n-congo-peacekeepers-
regrets-failing-to-stop-massacre-idUSKBN0F828120140703.

Mark Piesing, “Why are UN Peacekeepers so badly equipped for modern conflict?,” The Independent, (August 9,
2011), https://www.independent.co.uk/news/world/politics/why-are-un-peacekeepers-so-badly-equipped-for-
modern-conflict-2334052.html.

http://www.unpbf.org/application-guidelines/what-is-peacebuilding/.


63 As demonstrated in the “High Profile Incidents” section, the 2018 elections in Sierra Leone showed that what matters most is not whether someone hears a rumor via word of mouth or via text, but the sheer speed and frequency with which they hear the rumor, which is facilitated by mobile phones. Jamie Hitchen, “The WhatsApp rumors that infused Sierra Leone’s tight election,” African Arguments, (April 10, 2018), https://africanarguments.org/2018/04/10/the-whatsapp-rumours-infused-sierra-leone-tight-election-social-media/.


65 Ibid.


70 Ibid.


There are also concerns regarding potential misuse of such a technological solution if a peacekeeping mission with this technology fails or leaves a country and conflict re-emerges. Putting this kind of high-tech surveillance into the hands of a repressive regime would allow it to read all its citizens’ data and private messages.


After the successes of CLAs in the DRC, UN missions in the Central African Republic, Mali, and South Sudan also adopted the roles as part of their approach to peacekeeping. See: Ibid, p. 21.


Another advantage of employing local community members to report rumors spread on peer-to-peer networks is decreased potential for abuse. Multiple child sexual abuse scandals have eroded trust in the UN of both international human rights groups and local communities. A potential concern regarding UN personnel monitoring closed, peer-to-peer networks is the possibility for individual actors to use this access to networks to abuse community members. By expanding the responsibilities of CLAs to include digital monitoring and reporting, this policy recommendation limits opportunities for abuse of power. See: Kate Brennan, “The Unchanging Reality of the Sex Abuse Scandal,” Just Security, (July 24, 2018), https://www.justsecurity.org/59682/unchanging-reality-sex-abuse-scandal/.


Ibid, p. 22.

Ibid, p. 23.