Signals, Narratives, and Future Risks:

Mapping Myanmar's Information Ecosystem in 2025

The Red Flag

Signals, Narratives, and Future Risks: Mapping Myanmar's Information Ecosystem in 2025

Five years after the 2021 military coup, Myanmar's information ecosystem has become increasingly distorted and weaponized. This report presents The Red Flag's annual analysis of key signals, narratives, and future risks observed throughout 2025, drawing on systematic monitoring of digital platforms to inform research, advocacy, and civilian protection efforts.

Published by: The Red Flag

Year of Publication: 2025

Geographic Focus: Myanmar

Platforms Monitored: Facebook, Telegram, TikTok, YouTube

CONTENTS

THE RED FLAG

INTRODUCTION

Five years after the 2021 military coup, Myanmar is experiencing a protracted and multifaceted crisis characterized by severe humanitarian deterioration, systematic human rights violations, economic disintegration, and escalating armed conflict, collectively placing the country at significant risk of state failure. Myanmar's information ecosystem has become deeply distorted and repressive, fostering the pervasive misuse of information through propaganda, disinformation, hate speech, and the deliberate targeting of civilians. At the same time, much of the rest of the world advances toward more constructive applications of technology, including artificial intelligence, cryptocurrency systems, and digital governance.

The Red Flag has been monitoring and engaging with Myanmar's information ecosystem with two primary objectives: (1) strengthening information resilience and (2) promoting information integrity by countering misinformation and disinformation within communities and across social media platforms. Drawing on a sequence of studies and analyses, 2025 emerges as a critical year marked by significant political changes, the construction of dominant trends and narratives, widespread societal struggles, cross-border online scamming activities, mass migration, and escalating civilian casualties with profound physical and psychological impacts. This report presents an annual analysis of The Red Flag's information ecosystem monitoring, aiming to document key trends and narratives throughout the year, identify dominant forms of propaganda, examine platform-specific dynamics, and contextualize major events in 2025. It further distills lessons learned and outlines emerging trends and narratives likely to shape the information ecosystem in the coming years.

■ ■ ■

Methodology

For research, advocacy and civilian protection purposes, The Red Flag monitors four major platforms where harmful and influential content spreads widely; Facebook, Telegram, TikTok and Youtube.These platforms are chosen because they are widely used for political discussions, information sharing, and coordinated campaigns within the Myanmar Community. With the content categories, The Red Flag classify all collected content into four key categories;

1. Fact-check (Suspicious or false information)
   - » Misleading news, rumours, manipulated media, propaganda.
2. Dangerous Content
   - » Posts that may incite violence, threats, doxxing, intimidation, or risk to civilians.
3. Intel' (Research-relevant content)
   - » Information useful as evidence for documentation, human rights monitoring, or mapping actors/events.
4. Hate Speech / Keywords
   - » Words, phrases, or coded language used to target groups or individuals.

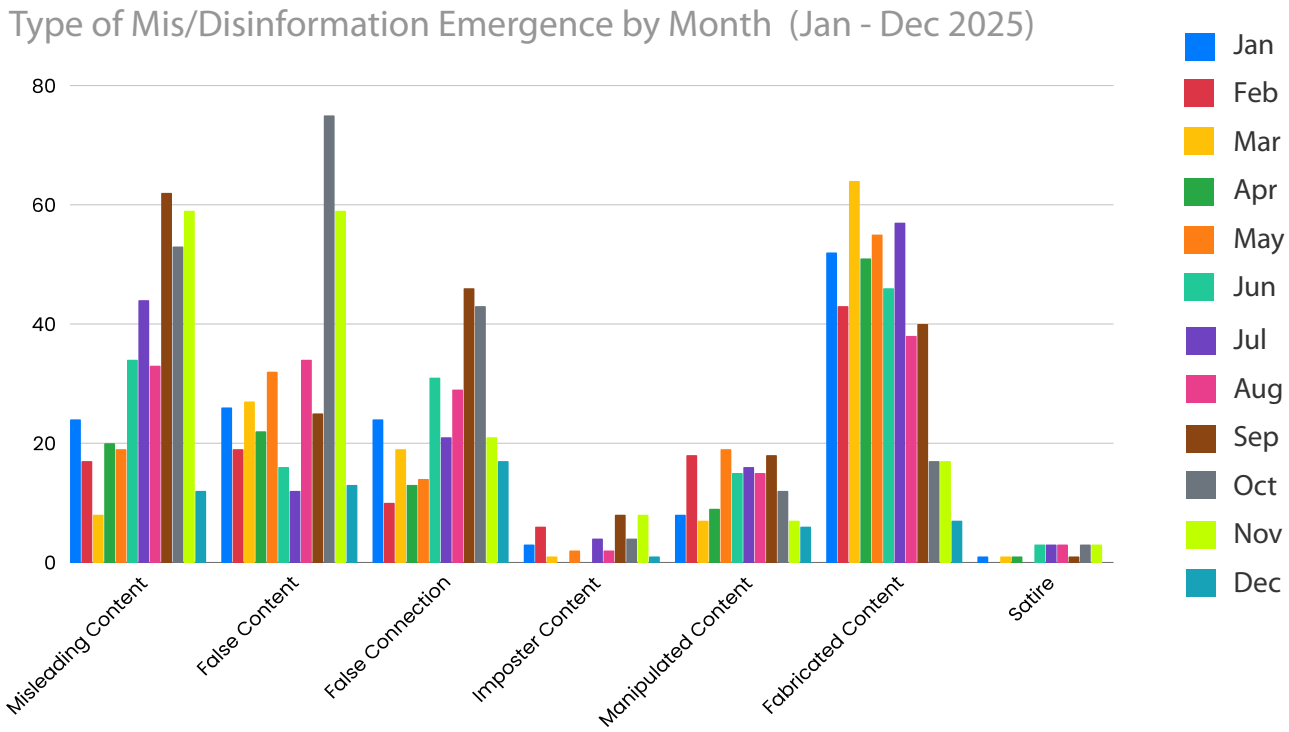
These categories help and show how each type of content impacts society and human rights.

