



Countering Foreign Malign Social Network Manipulation in the Homeland

Emerging Trends: Technologies, Tactics and Techniques
July 2022



Countering Foreign Malign Social Network Manipulation in the Homeland - Emerging Trends: Technologies, Tactics and Techniques

Abstract

The team has brought together professionals from the private sector tech industry, including a social media platform and the Department of Defense in order to identify and examine what technologies and social media platforms, tactics, and techniques are on the horizon by state and non-state actors for sowing discord within the United States. Some of the technologies that the team has been exploring include communication platforms (WhatsApp, Discord, Telegram) and the developing integration of Virtual Reality(VR)/Augmented Reality(AR) and Artificial Intelligence (AI) into the broader social media experience. The team has conducted research through open-source reporting, and provided insight from professional experiences, as well as brought on subject matter experts as guest speakers to provide context and further guide the discussion and research of the topic. The scope of the team's research is the identification of emerging trends in what social media platforms are being exploited, as well as the tactics and techniques that are unique to individual platforms. Our intent is to identify these trends in order to provide cautionary guidance to both the public and private sectors, especially in the leadup to an election cycle.

DISCLAIMER STATEMENT: The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Companies whose analysts participated in the Public-Private Analytic Exchange Program. This document is provided for educational and informational purposes only and may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.



**Homeland
Security**

Team Members

MEMBERS	COMPANY/AGENCY
Champion: Dana LaFon	NSA
Champion: Trisha Ripley	ODNI
Alexandra Armstrong	American Express
Michael Ficht	FBI
Wesley Moy	Johns Hopkins University
Darrell Hall	Department of Health and Human Services
Taylor Price	Dell Technologies
Janice R.	Department of Defense
Eric Schorr	Snap Inc.
Christine Sublett	Sublett Consulting, LLC.
Kimberly Young	DHS/I&A

Outline

- Cover Page
- Abstract
- Introduction
- Social media/Messaging apps
 - Tiktok
 - Discord
 - Whatsapp
 - Telegram
- Virtual Reality/Augmented Reality
- Gamification
- Clickbait
- Key findings
- Potential impacts
 - Case Study – Midterm Elections
- Recommendations
 - Private
 - Public
- Analytic Dissemination Plan
- Sources



Introduction

As technology changes and evolves, so will the tactics and techniques of those seeking to exploit that technology. Disinformation operations targeting the United States, both the public and the private sectors, continue to reflect the evolution of how our society uses technology to connect and communicate, especially via social media.

While disinformation operations continue to use traditional social media, such as Twitter and Facebook, malicious entities have expanded to new social media platforms such as Tiktok, as well as more targeted messaging apps like WhatsApp, Discord, and Telegram. These platforms each present a unique challenge compared to previous social media platforms. Emerging technologies like Virtual Reality/Augmented Reality (VR/AR) will continue to alter the ways people consume, share, and even experience information. New technologies, tactics, and techniques can also be harnessed in order to combat and mitigate the threat of disinformation.

The report below will analyze the unique nature, and therefore challenges, of these emerging technologies, and therefore the unique challenges to mitigating threats of disinformation. The 2022 midterm elections are expected to be a live display of how these new technologies, tactics, and techniques can be used to exploit the inherent tumultuous civil discourse that revolves around elections. Key findings derived from the analysis of the emerging technologies are translated into recommendations for the public and private sector to work together in order to combat disinformation operations that threaten the homeland.



Social Media/Messaging Apps

TikTok

The social media app “TikTok” was created by the Beijing-based software company “ByteDance” in 2018 and was originally only available for download in mainland China. Within one year, TikTok had gained over one billion users with the app's success, largely attributed to the algorithm designed to track each user’s history, likes, frequent searches, etc. targeting users with tailored content to retain user interaction. The algorithm reportedly also tracks user language preference, device types, and the country in which the account is based.ⁱ

Despite its original debut in the country, TikTok is now banned in China, as well as Bangladesh, Indonesia, Armenia, and Pakistan for privacy concerns. Additionally, TikTok was nearly banned in the United States after former President Trump’s administration claimed TikTok was selling American user information to the Chinese government to spread propaganda and interfere with the 2020 election cycle. Any attempts to ban the app were stifled after the Trump administration abandoned their own efforts to have Oracle and Walmart buy the platform and cut any connections to China after former President Trump lost the 2020 presidential election. While TikTok originally sparked debate over allegedly selling US citizens' PII (personally identifiable information) to China, a recent concern coming to light regarding TikTok is the app's ability to act as a platform to spread disinformation.

According to a visual investigations expert at the New York Times, TikTok’s rapid dissemination of content makes sharing disinformation easy for even novice malicious actors. Falsified images and videos quickly go “viral” while posts debunking the disinformation are often significantly less viewed and do not reach the target audience. In a study conducted by NewsGuard in September 2021, nine children aged 9 to 17 were instructed to create TikTok accounts and within 35 minutes of using the platform, all but one (88.89 percent) were shown misinformation related to COVID-19, and two-thirds (66.67 percent) were shown misinformation specific to COVID-19 vaccines.ⁱⁱ While disinformation varies from misinformation due to its deliberate malicious intent, this study indicates content is often not fact-checked and therefore an effective platform from which to conduct malicious information operations.

