The University of Texas at Austin
Center for Media Engagement
Moody College of Communication

POLITICAL TALK IN PRIVATE:
ENCRYPTED MESSAGING APPS IN SOUTHEAST ASIA AND EASTERN EUROPE

Zelly Martin, Katlyn Glover, Inga K Trauthig, Alexandra Whitlock, and Samuel Woolley

EXECUTIVE SUMMARY

The Propaganda Lab at the Center for Media Engagement expanded its research into the use of encrypted messaging apps (EMAs)[1] for political talk, analyzing both how EMAs are used by people for everyday political talk and how EMA technology is being used for coordinated manipulation campaigns in Indonesia, Myanmar, the Philippines, and Ukraine.

Our team conducted 21 semi-structured interviews between June and October 2021 with makers and trackers of propaganda and disinformation campaigns on EMAs in the mentioned four countries.

Our analysis revealed three major thematic findings:

1. The propaganda that spreads via EMAs in these countries is dynamic, meaning that it has been optimized for EMAs rather than for traditional media.
2. EMA use is (partially) socially constructed — *some* people use EMAs because they are encrypted, but this often isn't the primary reason users choose them; they are often focused instead on other elements of the apps, like staying in touch with family and friends.
3. Although these platforms enable intimate, private communication, they are also used to "blast" — broadcast or amplify — propagandistic content to many people at once.

These findings point to the significance of EMAs as a space of interest and concern for social media researchers, and, in particular, of looking at the ambiguities associated with EMA use; and they are worthy of attention for anyone interested in democracy, communication and the digital sphere.

SUGGESTED CITATION:

Martin, Z., Glover, K., Trauthig, I. K.,Whitlock, A., and Woolley, S. (December, 2021). Political talk in private: Encrypted messaging apps in Southeast Asia and Eastern Europe. Center for Media Engagement. https://mediaengagement.org/research/encrypted-messaging-apps-in-southeast-asia-and-eastern-europe

INTRODUCTION

Existing scholarship has established that social media is being used for political manipulation across the globe,[2] and not only on traditional social media platforms like Facebook and Twitter. Encrypted messaging apps (EMAs) are emerging as an attractive platform for political manipulation.[3] As recent literature has shown, EMAs are being used for propaganda, radicalization, misinformation, and disinformation in the United States,[4] India,[5] Pakistan,[6] Nigeria,[7] and various countries in Latin America.[8]

EMAs are often used both by activists to communicate in relative privacy,[9] such as by pro-democratic activists in Myanmar,[10] and by extremists to radicalize others and spread propaganda, such as by white supremacists and the Islamic State (IS).[11] Researchers have found that online extremist behavior has led to offline violence across the globe: in the United States,[12] the United Kingdom,[13] India,[14] and Uzbekistan,[15] just to name a few. These emerging platforms can thus have both beneficial and detrimental effects: in authoritarian regimes, activists can safely organize within the privacy of these apps, but dangerous organizations and individuals may also use them to illegitimately influence elections or radicalize individuals.

Crucially, our analysis sheds light on the how EMAs are being used for political purposes in environments and countries defined by a number of destabilizing socio-political factors, including persisting governmental turmoil and regular foreign interference across information ecosystems (and, in some cases, foreign interference in the offline world). In these spaces and places, digital platforms including EMAs are being normalized for political manipulation as well as for more general political talk. The problems associated with this now-common digital political manipulation are well-known, hence the mechanisms through which this political manipulation is being carried out are worthy of serious attention for anyone interested in democracy, communication, and the digital sphere.

The following three overall trends were most prevalent in our research:

1. **Adaptation strategies**

   EMA propaganda:

   - Is dynamic and human-powered
   - Hides in plain sight
   - Elicits emotions
   - Preys on low media literacy
   - Spreads in established community groups

2. **Social construction**

   EMAs are (partially) what people make of them:

   - Some apps are used explicitly for political talk, some are used for social talk, some are used for activism
   - The majority of users do not choose these apps specifically because of their encryption features
   - For a minority of users, the encryption is crucial

3. **Amplification via EMAs**

   Unusual, but effective

   - Activists use these platforms for intimate organizing
   - Propagandists use these platforms to blast many people at once

CASES AND METHODS

We began our research with the following question: *How does encrypted messaging use intersect with different types of political talk (such as mis- and disinformation, propaganda, or activism) and what are the characteristics of such content on EMAs?*

Under this exploratory research question focused on political talk, we congregated political content from differing provenance and contexts, and shared for varying motivations in different contexts. We define *disinformation* as false information shared with intent to deceive, and *misinformation* as false content that is spread accidentally by those who believe it to be true.[16] *Propaganda* refers to political information shared with the intent to persuade; while propaganda can be misleading, it is not always or by definition false.[17] We define *activism* as content spread to promote particular social and political causes. We are cognizant of the fact that one person's propaganda can be another person's activism.

From June 2021 to October 2021, our team conducted 21 qualitative, semi-structured interviews across Indonesia, Myanmar, the Philippines, and Ukraine. We spoke with activists, experts, fact-checkers, journalists, politicians, and producers of propaganda to gain the perspectives of both the makers and trackers of political talk on EMAs.[18]

Producers of disinformation and politicians provided invaluable insight into the actual disinformation campaigns and political propaganda, respectively. However, we treat these groups as potentially unreliable narrators because they have a stake in the disinformation campaigns and/or political propaganda they produce and it may have affected their answers. Therefore, data from these interviews is always interpreted with an extra caveat.