To support research and accurate record-keeping, the monitoring team collects content daily from the four platforms through systematic scanning and observation. All findings are recorded in The Red Flag's internal dataset, developed in line with The Red Flag's data policy, security protocols, and data entry standards. For the verification and analysis, the team manages to fact-check from credible news sources, trusted local networks and using the fact-check tools, i.e., OSINT (Open Source Intelligence) Tools and cluster the themes. The team uses a centralized database to store all collected entries, categories and subcategories, verified findings, screenshots and evidence to ensure consistency and supports long-term analysis. Based on this the team produces daily, weekly, monthly and yearly highlighting: Daily Alert, Briefing, Key trends and narratives, case studies, quarterly analysis and yearly analysis to partners, stakeholders and team. These specific deliverables support partners and internal teams by highlighting emerging risks, key narratives, misinformation flows, digital threats, and patterns of online harm.

■ ■ ■

Monthly Types of Mis/Disinformation Trends

A line graph shows monthly mis/disinformation (Type of mis/disinformation) over the past year, from January to December, with different colored lines representing various categories of mis/disinformation.



Over 1599 pieces of potential misinformation and disinformation were recorded through monitoring and subsequently filtered out through fact-checking. Based on the results of the fact-checking process and categorization of these data, this section analyzes the key characteristics and patterns of the most common types of misinformation by propagandists which are identified during the initial phase of monitoring and fact-checking. Four dominant forms of information manipulation emerged: Misleading Content, False Content, False Connection, and Fabricated Content.

These commonly include attempts to discredit EAOs and PDFs through selective framing, decontextualized clips, and narrative manipulation designed to fracture alliances, provoke internal distrust, and weaken the legitimacy of resistance groups. It also includes calls for

actions; airstrikes, doxxing, assassination, and calling to incite religious or ethnic hostility. Another salient tactic involves the portrayal of opposition figures as sexual predators or generally immoral people, weaponizing gender-based narratives to undermine the credibility of their targets. On the other hand, it consists of clear fabrications, tenuous links between unconnected events, and completely manufactured imagery or quotes created to confuse audiences, distort timelines, or build alternative realities. Put together, these patterns suggest a deliberate and systematic effort on the part of propagandists to undermine confidence, instill fear, and manipulate public opinion using both subtle distortion of narratives and overtly falsified materials.

YEARLY ANALYSIS

> "These channels frequently publish detailed personal information of ordinary social media users who comment on posts by independent news outlets ...

The Red Flag closely monitors the propaganda channels associated with the State Administration Council (SAC), examining the nature of their content and their intended targets. It regularly publishes monitoring and investigative reports to inform the public and key stakeholders. Based on this year's findings, three main patterns of propaganda disseminated through SAC-related social media channels can be identified: (1) criminalising political opposition groups, including Ethnic Resistance Organisations (EROs), People's Defence Forces (PDFs), and the National Unity Government (NUG), in order to justify atrocities; (2) persuading the public — particularly SAC supporters — of the regime's legitimacy; and (3) promoting fear among the population through doxxing to deter opposition to the junta.