WhatsApp/Discord/Telegram

While major social media platforms Twitter and Meta-owned Facebook have been the focus of much of the scrutiny in the misinformation space over the last several years, WhatsApp (also owned by Meta), Discord, and Telegram have garnered wider attention in light of their prevalent use for the spread of misinformation, particularly in connection to the COVID-19 pandemic and more recently with the Russia-Ukraine conflict.ⁱⁱⁱ



WhatsApp is a global instant messaging (IM) and Voice Over Internet Protocol (VoIP) application owned by Meta Platform (previously Facebook). The platform allows users to send text and voice messages, make voice and video calls, and share media content such as images, videos, documents and other content. As of 2015 it is the world's most popular messaging application, with an estimated over 2 billion users globally according to publicly available data from February 2020. It is considered the primary means of internet communication in regions including Latin America, the Indian subcontinent and large parts of Europe and Africa.

In 2018, a New York Times investigation on the use of social media in politics discovered that WhatsApp was being abused for the spread of disinformation related to the 2018 presidential elections in Brazil.^{iv} More recently, one of the most significant challenges in the moderation space for WhatsApp has been combating COVID-19 related misinformation.^v As messages can be rapidly shared on the platform by “forwarding” content to either individual users or private groups of users, WhatsApp has repeatedly imposed limits on message forwarding in order to curb the spread of health-related misinformation.^{vi} This proactive measure was used prominently during the height of the pandemic in countries such as India (where WhatsApp has an estimated over 200 million users) as well as in Australia.^{vii} Limits on message forwarding were first introduced in 2018 to combat general spam, with the platform noting an estimated 70% drop in the spread of such content in 2020.^{viii,ix} The measure was then expanded in 2021 in further response to the COVID-19 pandemic and remains in place today.^x

Discord is a VoIP and instant messaging social communications platform. Users of the platform can interact and communicate with voice calls, video calls, instant chat messaging and can share media files such as pictures and videos in community channels called “servers”. Servers are a collection of chat rooms and voice channels. As of 2022, Discord has an estimated over 350 million registered users and over 150 million monthly active users.^{xi}

Discord rose in popularity with the alt-right due to the private and anonymous aspects of the platform. In early 2017, Discord's leadership admitted to awareness of its platform being used by far-right and hate groups, highlighting that any groups engaged in illegal activities or violating the platform's terms of service would be removed.^{xii,xiii} Discord's move to a more proactive stance against the spread of disinformation and violent content on its platform however became more forceful following the deadly Unite the Right rally in Charlottesville, Virginia, on August 12, 2017.^{xiv} It was reported after the events of Charlottesville that the rally organizers had utilized Discord to plan and communicate in preparation for the rally. Discord ultimately reacted by shutting down servers associated with the alt-right and far-

right movements that had been involved in Charlottesville, and banning other users who had participated in associated servers. In April 2021, Discord reported that it had “removed more than 2,000 communities dedicated to extremism and other violent content” in late 2020 and was actively engaged in further removing these groups and their content from the platform.^{xv}

On February 25, 2022, Discord officially announced an update to its Community Guidelines, introducing a new provision that disallows any form of misinformation on the platform. Specifically, Discord’s new provision states, “users may not share false or misleading information on Discord that is likely to cause physical or societal harm”. Discord’s announcement was made in response to ongoing criticism and scrutiny tied specifically to the spread of misinformation related to COVID-19 and health-related topics, with the company stating that it hopes “this new rule will be an effective countermeasure against dangerous medical-related falsehoods – both during the pandemic and after its conclusion.”^{xvi}

Telegram is a cross-platform (both mobile and web) cloud-based instant message (IM) service. The service also provides end-to-end encrypted video calling, file sharing, and additional communications features. As of June 2022, Telegram had over 700 million active users worldwide – more than the individual user bases of Twitter, Snapchat, or Discord.^{xvii} It is the fifth most-popular messaging app after Meta-owned WhatsApp and Facebook Messenger, as well as WeChat and QQ, which currently dominate the Chinese messaging app market.

Over the last several years, Telegram has become an inviting platform for bad actors, particularly those seeking to rapidly spread mis/disinformation to mass audiences.^{xviii} Telegram itself does not have formal rules against spreading disinformation, and the application’s founder has publicly stated his disapproval of content moderation and removal.^{xix} Among Telegram’s most attractive features are its public and private channels, where content is broadcast one-way by the channel administrators or owners, and which can have an unlimited number of subscribers. Additionally, Telegram also has groups, which can have as many as 200,000 individual users. Content shared within these groups can be easily forwarded within the platform as well as downloaded by individual users and then spread via other social and digital media platforms.