Our interviews with fact-checkers, journalists, and experts in these spaces were conducted to gain a fuller picture of the political conversations happening in encrypted spaces. Having a multitude of perspectives, including that of activists, allowed for a richer picture of the varied ways in which EMAs are used in the countries we studied. This is in line with previous scholarship[19] which has investigated disinformation campaigns through qualitative interviews with producers and has triangulated the findings with the perspectives of observers. This strategy allowed us to draw conclusions about the political talk, including disinformation campaigns, propaganda, and activism, that is happening on EMAs throughout these countries.

Conversations with experts suggested that similar EMA disinformation campaigns were being run across Indonesia, Myanmar, the Philippines, and Ukraine, so we chose these countries as an exploratory set of case studies. We hoped to illuminate previously unexplored economic and geographic similarities and differences, such as social factors or digital development and infrastructure, across these countries. Each of the cases is unique, but all four are lower middle-income countries.[20] Previous research[21] has tied low socioeconomic status to likelihood in believing misinformation. We therefore aim to expand our understanding of belief in both mis- and disinformation in lower-income countries.

In addition, our case studies are small to middle-size countries embedded in regions that are overshadowed by much larger powers — Russia and China — making them potentially susceptible to disinformation campaigns that aim to align them with Russia's and China's political interests. We investigated these connections in four countries, each of which has recently experienced state-aligned mis- or disinformation campaigns, partly due to recent political turmoil. We investigated these connections in four countries with varying levels of internet use: Myanmar (23.6% in 2017, most recent data), the Philippines (46.9% in 2019), Indonesia (53.7% in 2020), and Ukraine (70.1% in 2019)[22] as a differentiating factor, given that data on EMA use in these countries is unavailable.[23]

All of these politically turbulent countries have been the targets of state-aligned mis- or disinformation campaigns. Fake news trolls have influenced elections in Indonesia,[24] and the Indonesian government recently (2019) shut down the Internet in Papua and West Papua in an effort to stop the flow of fake news[25] and temper offline violence.[26] In Myanmar, the democratically-elected government, the National League for Democracy, headed by Aung San Suu Kyi, was overthrown by the military branch of the government, the Tatmadaw, in 2021.[27] The citizens face regular Internet shutdowns and restrictions on social media, which creates a space for disinformation to breed.[28] In the Philippines, the 2016 use of troll farms by President Duterte and members of the Filipino Senate[29] was one of the early cases of the use of social media to influence elections, and disinformation continues to be a persistent problem there.[30] Ukraine became a hotbed for Russian disinformation following the fairly

recent (2014) Euromaidan protest and annexation of Crimea by Russia.[31] As in Myanmar, this recent political turmoil created a welcoming environment for producers of disinformation to sow confusion online.[32]

FINDINGS

In all four countries we studied, EMAs were relevant channels for political talk of various kinds. Amongst the most interesting findings were the socially defined and well-understood parameters of which apps to use for certain purposes. Generally, there is a continuum of purposes for which people use EMAs, ranging from informal, implicit, social, and familiar political communication — such as having conversations with friends or family about the COVID-19 vaccine — to formal, explicit political communication, as when paid political propagandists or democratic activists communicate to followers, or when members of the government and/or military communicate to supporters or to the general population. This broad finding is in line with other research and investigative reporting. However, our findings illuminate new characteristics of this political talk in our countries of interest.

Adaptation Strategies: EMA Propaganda Is Dynamic

Overview

Five main themes about EMA-distributed propaganda emerged in our research. First, we found that political propaganda is dynamic — no longer only designed for distribution through traditional media but optimized to work effectively on EMAs. Much EMA propaganda does not utilize automated computational methods (such as bot farms) but is instead spread through accounts run manually, by humans. We assume this is because human-run accounts are more difficult to identify and track than bot accounts. Why, then, did many interviewees across all four countries characterize the propaganda distributed via EMAs as "unsophisticated" in their countries?

Our second finding — that EMA propaganda hides in plain sight, in that it is often openly positive about who it aims to promote or negative about who it aims to disparage — may provide support for the claim about its unsophistication.

Third, we found that this type of propaganda is typically intended to elicit an emotional response. This finding may be related to our fourth observation: according to our interviewees, media literacy is quite low among all four of these countries' populations, and disinformation producers are able to exploit this literacy gap to their advantage.

Finally, we found that political propaganda, and in some cases disinformation, spreads in known-community groups, some of which are thought of as political groups and some of which are thought of as purely social. As our lab's previous research has shown, the use of known networks is a highly effective strategy for spreading disinformation.[33]

Case Studies

Indonesia

Disinformation campaigns on traditional social media differ from those on EMAs. On Facebook, Twitter, and YouTube, "buzzers" (people hired to have conversations online or to make information viral in an effort to affect public opinion) are hired by political candidates to manufacture consensus[34] — create real political support from orchestrated conversations between fake accounts — in what our interviewee called "cyberwars." Political parties hire digital marketing firms to create fake accounts and have political discussions online under Facebook posts, YouTube videos, etc.

These political discussions are intended to push positive information about candidates in a seemingly organic way; normal users might find it hard to detect that the account has been paid to say good things about a candidate, in part because this strategy is human-powered. An interviewee who leads a team of buzzers told us, "They work non-stop, especially...when the day of the election is near." On EMAs, the political manipulation strategy is also human-powered, but buzzers are unable to have orchestrated conversations. In our data, EMAs in Indonesia are used solely to push out positive information about candidates rather than to engage in orchestrated discussions.