These channels consistently target EROs and PDFs by portraying their activities as criminal, whether related to armed resistance against the junta or non-combat functions such as fundraising and community engagement. The content varies depending on the group's activities, the context of the areas under their control, and broader conflict dynamics. For example, propaganda targeting the Kachin Independence Army (KIA) in Kachin State focuses on the extraction and alleged misuse of rare earth resources, while content targeting the Karen National Union (KNU) in Karen State emphasises alleged involvement in online scam operations. In contrast, racial hatred remains the primary narrative used against the Arakan Army (AA) in Rakhine State. Across the country, PDF groups are frequently accused by these channels of committing violence against civilians, including women and children.

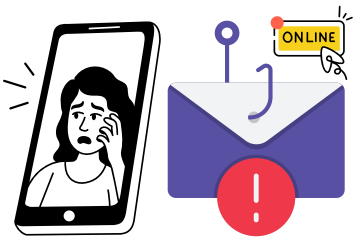
In 2025, a substantial number of soldiers surrendered during combat to EROs and PDFs. However, SAC-affiliated propaganda channels denied these reports and portrayed them as fabricated, instead claiming that only resistance fighters from PDFs and EROs had surrendered. Although many netizens are sceptical of the content disseminated by these channels and may not be easily deceived, the propaganda nonetheless appears to reach its intended audience. Defectors from the military report that soldiers and their family members consume news from these channels, either voluntarily or under coercion. Through this process, the military seeks to reinforce its legitimacy and moral support among its followers.

The most severe and persistent tactic employed by SAC-associated propaganda channels since the coup is doxxing, which aims to instil fear among the population and demonstrate the regime's power. These channels frequently publish detailed personal information of ordinary social media users who comment on posts by independent news outlets criticising the military junta or sharing information about revolutionary activities. They then call on security forces to arrest the individuals whose information has been exposed, often leading to arbitrary arrests by the police. As a result, citizens have become increasingly cautious about expressing their opinions in public, both online and offline, leading to widespread self-censorship on social media.

EMERGING NARRATIVES AND TYPES OF PROPAGANDA

During the year 2025, The Red Flag observed an increase in emerging narratives and types that were designed to bypass the traditional fact-checking process. These include:

Online Scam:



Among the various narratives employed by SAC-affiliated propaganda channels to undermine resistance groups, particular attention should be paid to content related to KK Park, a notoriously known online scam centre near the Thailand–Myanmar border. Since early 2025, military-associated propaganda channels have consistently accused the Karen National Union (KNU), the Myanmar National Democratic Alliance Army (MNDAA), and the National Unity Government (NUG) of involvement in this illicit activity.

In response to pressure from China, the military launched raids on the scam centre in October, demolishing infrastructure and arresting approximately 350 individuals. During and after these operations, the military reinforced the narrative promoted by its propaganda channels by continuing to blame the KNU for involvement in the scam operations, despite its long-standing inaction and the widespread scepticism surrounding these claims. This episode illustrates the close alignment between narratives disseminated through online propaganda channels and official statements issued by the military, highlighting their coordinated role in shaping public perceptions.

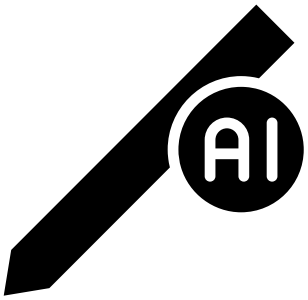
Sham Election:

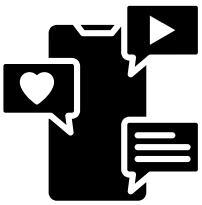
Another key propaganda message observed this year relates to the promotion of a sham election. Several founders of military-affiliated propaganda Telegram pages, including Kyaw Soe Oo, Kyaw Myo Min, and Thazin Oo, travelled to major cities and reported that these areas were fully under the regime's control. Through such reporting, these actors sought to project an image of stability and territorial dominance by the SAC.

In addition, the SAC mobilised celebrities—both those who had openly supported the regime and those who had previously opposed it but later signed pledges—to promote news related to the planned election. As a result, public opinion has become sharply divided between those who support and those who oppose the celebrities participating in the election campaign. This strategy appears to reflect the regime's intention to fragment society along multiple fault lines, thereby trapping the public in cycles of disagreement and misinformation that distract from broader opposition to the junta.