In Eastern Europe in particular, Telegram is being used as a multifaceted communication tool. In a more recent prominent example, Telegram is being used to organize Ukrainian resistance, connect families separated by the conflict, and even share media from conflict zones.^{xx} Media from the war, especially videos and pictures of Russian and Ukrainian



activities in civilian areas potentially associated with war crimes, is being collected by non-governmental organizations, the Ukrainian government, and other entities, for future use at The Hague.

In contrast, Telegram is also being used by both state and non-state Russian actors to spread pro-Russian narratives about the conflict in Ukraine and to censor any contradictory evidence.^{xxi} Following Russia's invasion of Ukraine, many of the world's largest social and digital media platforms either removed their presence and products from the Russian market or were banned by the Russian state directly. Telegram however, is one of the only remaining global messaging applications operating in Russia, with reportedly over 50 million individual Russian users.^{xxii} Pro-Russian Telegram channels often feature state propaganda such as videos and images, as well as messaging put out directly from the Kremlin. Telegram has also acquiesced to Russian government demands regarding political censorship, notably shutting down Russian political bots associated with the Russian opposition in September 2021.^{xxiii}

On the domestic front, Telegram has also come under scrutiny for its use by far-right extremists in the United States. In the wake of the January 6 riot on Capitol Hill, Telegram issued a rare takedown order for channels associated with white supremacist and neo-Nazi groups on its platform, citing terms of service that explicitly forbid public calls for violence.^{xxiv} Telegram has previously garnered heavy criticism for its failure to properly moderate viral disinformation trends such as QAnon content as well as COVID-19 misinformation related to the virus itself as well as COVID-19 vaccines.^{xxv}

Fighting the spread of disinformation on Telegram however has become a more significant challenge for countries where the app is still allowed legally given the private and encrypted nature of the application. Telegram has often acquiesced to national governments seeking to disincentivize the platform's use as a method of disinformation. In Brazil, for example, the application was blocked in March 2022 over concerns with the spread of disinformation ahead of elections.^{xxvi} Two months later in May 2022, the Brazilian Electoral Court and Telegram signed an agreement to fight disinformation in the country.^{xxvii} In Iran, however, Telegram has been effectively banned since 2018, when the Iranian government cracked down on the application's use as a means of connecting to channels and groups outside of the country.^{xxviii}

Still, there are also more proactive measures that may be useful in combating misinformation on Telegram in particular. Writing for Reuters Institute and the University of Oxford in October 2021, journalist Bermet Talant writes,



“According to journalists and digital researchers from Ukraine, Brazil, Germany, Canada, Belarus, and Spain that I interviewed about Telegram, there are ways to address the issue – both on and off the platform. These include investigating Telegram movements and their political or financial interest, producing more responsible journalism, getting clearer communication from governments, and following the continued moderation efforts on other social media platforms.”^{xxix}

In addition, “media outlets and public organizations could themselves take advantage of Telegram’s broadcasting functionalities and chatbots to reach broader audiences and build communities”, essentially fighting the misinformation with real information.^{xxx} While Talant’s recommendations are focused on the journalism sector, they are also applicable to other groups and entities attempting to fight the spread of misinformation, including in the government and within the broader private sector.

Virtual Reality/Augmented Reality

Virtual and augmented reality technologies have been around for a couple of decades but are entering a new phase of adoption and use by everyday consumers, as well as businesses and educators.^{xxxi} VR/AR offer users an immersive experience, a way to make the user “feel part of what is being presented to them”. The ability to further stimulate an emotional reaction when engaging with content is another attack capability to spread disinformation and manipulate the content consumer.^{xxxii}

“Misinformation and propaganda are already present concerns,” says Saleem Khan (a Toronto-based journalist and VR advisor). “But with immersive technology like virtual reality there’s a fundamental difference: When you’re immersed in an experience, the brain registers it differently than if you’re reading an article or watching a video. A different part of the brain is active; what you see or hear here in the VR experience is recorded as a real memory.”^{xxxiii}

According to a Pew Research Center survey, more than 80% of Americans get their news from digital devices and 53% receive news from social media with younger consumers preferring digital platforms over traditional.^{xxxiv} Virtual Reality (different reality immersion) and Augmented Reality (different visual experience within a real environment^{xxxv}) are expected by some to become the next big social media experience, even replacing some everyday interactions.^{xxxvi} This leaves Americans already poised to consume information from social media vulnerable to exploitation of an emerging technology designed to trigger an emotional reaction more effectively than traditional news sources. This type of information consumption environment is a uniquely effective delivery mechanism for disinformation.