Media literacy is low in Indonesia, and these strategies have proven effective. A leader at a prominent fact-checking organization in the region is convinced that "It is really easy to deceive Indonesians."

Myanmar

EMA political propaganda is overt in Myanmar; pro-military EMA channels are run by individual supporters of the military or by individual administrators in the military and are explicitly named after military commanders, often with expressions of love or support in the title ("I love Sargeant x"). As one Burmese journalist told us,

> *"It's really obvious for people in Myanmar to understand which groups are pro-military and which groups are not."*

These human-run accounts, which spread disinformation within groups of people who are already supporters of the Tatmadaw, at times extend their reach to the general population. A notable example occurred when the Tatmadaw pushed a disinformation campaign on EMAs and through SMS messages about the release of Aung San Suu Kyi. This disinformation campaign took place while the Internet was shut down in Myanmar, giving

users no ability to check the veracity of the claims about her release. During this period, one of our interviewees received identical false messages about Aung San Suu Kyi's release from over 200 unknown numbers.

This particular (highly successful) campaign played both on the emotions and the low media literacy of the population: citizens were overjoyed that their democratically-elected representative had been released, and they were not able to identify that the information was untrue. According to activists, they try to combat mis- and disinformation directly in Telegram channels by reaching out to the post owners and asking them to take posts down, but disinformation remains rampant, especially on Telegram.

The Philippines

Individuals within the government run massive groups that include over two million citizens to increase support for the president and share information from the government. They use stickers with Duterte's image on EMAs to increase support. While increasing support for a president is not inherently problematic, it becomes so when we consider that Duterte used troll farms to win elections; these groups are seeking to increase support for a corrupt president.

In some way, these dynamics can be seen as a different iteration or evolution of the use of troll farms and in itself a form of corruption. While still unnaturally bolstering support for an authoritarian leader, the disinformation is not deceptively hiding its aims.

Members of the government told us that they themselves run these channels as part of their job descriptions. They explicitly stated that they do not use troll farms to do this. Whether or not this is true across the government or even across these interviewees' sectors, they indicated that humans run these specific accounts, which are openly sharing information and encouraging support for President Duterte. They also stated that they target millennials for their messaging and aim to be as entertaining as possible.

According to an interviewee working in cybersecurity, some computational propaganda may be present, but human propaganda appears to be more prevalent.

Ukraine

Standard computational propaganda is still an issue in the region, but our interviewees highlighted unique ways in which EMA disinformation campaigns are successful despite their lack of technical sophistication.

As in the Philippines, in Ukraine, disinformation is sometimes spread through appealing to positive emotions: one politician informed us that people read and spread disinformation because it's like a "novel but with real persons" — it's entertaining.

Actors also appeal to negative emotions such as fear by adapting existing conspiracy theories to play on both historical issues and current events. Ukraine's history of Russian

occupation — and Russia's ongoing claims to parts of Ukraine — is worrying many citizens, and because of this, they are particularly likely to suspect foreign interference. Therefore, propagandists often use anti-Western tropes to play on these emotions. Propagandistic content plays on fears that Ukraine is not a sovereign state and that all decisions are affected by the West. This emotional and rhetorical tactic, combined with careful masking of overtly pro-Russian sentiments, has proven successful for propagandists in Ukraine. For example, according to one prominent researcher we interviewed in Ukraine, "nearly half of the Ukrainian population believes that the International Monetary Fund controls the Ukrainian government."

In addition to activating historical fears, the conspiracy theories are adapted to also hook in with current events. One week, producers might push the belief that the IMF governs Ukraine, and the next week they might shift to saying that George Soros, an American philanthropist, controls the Ukrainian government.

This conspiratorial messaging has been successful, penetrating to the local levels by spreading through known community groups. The process is sly but simple; it does not require large scale organization and technical prowess but rather depends on particular manipulative rhetorical strategies and responsiveness to local circumstances. When these techniques are paired with elements of computational propaganda — the ability to amplify the messages across known-group EMA channels — the campaigns they support are particularly successful.

Social Construction: EMAs (Partially) Are What People Make Of It

Overview

The choice of which EMA app to use varies greatly across populations and countries because potential users' understandings of the various apps are socially constructed. Potential users hold specific, socially constructed perceptions of what groups each app is designed for. For example, perceptions of apps' user bases are heavily shaped by users' demographics, particularly their age. Apps are also often chosen for professional reasons, based on perceptions of the features they have to offer.

The characteristics of particular EMAs also lend themselves more to some groups of users than others. For example, pro-democracy activists strategically chose EMAs as a tool for communication due to the protection they provide through encryption, similar to journalists and pro-democracy activists, relying on EMAs for more secure communication.

People's perceptions of various apps are also colored by historical experiences in their respective countries. For instance, in Ukraine, interviewees of different backgrounds asserted their conviction that Telegram is heavily dominated by Russians — an impression

that was confirmed by local Ukrainian journalists, who outlined how Telegram channels meant for news are co-opted by Russian disinformation producers.