AI-generated content:

There has been a notable surge in the production and distribution of AI-generated content in propagandists' accounts across different digital platforms. Current observations indicate that the materials being circulated are increasingly clear, polished, and extended in length, often lasting several minutes. This level of sophistication suggests the growing use of paid or advanced AI models rather than basic or free versions. The consistency, coherence, and targeted nature of the content indicate the likely involvement of technical experts capable of crafting high-quality prompts to optimize AI outputs.



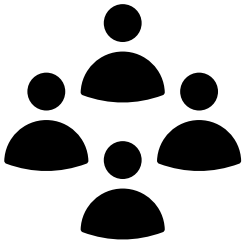


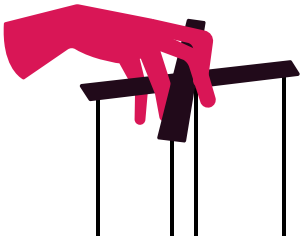
Multi-platform presence:

Instead of relying on a single platform, the bad actors actively try to establish a presence across all major platforms. They also make efforts to generate income from these platforms by expanding their reach. In many cases, they encourage audiences to follow them from one platform to another, intentionally linking their channels to maintain and grow their overall influence.

Framing as public demand:

In previous years, their persuasion strategy focused on portraying certain areas as completely free of civilians, claiming that only insurgents were present. This narrative was used to legitimize the airstrikes of SAC. However, in 2025, the messaging has shifted. They now promote a narrative that civilians themselves are requesting airstrikes, suggesting public support for bombing operations. Through this framing, they attempt to legitimize airstrikes as necessary actions to reclaim territory that has slipped from military control.





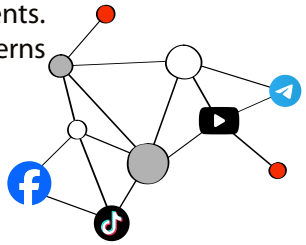
Imitation of Bad Actor Content:

The accounts appear to be ordinary; they engage in distribution patterns that closely resemble the content and behaviors of well-known bad actors. This suggests that these accounts may either be extensions of the bad actors themselves or operated by the same groups. It indicates an intentional effort to adopt alternative identities and disseminate mis/disinformation through seemingly ordinary channels.

■ ■ ■

PLATFORM ANALYSIS

The Red Flag conducted a platform-based analysis to examine the mechanisms and dynamics through which misinformation is spreading across different digital environments. This assessment identifies the unique tactics, content formats, and dissemination patterns associated with each platform.



Facebook

Facebook remained one of the most influential digital platforms in Myanmar, despite continued access restrictions imposed by the SAC that require users to rely on VPNs. For domestic users in Myanmar, Facebook remains the primary space for information, communication, and community engagement, thus a major source of misinformation. Unverified posts would spread like wildfire on the platform during times of conflict and natural disasters. The Red Flag records a significant increase in new Facebook pages, named with local or regional names as if they were community-driven, but which actually demonstrate linguistic patterns and narratives closely aligned with pro-military propaganda channels on Telegram. Content from both platforms, Telegram and Facebook, was often screenshot and amplified via organized cross-platform sharing. Comment sections also revealed signs of inauthentic activity, such as several accounts posting identical or almost identical comments to manipulate public perception. On the other hand, scammer pages have become more sophisticated: impersonation of revolutionary groups to rip off people's trust, running donation fraud, and setting up fake personal accounts in fake business or money-exchange identities. Several of these were taken down through the Meta Trusted Partner Channel by The Red Flag. More interestingly, individuals believed to be affiliated with the military and its allies began to rebuild their presence on the Facebook platform. The Red Flag has identified a verified account marked with a blue badge that seemed linked to an Ministry of Information leadership figure. The said account with a blue mark has been spreading misleading content and propaganda. If a page or profile has a blue verification mark, people tend to trust it. But since today, blue marked badges can be bought, so it does not represent any credibility feature; it's just commercial. This creates an opportunity for actors that want to spread propaganda, misinformation, or disinformation. They can buy the blue badge to look legitimate and earn public trust. Overall, these are indicative of a deepening organized effort to revive pro-military influence on Facebook and strategically shape public opinion online in Myanmar.