“Virtual and augmented reality are creating new, immersive experiences for audiences. We can “feel” stories rather than just watching or reading them. But is more emotion what’s really missing from news? Will feelings be the new facts?”^{xxxvii}

Industry watchers are concerned social media companies already challenged with moderating content and mitigating the spread of disinformation on simpler platforms will be completely unprepared to prevent the problem becoming worse in the metaverse.^{xxxviii}

Gamification

As misinformation spread and radicalization evolved, right-wing extremist groups have taken to recruiting, training, and communing with users as young as 13 years old on popular gaming platforms. These country agnostic spaces leverage memes and code phrases to circumvent content filters and censors; i.e. “commit not alive” to refer to suicide or murder^{xxxix}. Most of the children and adults who are exposed to these channels are either already radicalized or quickly become so off-platform in search of community. Some of the longest, most entrenched extremist groups exist in channels on the popular gaming platform Steam where they have a wide chance of exposure^{xl}. Most have not been removed from Steam because they conduct radicalization off-platform, but initial vetting on Discord channels often includes ideology questionnaires and “skin color checks”^{xli}. Extremists “off-ramp”^{xlii} vetted prospects to blogs, encrypted messaging, and “alt-tech” social media platforms that either cannot intervene to prevent the promotion of hate speech or extremism due to lack of a centralized control or visibility, or **will** not intervene due to adherence to an absolutist vision of free speech or outright support of the extremist ideologies.

Capital Suitors with Political Motivation, per the alignment chart coined by Doublethink Labs^{xliii}, oftentimes employ a multi-platform streaming strategy with chat shows and podcasts, promoting extreme right wing ideologies and drawing more viewers than if they were solely to rely on gaming streams^{xliv}. This builds audiences, fosters a sense of community with followers, and monetizes via donations or answering paid questions. Gaming tournaments hosted by right-wing groups are amplified by negative media coverage, which makes them seem “cool” and provides legitimacy to their efforts^{xlv}. The popular streaming platform Twitch mostly battles with sporadic, small-scale content and influencers, which is possibly reflective of the network’s stricter controls^{xlvi}. The less regulated DLive streaming platform has a concentration of right-wing streamers, mostly due to lack of other options rather than platform preference, and many have expressed plans to move to the Odysee and Trovo platforms out of frustrations with User Experience/User Interface (UE/UI) and network reliability^{xlvii}.

These extremist communities strengthen in-group affiliation through live-streamed activities including:

- Raiding^{xlvi} - gamified online harassment and coordinated trolling activity against their political opponents, to include racial minority and LGBTQ persons and groups
- Omegle Redpilling^{xlix} - using the live video chat platform Omegle which pairs users with another random user to troll and spew racist content when they encounter someone of another race

Mastodon, a decentralized, open-source social networking platform found themselves raided and occupied by extremists who fled Twitter to create an “instance” called “Gab” on Mastodon’s “fediverse”.^l Mastodon’s platform gives users a high level of structural control to create instances which can either be connected to other instances in Mastodon’s fediverse, or which can operate entirely autonomously. This left no centralized way to remove Gab, but the Mastodon community collectively banded together to starve the Gab instance of access to the rest of the fediverse. Introduced in May 2019, the Mastodon Server Covenant was instrumental to this war of attrition by requiring instances to agree to a series of conditions, including “active moderation against racism, sexism, homophobia and transphobia” in exchange for being listed on Mastodon’s main instance. While this did not stop instances from existing, it provided a formal basis for excluding Gab and other potentially harmful communities from the amplification of being listed by the main Mastodon instance. Much as extremists are leaving DLive over UE/UI complaints^{li}, making Mastodon a complex, frustrating, time-consuming, and costly experience for Gab users and Gab operators seemingly succeeded in driving out Gab as of December 2020.

Additionally in the fight against misinformation, gamification has arisen as a strategy to help the average user spot, rethink, and counter misinformation on a holistic level, to go beyond specific fact checking and content moderation efforts. Topic-based games such as CoronaChampion focus on specifically immersing users to debunk myths around COVID-19, while skill-based games like Go Viral, Bad News, and Harmony Square take an offensive approach to misinformation inoculation by putting users in the driver’s seat to spread sensational but fake information to advance through each level^{lii}. These puzzle interactions and quizzes train users how to spot false information and be better informed citizens by guiding them through a slowed down discernment process as they consume information in-game. A study assessing Harmony Square tested users before and after the game to see how handily they spotted misinformation, and found that players post-game:

- found misinformation significantly less reliable
- were significantly more confident in their assessment
- were significantly less likely to share misinformation in their social network
- were not impacted by their political ideology during the learning process
- improved at spotting emotionally exploitative and polarizing language
- built cognitive resistance and psychological immunity for at least one week, and longer with skill reminders or “booster shots”

While not assessed for Harmony Square specifically, research has shown that gamified inoculation effects can persist for months^{liii}.

Clickbait

With the constantly increasing bar to have "verified" accounts, financially motivated misinformation peddlers, often internationally based, frequently age and verify groups of accounts, many as gaming streams or other content to add legitimacy, and then repurpose them with false and sensational videos until the platform notices the change^{liv}. The goal is quick clicks, not long-term influence^{lv}, so some of these videos are regular postings of videos using AI-generated voice readings of articles with conspiracy content or divisive political narratives^{lvi}. Platforms have more difficulty automatically removing videos that use homoglyphs in the video or article titles to evade content moderation algorithms^{lvii}. Monetization of these videos mainly comes from leveraging^{lviii}:

- they are quick to upload and generate ad revenue
- affiliate product advertising directs people to other websites for trinkets, flags, or vitamin supplements and pays original site by click
- donation solicitation for patriotic causes or animal welfare funds.