Case Studies

Indonesia

In Indonesia, the issue of encryption does not seem to be top of mind for many users when they select EMAs for personal communication. For a minority, however, the encryption protocols of Telegram and Signal are seen as more trusted than WhatsApp, and activists in the country seem to rely on Signal and Telegram for coordination. As we will also see in the case of Ukraine, Signal seems to be widely perceived as the most secure EMA.

WhatsApp seems to be the most prevalent EMA, likely in part because Facebook has a continuing stronghold on the nation and in part because of the legacy of Free Basics,[35] a program that gave people free access to certain websites, including Facebook. The program ended in 2018, but left a legacy of ubiquitous use in Myanmar (as it did in Indonesia). According to one of our interviewees, the app is used for daily discussions between friends and family.

WhatsApp is also used politically, with buzzers using it to push out positive information about candidates. Their goal does not seem to be the manufacturing of consensus (as is the case with traditional social media). Strategically speaking, EMAs are not buzzers' first choice for creating political discussions online because they are unable to track engagement.

Telegram and Signal are relied on by activists in Indonesia, who coordinate on these apps. According to the founder of a prominent fact checking organization in Indonesia, WhatsApp's privacy and security are not as trusted among those worried about privacy. This could be one reason that WhatsApp is primarily reserved for matters of daily social life.

Myanmar

In Myanmar, several apps are used by both activists and the military junta to spread their messaging, but both groups focus on Telegram and Signal. Facebook and Twitter are still considered the main sites for social media engagement, but all are regularly affected by the government shutdowns and Facebook and Twitter are often only accessible through VPNs.

Facebook still dominates the social media sphere in Myanmar — "Facebook is the internet in Myanmar," one journalist told us — due to the legacy of Free Basics.[36] Facebook (along with the rest of the internet) have been periodically shut down in Myanmar, but people continue using these platforms by accessing them through VPNs, which hide their locations. Curiously, though, despite Facebook's stranglehold, WhatsApp plays a less important role in Myanmar than other EMAs.

Telegram and Signal are primarily used by activists to organize, in part because they do

not need to use VPNs in order to use the apps. Multiple activists informed us that before the coup, Facebook and Viber were the most popular apps, but after the coup, Telegram became the most used. Activists have also constructed an image of Telegram and Signal as being safe from military surveillance and of Facebook Messenger as not being secure. In addition, Telegram users can hide their numbers and change their names, while Facebook (which owns WhatsApp) requires real names. Although Telegram remains a hotbed of disinformation in Myanmar (as it is in other countries), activists and journalists informed us that it can also be a source of legitimate information, as they are able to access and distribute news about Myanmar both within and outside of the country. Strategically, Burmese activists choose Telegram, which allows messages to be deleted on both ends; this removes the fear of being picked off the street and having one's phone examined by the military junta.

EMAs (including Telegram*)* and *SMS* are both used by the military junta to spread disinformation. For example, the Tatmadaw utilized EMAs and SMS to spread the aforementioned conspiracy theory that Aung San Suu Kyi had been released while she was still in custody. They seem to be strategically relying on these platforms because they know they can reach many Burmese — especially Burmese activists — this way.

The Philippines

In the Philippines, Viber and WhatsApp are the most-used EMAs, according to our interviewees. These apps are used both by members of the public and by members of the government, but Viber was characterized as having been "invaded" by the government.

Both apps are used for political talk and are generally used for reasons other than their encryption features. In addition, social media platforms such as Facebook (including Facebook Messenger) are used by many, although according to members of Duterte's government, Twitter is primarily used by those who are anti-Duterte.

According to our interviewees, Viber appears to be the app that is most used for political propaganda. Our interviewees from governmental departments in charge of communication explained their strategic decision to use Viber in simple terms: "We always go where the people are." In the Philippines, this also means that they do not use Twitter because that is where "opponents of the president" are.

Viber is in wider use than Telegram, although our interviewees generally considered Telegram to be safer. They use Viber because that's where their communities are located. For users, the value comes not in encryption but in being able to communicate with many people at once and in utilizing these platforms in the same way that public Facebook groups or Twitter might be used. They share pro-government messaging in massive groups with millions of Filipino citizens.

WhatsApp and Viber are equally effective for spreading disinformation because of their ability to host large groups. According to an interviewee who worked in politics (but not in Duterte's government), political disinformation spreads in private chat groups of family and friends on WhatsApp and Viber. He also said that large public groups on WhatsApp and Viber become "echo chambers" hosting only political junkies, because people leave these groups when they don't like the content.

Ukraine

In Ukraine, Telegram is seen as almost solely reserved for political topics and news. Signal plays a less prominent role for most Ukrainians, but activists and politicians often use it because they identified it as the most secure option.

Viber is extremely popular in Ukraine and is reserved for communications between family, friends, and communities (such as parents' groups of school classes). It is considered to be a non-political communication channel because of this use. If disinformation makes its way into these channels, however, it is particularly powerful because people are generally unguarded when conversing on Viber. As previous research has shown, information on EMAs often comes from trusted family and friends. For instance, disinformation about COVID-19, which would be considered political conversation by analysts, is not perceived as such by Ukrainians conversing on Viber. A prominent Ukrainian researcher told us,

> *"It's actually part of the reason, one of the reasons, why disinformation is so easily accepted when it is received from Viber, because it often comes from the people who you personally know and you personally trust. And it also is often a piece of information that, as I said, doesn't look political."*

Viber conversations sometimes take on pro-Russian tones, according to a former journalist and current politician in the country, who views this as suggesting possible Russian influence. Although he remained adamant that Viber is currently not political, he did say, "Russians' next step will be Viber."