Key Findings

TikTok's success is largely attributed to an algorithm designed to track each user's history, likes, frequent searches, etc. targeting users with tailored content to retain user interaction; however, TikTok's rapid dissemination of content makes sharing disinformation easy for even novice malicious actors. Falsified images and videos quickly go "viral" while posts debunking the disinformation are often significantly less viewed and do not reach the target audience. Therefore, TikTok serves as an easily accessible platform for malicious actors to spread disinformation and conduct influence operations.

Among the aforementioned digital communications applications, Telegram currently poses the greatest challenge for the spread of disinformation given its lack of specific terms of service against such activities and its purposeful disregard for moderating content that does not fall under a specific set of criteria (i.e. calls for violence). Both WhatsApp and Discord have made progress in their respective efforts for countering the spread of disinformation, with the implementation of mechanisms such as limits on message forwarding (WhatsApp) and updated provisions disallowing any form of misinformation (Discord).

Game platforms offer ways to both spread and combat misinformation, which will be delivered to users often without them even seeking it. Similarly, clickbait misinformation plays on victims' emotions and patriotism for financial gain, even when the MDM operators lack a political agenda.

VR/AR technology offers new ways for users to consume media, even "experience it". Reality and truth can be distorted in an increasingly believable way, which can degrade a person's ability to filter out disinformation.

Other findings:

- Content-based moderation helps remove specific harmful content but does not address algorithmic amplification of bad content
- Text-only comments limit fact-checking
- Lack of effective content-labeling and moderation on most platforms
- “Negative” content often has more engagements than “positive”
- Limits on the ability of individual actors to spread information and/or content virally (i.e. mass forwarding) have helped combat this trend
- Companies require concrete terms of service and user provisions specifically against the abuse of their respective platforms for the spread of viral disinformation

Potential Impacts

Case Study / 2022 Midterm Elections

Elections are a prime target for disinformation operations, especially for malicious state actors seeking to manipulate the voting population and degrade civil discourse. For example, during the 2016 election, “Black and Latino voters were targeted, receiving text messages that they could cast their vote for Democratic candidate Hillary Clinton on their phones instead of going to a voting location.”^{lix}

Lawmakers were recently warned during an election hearing that the 2022 midterm elections will be no different, and were specifically cautioned about conspiracy theories spreading on social media about election fraud.^{lx}

“Election misinformation remains rampant online. This month, “2000 Mules,” a film that falsely claims the 2020 election was stolen from Mr. Trump, was widely shared on Facebook and Instagram, garnering more than 430,000 interactions, according to an analysis by The New York Times. In posts about the film, commenters said they expected election fraud this year and warned against using mail-in voting and electronic voting machines.”^{lxi}

Messaging apps like Telegram, Whatsapp and Discord could be used to spread false information about voting options, or conspiracies like election fraud, and the private channels and more familiar group texts on these messaging apps could present the information as more believable and trustworthy since the information is coming from contacts in a community with whom the users are already familiar.

The conflict in Ukraine and COVID-19 pandemic demonstrated how TikTok can be used to not only spread disinformation, especially by “micro-influencers”, but also inundate new users to the platform quickly with misinformation.^{lxii} Younger voters who use TikTok can quickly receive disinformation regarding the election. The “scrolling” nature of the platform

and restriction of media from the comment sections makes refuting disinformation difficult on the platform.^{lxiii}

Newer technology like digital fakes and VR/AR could present unique challenges as well. Mike Rothschild is a journalist who researches conspiracy theories and says that “people who believe these theories believe they are fighting a war between good and evil”.^{lxiv} Rhetoric around elections is usually heightened and could be framed to be an existential crisis, which are ideal conditions for conspiracies to take hold and spread. VR/AR technology can exacerbate this problem by allowing users to “experience” the conspiracy; this immersive experience can trigger a stronger emotional reaction and boost the likelihood of the disinformation and conspiracy theory to be spread and become harder for accurate information to rebut the false information.

Both the public and the private sector should take the lessons learned from the 2016 and the 2020 elections to use what mitigation tactics and policies were effective at combating disinformation and apply it to the 2022 midterm elections (as well as the 2024 election), as well as confront the unique challenges posed by the growing use of newer technologies and platforms, like TikTok, Telegram and VR/AR. Gamification has shown promising results in engaging users to mitigate the spread of disinformation themselves. However, the policies of the social media platforms should shoulder the lion’s share of the responsibility in identifying misinformation and limiting the spread.

Recommendations

Private

- Crack down on and call attention to paid content that is mis- or unlabeled even when payment happens off platform^{lxv}
- Follow and collaborate on continued moderation efforts on other social media platforms
- As it did for the November 2020 election, Meta could freeze political advertising a week before the election; this could slow the spread of misinformation.
- Create reportable categories more than “Other”, to include Doxing and avenues to spot and report bad content
- Avoid publishing user-generated content on news websites
- Balance news value against ease of verification
- Produce more responsible journalism, use expert journalists and correspondents as recurring content creators to build better informed audiences and communities
- Have media outlets and public organizations use Telegram’s broadcasting functionalities and chatbots to reach audiences and build communities
- Fact checking community can disseminate info and improve media literacy with chat bots and gamification



- Work with independent media instead of sole reliance on government
- Create bespoke efforts targeted at communities based on the false narratives they receive
- Leverage successful adversary techniques like brigading
- Implement tiered moderation where content is flagged but not removed in order to map out accounts and networks that re-share it

Public

- Incentivize social media platforms to regulate MDM or risk liability
- Create new criminal categories to address the sharing and disseminating of disinformation
- Investigate Telegram movements and their political or financial interest
- Implement MDM inoculation and media literacy education

Analytic Deliverable Dissemination Plan

US CYBERCOM J25 Partner Engagements

University of Texas, Propaganda Research Center

Project for Democracy and the Internet at Stanford University

The Atlantic Council

MS-ISAC DHS

WhatsApp

Telegram

Discord

TikTok

Meta

Alphabet

The Department of Treasury

Center for Disease Control

The Department of Education



**Homeland
Security**



Sources

Bloomberg | Pub 2021-12-15 | Misinformation Has Already Made Its Way to Facebook's

ChannelNewsAsia | Pub 2022-03-29 | "Commentary: Telegram's lenience on disinformation has made it a valuable tool in the Ukraine war"

The Cold Wire | 2021-08-14 | When Was TikTok Made? (Everything To Know)

Devex | 01 July 2021 | These games target COVID-19 misinformation. But do they work?

Digiday | Pub 2022-03-07 | 'Misinformation on TikTok is a whole different beast' | <https://digiday.com/media/misinformation-on-tiktok-is-a-whole-different-beast-how-publishers-are-tackling-the-ukraine-russia-war-disinformation-problem-on-tiktok/>

Discord Blog | Pub 2022-02-25 | Addressing Health Misinformation

The Guardian | Pub 2021-07-23 | "Facebook forced to limit misinformation spread via WhatsApp amid Sydney lockdown"

Harvard Kennedy School Misinformation Review | NOVEMBER 6, 2020 | Breaking Harmony Square: A game that "inoculates" against political misinformation

Institute for Strategic Dialogue | 19 January 2022 | Conspiracy Clickbait: Farming Facebook

LawfareBlog | Pub 2022-04-06 | Telegram's Embrace of Contradiction

The Moscow Times | Pub 2021-09-27 | "Telegram Messenger Blocks Navalny Bot During Russian Election"

NBCNEWS | July 4, 2022, 8:21 PM EDT / Updated July 5, 2022, 10:46 AM EDT | Highland Park shooting person of interest left online trail of violent imagery

News Guard | Pub 2021-09-20 | According to a visual investigations expert at the New York Times, TikTok's rapid dissemination of content makes sharing disinformation easy for even novice malicious actors

The New York Times | Pub 2018-10-17 | Fake News Is Poisoning Brazilian Politics. WhatsApp Can Stop It.

The New York Times | Pub 2022-06-23 | As Midterms Loom, Elections Are No Longer Top Priority for Meta C.E.O.

The New York Times | Pub 2022-03-18 | "Brazil Blocks Telegram Over Disinformation Concerns"



**Homeland
Security**



NPR | Pub 2021-04-05 | “Group-Chat App Discord Says It Banned More Than 2,000 Extremist Communities”

Ohio Capital Journal | Pub 2022-06-24 | US House Members Warned About Disinformation in Upcoming Campaigns | <https://ohiocapitaljournal.com/2022/06/24/u-s-house-members-warned-about-disinformation-in-upcoming-campaigns/>

PBS | Pub 2021-11-05 | “Millions depend on private messaging apps to keep in touch. They’re ripe with misinformation”

Pew Research | Pub 2021-01-12 | More than eight-in-ten Americans get news from digital devices | <https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/>

Protocol | Pub 2022-03-22 | “In Russia, Telegram has become the messaging app of choice”

QZ | Pub 2018-11-15, Updated 2022-07-20 | How Virtual Reality and Fake News Are Changing the Media | <https://qz.com/1843542/how-virtual-reality-and-fake-news-are-changing-the-media/>

Reuter’s Institute & Oxford University | Pub 2021-10-12 | How journalists can address misinformation on Telegram (Full Academic Paper)

Rock Content | Pub 2020-12-07 | What is an Immersive Experience and How to Use it in Your Marketing | <https://rockcontent.com/blog/immersive-experience/>