Telegram has the reputation of being "the political app" among the EMAs in the Ukraine. Telegram content is overtly political, as it is used mostly to discuss particular political candidates, parties, or policies. Journalists often use information from large Telegram channels to inform their reporting. Propagandists use this to their advantage: Telegram channels first attract journalists by sharing legitimate news, then administrators begin feeding the journalists disinformation, which then spreads from EMAs to more traditional media.

Signal is the EMA that Ukrainians see as the most secure. One interviewee, a leading

Ukrainian researcher, emphasized that he is wary of Western government officials eavesdropping on Ukrainians, including himself, and that this is why he uses Signal for conversations about his research. Similarly, politicians or those who are concerned about sharing secrets also use Signal because of its encryption. In general, however, the issue of encryption — or the issue of digital privacy writ large — does not seem top of mind for many people in Ukraine. For most people, the decision to communicate over EMAs does not seem to stem from their concern for privacy but rather from these apps' status as part of daily life.

Amplification via EMAs: Unusual, But Effective

Overview

EMAs have generally been associated with private, secure communication, but they are now being used both for one-to-one communication and for one-to-many communication. They are thus poised to take the place of traditional social media networks like Facebook and Twitter.

In the countries we studied, members of the government are now using EMAs to speak to large swaths of the population and activists are using them to broadcast messaging to many members at once. These uses do not require encryption or privacy protocols; in one-to-many communications, propagandists are there because that is where the people are.

Those who use EMAs for one-to-one or small-scale communications generally do so *because* they are encrypted. Activists in particular tend to utilize these platforms to receive safe, secure information about "secrets" or to share information that could be dangerous to them. For these folks, encryption remains a valuable feature.

Case Studies

Indonesia

WhatsApp groups are attractive to those looking to spread false information. These large, topic-specific groups revolve around topics like religion or ethnicity and are designed to allow people to join a community of likeminded individuals. These groups are large and attract many users — most groups hit the WhatsApp maximum of 256 members. Information shared in the groups largely revolves around the topic of their shared interest, so users in the group often do not notice when discussions turn political (as with the previously discussed Viber groups in Ukraine). Indonesia has a low level of media literacy, which is compounded by the fact that users' guards are down in these groups because of their seemingly innocent functions.

The coordinator of a major fact-checking organization told us they believe some of these groups are purposefully created by disinformation actors to spread false information because "You can see the same message in multiple different groups." According to a

researcher in Indonesia, information in these topic-specific groups often spreads to other community groups, allowing the disinformation to travel far and wide.

WhatsApp groups and Telegram channels are also often used by influencers and other disinformation actors to promote backlinks to their YouTube videos and other content.

Myanmar

In Myanmar (unlike the other countries mentioned), EMAs are rarely used to speak to large groups of people, perhaps due to the current authoritarian rule. Utilizing these apps for large-scale communication is not safe for activists, and it is not practical for the military junta, who often shut down the internet (and thus EMAs) altogether. EMAs are used by activists mainly for small-scale organizing. Producers of disinformation (the military junta) tend to use these platforms not for mass communication (one-to-many communication), but to spread propaganda within their groups. According to a Burmese journalist, the propaganda typically does not spread far outside their official channels.

Telegram and sometimes Signal are used by activists for several purposes: to coordinate which hashtags they are going to tweet out and at what time, to teach their followers how to use Twitter effectively, to source reliable information from news organizations, to fact-check information, and to spread legitimate news — unique educational uses for EMAs that we did not observe in other countries. These uses of EMAs take advantage of the intimate, private, and secure nature of these platforms. In contrast, activists rely on Facebook and Twitter to reach large groups.

The Philippines

Viber (and, to a lesser extent, Facebook Messenger) are used by members of the government to speak to many citizens (up to 2.6 million) at once. According to two government officials, “We try to adapt a shotgun approach ... we try to blast them.”

Viber is also used by members of the government for smaller-scale inter-government communication, but this has little to do with its encryption or security protocols; it is because Viber is where the people — including the government employees — are.

Ukraine

Telegram’s large channels (and only its large channels) are attractive to propagandists, who use them to specifically target journalists. Telegram is hugely influential in Ukraine because journalists often use information from large Telegram channels to inform their reporting. As various informants in Ukraine explained, Telegram channels lure journalists to join these channels by sharing factual information, then eventually, after gaining their trust, propagandists begin to share false information, which journalists are likely to trust because of their previous encounters with the propagandists.

Large, anonymous Telegram channels are vulnerable to bots, and our interviewees seem to believe that bots are behind much of the growth of these channels. Bots run by third-party PR firms or political consulting companies are often hired by politicians to take advantage of the dynamic described above, at first offering factual information to build trust, then shifting to sharing blatantly false information.

It appears that large Telegram channels are being used to push a Russian agenda into traditional media with bots. As a Ukrainian disinformation expert shared, "Anonymous Telegram channels, which push for Russian agenda...become very popular, sometimes due to organic reasons but sometimes due to bots...And their large audience attracts attention from the local fringe online media." A former journalist turned politician used even stronger language, stating that "printing media are dead" and these Telegram channels are "ruled by Russians or some Ukrainian politicians."

CONCLUSION

This study confirmed some existing knowledge, showing that EMAs matter for large parts of the population in our case studies. It also revealed new understandings that identified which EMAs are used for different types of political talk in each country — a finding that likely suggests how effective these various apps are for different types of political talk and political propaganda.

Our research illuminated three key elements. First, it documented some of the adaptation strategies used by producers of disinformation and activists alike to make EMAs work for their goals. Second, it showed how different actors select which EMAs to use based on several factors: their motives for communication, who they want to reach, what kind of conversation they want to have, and whether they fear surveillance. Third, it identified an unexpected use of EMAs, that of large-scale amplification of messaging. The research reported here has implications for policymakers, platform designers, researchers, civil society, and the public writ large.

- Perhaps our most interesting finding is that the decision about which app to use for each type of conversation — from political conversation to private talk to risky or illegal organizing — appears to be based on socially constructed perceptions of what each app is good for: family chat, discussion of shared interests with strangers, or political news.
- Building on this insight, policies should work to address the issue of disinformation being shared within these multiple types of conversations. Currently, little of the propaganda being shared via EMA is driven by bots, and technological fixes may not be enough. Human perception is best addressed with human solutions: inoculation programs, fact-checkers, and digital literacy programs.

- This is not to say that technological adjustments — efforts to identify computational propaganda or limitations on how many times a message can be forwarded or how far it can be forwarded[37] — are futile. Instead, we recommend complementing these technological adjustments with a more societally-based approach. Broadly speaking, platforms could work with local fact-checkers and communities (for instance, activists in Myanmar) to cater interventions to their needs.
- EMAs are also comparatively young, emerging over the course of the 2010s. Social scientists should focus studies on understanding their functions and effects on societies and political systems in order to broaden our understanding and provide context outside of user statistics.

As the popularity of EMAs such as WhatsApp, Telegram, and Signal increases globally, both activism and disinformation alike will adapt to make use of these platforms. Civil society, tech companies, and international and local policymakers, however, can work together to protect data privacy and activism while limiting disinformation and propaganda.[38] Recent interventions by Meedan, such as WhatsApp tiplines[39] and WhatsApp fact-checking,[40] have demonstrated how to intervene in the spread of disinformation on these platforms. Outreach and conversation by tech companies with local fact-checkers, researchers, and civil society is crucial to ensure that disinformation is being identified, blocked, and countered without endangering activists' safety and privacy.

ACKNOWLEDGMENTS

Thank you to Martin Riedl for the editorial help. This report was funded by Omidyar Network, Open Society Foundations, and the John S. and James L. Knight Foundation.

ENDNOTES

[1] Gursky, J., Glover, K., Joseff, K., Riedl, M.J., Pinzon, J., Geller, R., & Woolley, S. C. (2020, October 26). Encrypted propaganda: Political manipulation via encrypted messages apps in the United States, India, and Mexico. *Center for Media Engagement*. https://mediaengagement.org/research/encrypted-propaganda

[2] Woolley, S. C., & Guilbeault, D. (2019). United States: Manufacturing consensus online. In S. C. Woolley & P. N. Howard (Eds.), *Computational propaganda: Political parties, politicians, and political manipulation on social media* (pp. 185-211). Oxford University Press; Woolley, S. C., & Howard, P. N. (2017). Computational propaganda worldwide: Executive summary. In S. C. Woolley & P. N. Howard (Eds.), Working Paper 2017.11. Oxford, UK: Project on Computational Propaganda. Comprop.poii.ox.ac.uk. 14 pp.

[3] Malley, C. (2021, January 12). Signal Downloads Increase 4200%, Spurred by WhatsApp Sharing User Data with Facebook. *Hypebeast.* https://hypebeast.com/2021/1/signal-downloads-increase-4200-spurred-by-whatsapp-sharing-user-data-with-facebook; Mantas, H. (2021, Jan. 14). *Growing usage of encrypted messaging apps could make it harder to combat misinformation.* Poynter. https://www.poynter.org/fact-checking/2021/growing-usage-of-encrypted-messaging-apps-could-make-it-harder-to-combat-misinformation/

[4] Gursky, J., Glover, K., Joseff, K., Riedl, M.J., Pinzon, J., Geller, R., & Woolley, S. C. (2020, October 26). Encrypted propaganda: Political manipulation via encrypted messages apps in the United States, India, and Mexico. *Center for Media Engagement*. https://mediaengagement.org/research/encrypted-propaganda

[5] Banaji, S., Bhat, R., Agarwal, A., Passanha, N., & Sadhana Pravin, M. (2019). WhatsApp vigilantes: An exploration of citizen reception and circulation of WhatsApp misinformation linked to mob violence in India. Department of Media and Communications, London School of Economics and Political Science, London, UK; Gursky, J., Glover, K., Joseff, K., Riedl, M.J., Pinzon, J., Geller, R., & Woolley, S. C. (2020, October 26). Encrypted propaganda: Political manipulation via encrypted messages apps in the United States, India, and Mexico. *Center for Media Engagement*. https://mediaengagement.org/research/encrypted-propaganda; Pasquetto, I. V., Jahani, E., Baranovsky, A., & Baum, M. A. (2020). Understanding misinformation on mobile instant messengers (MIMs) in developing countries. Shorenstein Center on Media, Politics, and Public Policy. https://www.shorensteincenter.org/wp-content/uploads/2020/06/Misinfo-on-MIMs-Shorenstein-Center-May-2020.pdf