Science Direct | Pub 2020-04 | A systematic review of immersive virtual reality applications for higher education | <https://www.sciencedirect.com/science/article/pii/S0360131519303276#b96>

Sierra Sun Times | Pub 2022-05-18 | “U.S. Senator Catherine Cortez Masto Joins Colleagues in Urging WhatsApp, Telegram, and Signal to Stop Spread of Spanish-Language Mis/Disinformation on Their Group Messaging Apps”

TechCruch | Pub 2021-01-13 | “Telegram blocks ‘dozens’ of hardcore hate channels threatening violence”

Telegram | 700 Million Users and Telegram Premium

Vox | Jul 11, 2022, 7:30am EDT | TikTok is full of shady secret advertisements

Vox | Pub 2021-01-20 | “Why right-wing extremists’ favorite new platform is so dangerous”

The Washington Post | Pub 2022-03-28 | “On Telegram, Ignoring Lies Could Protect the Truth in Russia”



**Homeland
Security**

WhatsApp Help Center | How to prevent the spread of misinformation

Wired | Pub 2018-08 | Digital Reality and the Revival of Journalism | <https://www.wired.com/wiredinsider/2018/08/digital-reality-and-the-revival-of-journalism/>

Wired | Pub 2018-06-16 | “The Unexpected Fallout of Iran's Telegram Ban”

ZDNet | Pub 2022-05-19 | “Telegram and the Brazilian Electoral Court sign agreement to fight disinformation”

ⁱ The Cold Wire | 2021-08-14 | When Was TikTok Made? (Everything To Know)

ⁱⁱ News Guard | Pub 2021-09-20 | Toxic TikTok: Popular social-media video app feeds vaccine misinformation to kids within minutes after they sign up

ⁱⁱⁱ Sierra Sun Times | Pub 2022-05-18 | “U.S. Senator Catherine Cortez Masto Joins Colleagues in Urging WhatsApp, Telegram, and Signal to Stop Spread of Spanish-Language Mis/Disinformation on Their Group Messaging Apps”

^{iv} The New York Times | Pub 2018-10-17 | Fake News Is Poisoning Brazilian Politics. WhatsApp Can Stop It.

^v WhatsApp Help Center | How to prevent the spread of misinformation

^{vi} PBS | Pub 2021-11-05 | “Millions depend on private messaging apps to keep in touch. They’re ripe with misinformation”

^{vii} The Guardian | Pub 2021-07-23 | “Facebook forced to limit misinformation spread via WhatsApp amid Sydney lockdown”

^{viii} TechCrunch | Pub 2018-07-19 | WhatsApp limits message forwarding in bid to reduce spam and misinformation

^{ix} TheVerge | Pub 2020-04-27 | “WhatsApp says its forwarding limits have cut the spread of viral messages by 70 percent”

^x NiemanLabs | Pub 2022-04-04 | “WhatsApp seems ready to restrict how easily messages spread in a bid to reduce misinformation”

^{xi} The Wall Street Journal | Pub 2021-03-08 | “What Is Everybody Doing on Discord?”

^{xii} The New York Times | Pub 2017-08-15 | “This Was the Alt-Right’s Favorite Chat App. Then Came Charlottesville.”

^{xiii} The New York Times | Pub 2017-08-18 | “‘The Daily’: The Alt-Right and the Internet”

^{xiv} The Washington Post | Pub 2018-08-07 | “Subpoena for app called ‘Discord’ could unmask identities of Charlottesville white supremacists”

^{xv} NPR | Pub 2021-04-05 | “Group-Chat App Discord Says It Banned More Than 2,000 Extremist Communities”

^{xvi} Discord Blog | Pub 2022-02-25 | Addressing Health Misinformation

^{xvii} Telegram | 700 Million Users and Telegram Premium

^{xviii} LawfareBlog | Pub 2022-04-06 | Telegram’s Embrace of Contradiction

^{xix} Ibid.

^{xx} ChannelNewsAsia | Pub 2022-03-29 | “Commentary: Telegram's lenience on disinformation has made it a valuable tool in the Ukraine war”

^{xxi} The Washington Post | Pub 2022-03-28 | “On Telegram, Ignoring Lies Could Protect the Truth in Russia”

^{xxii} Protocol | Pub 2022-03-22 | “In Russia, Telegram has become the messaging app of choice”

^{xxiii} The Moscow Times | Pub 2021-09-27 | “Telegram Messenger Blocks Navalny Bot During Russian Election”

^{xxiv} Vox | Pub 2021-01-20 | “Why right-wing extremists’ favorite new platform is so dangerous”

^{xxv} TechCruch | Pub 2021-01-13 | “Telegram blocks ‘dozens’ of hardcore hate channels threatening violence”

^{xxvi} The New York Times | Pub 2022-03-18 | “Brazil Blocks Telegram Over Disinformation Concerns”