[6] Pasquetto, I. V., Jahani, E., Baranovsky, A., & Baum, M. A. (2020). Understanding misinformation on mobile instant messengers (MIMs) in developing countries. Shorenstein Center on Media, Politics, and Public Policy. https://www.shorensteincenter.org/wp-content/uploads/2020/06/Misinfo-on-MIMs-Shorenstein-Center-May-2020.pdf

[7] Pasquetto, I. V., Jahani, E., Baranovsky, A., & Baum, M. A. (2020). Understanding misinformation on mobile instant messengers (MIMs) in developing countries. Shorenstein Center on Media, Politics, and Public Policy. https://www.shorensteincenter.org/wp-content/uploads/2020/06/Misinfo-on-MIMs-Shorenstein-Center-May-2020.pdf

[8] Bandeira, L., Barojan, D., Braga, R., Peñarredonda, J. L., & Argüello, M. F. P. (2019). *Disinformation in democracies: Strengthening digital resilience in Latin America*. Atlantic Council.; Evangelista, R., & Bruno, F. (2019). WhatsApp and political instability in Brazil: Targeted messages and political radicalisation. *Internet Policy Review, 8*(4), 1-23.; Gursky, J., Glover, K., Joseff, K., Riedl, M.J., Pinzon, J., Geller, R., & Woolley, S. C. (2020, October 26). Encrypted propaganda: Political manipulation via encrypted messages apps in the United States, India, and Mexico. *Center for Media Engagement*. https://mediaengagement.org/research/encrypted-propaganda; Recuero, R., Soares, F., & Vinhas, O. (2020). Discursive strategies for disinformation on WhatsApp and Twitter during the 2018 Brazilian presidential election. *First Monday, 26*(1). https://doi.org/10.5210/fm.v26i1.10551

[9] Nierenberg, A. (2020, June 11). Signal Downloads Are Way Up Since the Protests Began. *New York Times*. https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html

[10] Yadav, A. (2021, Aug 6). *How pro-democracy activists in Myanmar keep their movement alive with hashtags.* Medium. https://medium.com/dfrlab/how-pro-democracy-activists-in-myanmar-keep-their-movement-alive-with-hashtags-34ff2d3eddf2

[11] Bloom, M., Tiflati, H., & Horgan, J. (2019). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence, 31*(6), 1242-1254; Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, J. (2020). Online extremism: research trends in internet activism, radicalization, and counter-strategies. *International Journal of Conflict and Violence, 14*, 1-20.

[12] Hatzipanagos, R. (2018, November 30). How online hate turns into real-life violence. *Washington Post*. https://www.washingtonpost.com/nation/2018/11/30/how-online-hate-speech-is-fueling-real-life-violence/

[13] Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes. *Criminology & Public Policy*, *16*(1), 99-117.

[14] Banaji, S., Bhat, R., Agarwal, A., Passanha, N., & Sadhana Pravin, M. (2019). WhatsApp vigilantes: An exploration of citizen reception and circulation of WhatsApp misinformation linked to mob violence in India. Department of Media and Communications, London School of Economics and Political Science, London, UK.

[15] Rhozinski, R. & Muggah, R. (2021, June 15). *Central Asia's growing internet carries new risks of violence.* United States Institute of Peace. https://www.usip.org/publications/2021/06/central-asias-growing-internet-carries-new-risks-violence

[16] This follows Wardle and Derakhshan's definitions of misinformation and disinformation: disinformation is "information that is false and deliberately created to harm a person, social group, organization or country;" misinformation is "information that is false, but not created with the intention of causing harm;" malinformation is "information that is based on reality, used to inflict harm on a person, organization or country." Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. *Council of Europe, 27,* 20.

[17] This follows Derakhshan and Wardle (2017), who define propaganda as "true or false information spread to persuade an audience, [that] often has a political connotation and is often connected to information produced by governments." Derakhshan, H., & Wardle, C. (2017). Information disorder: definitions. *AA. VV., Understanding and addressing the disinformation ecosystem*, 5-12.Derakhshan, H., & Wardle, C. (2017). Information disorder: definitions. *AA. VV., Understanding and addressing the disinformation ecosystem*, 5-12.

[18] All interviewees are referred to broadly by their role (i.e., journalist, activist, researcher, etc.) without identifying specifics as to their position, job title, company, etc. to protect the safety and privacy of interviewees, in line with University of Texas' Institutional Review Board-approved specifications.

[19] Ong, J. C., & Cabanes, J. V. A. (2018). Architects of networked disinformation: Behind the scenes of troll accounts and fake news production in the Philippines. *Architects of networked disinformation: Behind the scenes of troll accounts and fake news production in the Philippines*. 74. https://doi.org/10.7275/2cq4-5396; Woolley, S. C., & Guilbeault, D. (2019). United States: Manufacturing consensus online. In S. C. Woolley & P. N. Howard (Eds.), *Computational propaganda: Political parties, politicians, and political manipulation on social media* (pp. 185-211). Oxford University Press.

[20] World Bank. *Lower middle income.* World Bank. https://data.worldbank.org/country/XN

[21] Pan, W., Liu, D., & Fang, J. (2021). An examination of factors contributing to the acceptance of online health misinformation. *Frontiers in Psychology*, *12*, 524.

[22] World Bank. *Individuals using the Internet (% of population) - Myanmar, Philippines, Indonesia, Ukraine.* World Bank. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=MM-PH-ID-UA&view=chart

[23] World Bank. *Individuals using the Internet (% of population) - Myanmar, Philippines, Indonesia, Ukraine.* World Bank. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=MM-PH-ID-UA&view=chart

[24] Paulo, D. A. (2020, December 22). Meet the fake news trolls who influenced US and Indonesian polls for money. *Channel News Asia*. https://www.channelnewsasia.com/cnainsider/trolls-fake-news-industry-elections-veles-malaysia-indonesia-us-904676

[25] Bayuni, E. M. (2019, September 2). How to lose propaganda war over Papua. *Jakarta Post*. https://www.thejakartapost.com/academia/2019/09/02/how-to-lose-propaganda-war-over-papua.html

[26] Cuthbertson, A. (2019, May 23). Indonesia blocks Facebook and WhatsApp features after 'fake news-inspired' riots and deaths. *The Independent*. https://www.independent.co.uk/life-style/gadgets-and-tech/news/indonesia-facebook-whatsapp-ban-blocked-election-riots-a8926706.html

[27] Cuddy, A. (2021, April 1). Myanmar coup: What is happening and why? *BBC*. https://www.bbc.com/news/world-asia-55902070; Reuters Staff. (2021, Jan. 31). Explainer: Crisis in Myanmar after army alleges election fraud. *Reuters*. https://www.reuters.com/article/us-myanmar-politics-explainer/explainer-crisis-in-myanmar-after-army-alleges-election-fraud-idUSKBN2A113H

[28] Guest, P. (2021, Feb. 2). *How misinformation fueled a coup in Myanmar.* Rest of World. https://restofworld.org/2021/how-misinformation-fueled-a-coup-in-myanmar/

[29] Mahtani, S. & Cabato, R. (2019, July 26). Why crafty Internet trolls in the Philippines may be coming to a website near you. *Washington Post*. https://www.washingtonpost.com/world/asia_pacific/why-crafty-internet-trolls-in-the-philippines-may-be-coming-to-a-website-near-you/2019/07/25/c5d42ee2-5c53-11e9-98d4-844088d135f2_story.html

[30] Chang, A. (2020, Feb. 3). 'A Thousand Cuts' documentary tracks disinformation in Duterte's Philippines. *NPR*. https://www.npr.org/2020/02/03/802392333/a-thousand-cuts-documentary-tracks-disinformation-in-dutertes-philippines

[31] Zhdanova, M., & Orlova, D. (2019). Ukraine: External threats and internal challenges. In S. C. Woolley & P. N. Howard (Eds.),*Computational propaganda: Political parties, politicians, and political manipulation on social media* (pp. 41-63). Oxford University Press.

[32] Fedchenko, Y. (2016, March 21.) *Kremlin propaganda: Soviet active measures by other means.* StopFake. http://www.stopfake.org/en/kremlin-propaganda-soviet-active-measures-by-other-means; Jankowicz, N. (2019, April 17). Ukraine's election is an all-out disinformation battle. *The Atlantic*. https://www.theatlantic.com/international/archive/2019/04/russia-disinformation-ukraine-election/587179/

[33] Gursky, J., Glover, K., Joseff, K., Riedl, M.J., Pinzon, J., Geller, R., & Woolley, S. C. (2020, October 26). Encrypted propaganda: Political manipulation via encrypted messages apps in the United States, India, and Mexico. *Center for Media Engagement*. https://mediaengagement.org/research/encrypted-propaganda

[34] Woolley, S. C., & Guilbeault, D. (2019). United States: Manufacturing consensus online. In S. C. Woolley & P. N. Howard (Eds.), *Computational propaganda: Political parties, politicians, and political manipulation on social media* (pp. 185-211). Oxford University Press.

[35] Hatmaker, T. (2018, May 1). Facebook's Free Basics program ended quietly in Myanmar last year. *TechCrunch*. https://techcrunch.com/2018/05/01/facebook-free-basics-ending-myanmar-internet-org/; Tobin, M. (2021, June 8). *How Facebook Discover replicated many of Free Basics' mistakes.* Rest of World. https://restofworld.org/2021/facebook-connectivity-discover/.

[36] Hatmaker, T. (2018, May 1). Facebook's Free Basics program ended quietly in Myanmar last year. *TechCrunch.* https://techcrunch.com/2018/05/01/facebook-free-basics-ending-myanmar-internet-org/ ; Tobin, M. (2021, June 8). *How Facebook Discover replicated many of Free Basics' mistakes.* Rest of World. https://restofworld.org/2021/facebook-connectivity-discover/.

[37] Howard, A. B. (2019, Jan. 26). *How adding friction to group messaging can help defuse disinformation.* Defusing disinfo. https://defusingdis.info/2019/01/26/how-adding-friction-to-group-messaging-can-help-defuse-disinformation/

[38] Stanford Internet Observatory. *Balancing trust and safety on end-to-end encrypted platforms.* Stanford Internet Observatory. https://cyber.fsi.stanford.edu/io/content/e2ee-workshops

[39] Meedan. (2020, Dec. 7). *Promoting WhatsApp tiplines: Insights from our fact-checking partner's promotional campaigns.* Meedan. https://meedan.com/blog/promoting-whatsapp-tiplines-insights-from-our-fact-checking-partners/

[40] Meedan. (2020, Dec. 7). *One year of running the WhatsApp end-to-end fact-checking project.* Meedan. https://meedan.com/blog/one-of-year-of-running-the-end-end-to-fact-checking-project/