- xxvii ZDNet | Pub 2022-05-19 | “Telegram and the Brazilian Electoral Court sign agreement to fight disinformation”
- xxviii Wired | Pub 2018-06-16 | “The Unexpected Fallout of Iran's Telegram Ban”
- xxix Reuter’s Institute & Oxford University | Pub 2021-10-12 | How journalists can address misinformation on Telegram (Full Academic Paper)
- xxx **ibid.**
- xxxi Science Direct | Pub 2020-04 | A systematic review of immersive virtual reality applications for higher education
- xxxii Rock Content | Pub 2020-12-07 | What is an Immersive Experience and How to Use it in Your Marketing
- xxxiii Wired | Pub 2018-08 | Digital Reality and the Revival of Journalism
- xxxiv Pew Research | Pub 2021-01-12 | More than eight-in-ten Americans get news from digital devices
- xxxv Rock Content | Pub 2020-12-07 | What is an Immersive Experience and How to Use it in Your Marketing
- xxxvi Bloomberg | Pub 2021-12-15 | Misinformation Has Already Made Its Way to Facebook’s Metaverse
- xxxvii QZ | Pub 2018-11-15, Updated 2022-07-20 | How Virtual Reality and Fake News Are Changing the Media
- xxxviii Bloomberg | Pub 2021-12-15 | Misinformation Has Already Made Its Way to Facebook’s Metaverse
- xxxix NBCNEWS | July 4, 2022, 8:21 PM EDT / Updated July 5, 2022, 10:46 AM EDT | Highland Park shooting person of interest left online trail of violent imagery | pp6
- xl Institute for Strategic Dialogue | 12 August 2021 | Gamers Who Hate: An Introduction to ISD’s Gaming and Extremism Series | p8
- xli Institute for Strategic Dialogue | 19 August 2021 | Gaming and Extremism: The Extreme Right on Discord | p5
- xlii Institute for Strategic Dialogue | 12 August 2021 | Gaming and Extremism: The Extreme Right on Steam | p4
- xliii Doublethink Lab | Oct 24, 2020 | Deafening Whispers: China’s Information Operation and Taiwan’s 2020 Election | p15
- xliv Institute for Strategic Dialogue | 26 August 2021 | Gaming and Extremism: The Extreme Right on DLive | p5
- xlv Institute for Strategic Dialogue | 26 August 2021 | Gaming and Extremism: The Extreme Right on DLive | p6
- xlvi Institute for Strategic Dialogue | 2 September 2021 | Gaming and Extremism: The Extreme Right on Twitch | p4
- xlvii Institute for Strategic Dialogue | 26 August 2021 | Gaming and Extremism: The Extreme Right on DLive | p7
- xlviii Institute for Strategic Dialogue | 12 August 2021 | Gamers Who Hate: An Introduction to ISD’s Gaming and Extremism Series | p9
- xliv Institute for Strategic Dialogue | 2 September 2021 | Gaming and Extremism: The Extreme Right on Twitch | p4
- l Institute for Strategic Dialogue | 28 September 2021 | Open Source, Self Defence: Tackling the Challenge of Extremist Websites and Open Source Tech | p12
- li Institute for Strategic Dialogue | 26 August 2021 | Gaming and Extremism: The Extreme Right on DLive | p7
- lii devex | 01 July 2021 | These games target COVID-19 misinformation. But do they work?
- liii Harvard Kennedy School Misinformation Review | NOVEMBER 6, 2020 | Breaking Harmony Square: A game that “inoculates” against political misinformation | p4
- liv Institute for Strategic Dialogue | 19 January 2022 | Conspiracy Clickbait: Raking in the Views | p7
- lv Institute for Strategic Dialogue | 19 January 2022 | Conspiracy Clickbait: Raking in the Views | p8
- lvi Institute for Strategic Dialogue | 19 January 2022 | Conspiracy Clickbait: The Art of the (Affiliate Marketing) Deal | p12
- lvii Institute for Strategic Dialogue | 19 January 2022 | Conspiracy Clickbait: Farming Facebook | p14
- lviii Institute for Strategic Dialogue | 19 January 2022 | Conspiracy Clickbait: Farming Facebook | p6-8,12
- lix Ohio Capital Journal | Pub 2022-06-24 | US House Members Warned About Disinformation in Upcoming Campaigns |
- lx Ohio Capital Journal | Pub 2022-06-24 | US House Members Warned About Disinformation in Upcoming Campaigns
- lxi New York Times | Pub 2022-06-23 | As Midterms Loom, Elections Are No Longer Top Priority for Meta C.E.O.

^{lxii} News Guard | Pub 2021-09-20 | According to a visual investigations expert at the New York Times, TikTok’s rapid dissemination of content makes sharing disinformation easy for even novice malicious actors

^{lxiii} Digiday | Pub 2022-03-07 | ‘Misinformation on TikTok is a whole different beast’

^{lxiv} Ohio Capital Journal | Pub 2022-06-24 | US House Members Warned About Disinformation in Upcoming Campaigns

^{lxv} Vox | Jul 11, 2022, 7:30am EDT | TikTok is full of shady secret advertisements | pp3