Telegram

Bad actors heavily shifted their operations to Telegram after Facebook became inaccessible without a VPN, and the platform took down many propagandist pages and accounts. The propagandists on Telegram adopt multiple tactics: creating as normal civilian Facebook accounts after the original ones were banned, often openly stating in Telegram that they will change the names later to avoid detection and to maintain influence. Telegram channels have also been used as hubs for organized doxxing, threats related to airstrikes, assassination, coercive messages on military conscription, and other tactics aimed at silencing critics and instilling fear. Importantly, those actors circulate those incidents of arrest or airstrikes against previously doxxed people on Telegram to increase fear and show their effectiveness in order to pressure others into silence. Simultaneously, mobilization of followers to mass-report unwanted Facebook accounts, including those of defectors and activists, sometimes framed with misleading content. Throughout this year, bad actors have also supported the SAC's agenda by disseminating AI-generated short videos on Telegram. All in all, Telegram has developed into the main place where pro-junta and opportunistic actors spread religious, ethnic, interest-based, and violence-driven divisive propaganda

Cont'd

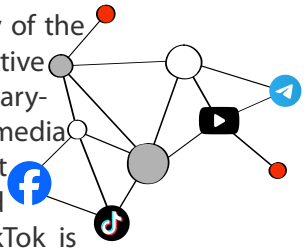
PLATFORM ANALYSIS

and coordinate cross-platform manipulation and intimidation, taking advantage of anonymity and low regulation of the platform.

Youtube

On YouTube, a considerable number of very active bad actors can be noted, taking up the role of news broadcasters, using news-discourse narration, professional templates, and live reporting formats. These methods have intentionally been used with the objective of creating a perception of credibility among followers and distributing a massive amount of deceptive and dangerous information. Instead of engaging in responsible journalism, these actors perpetuate fake news, unsubstantiated claims, conflict-linked rumors, and videos with remixed contexts. Their messages include calls to action, which may be coercion-oriented or provocative, resulting in fear and polarization, hostility, and aggressive behavior among their targets. They also make it very easy to quickly go viral on a platform such as YouTube, where they can profit off of their content and spread problematic messages effectively, especially to people unaware of this information being presented in a misleading way. Importantly, these malicious actors will oftentimes include a variety of different kinds of problematic content in a single transmission, including misleading information, false information, and dangerous stories.

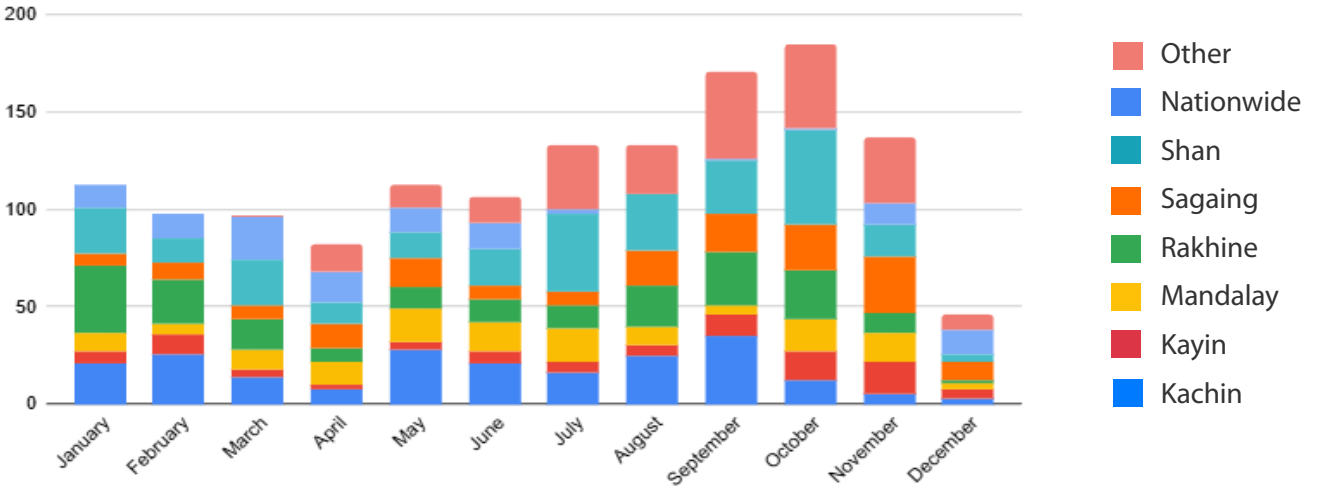
TikTok



Based on observations, many of the key actor groups are also active on TikTok. These include military-linked lobby networks, media impersonators, ultranationalist actors, and military-controlled state media. In this way, TikTok is simply another space where these actors operate and compete for influence, as they do elsewhere. In fact, such actors do not restrict themselves to video formats in terms of content dissemination. The static image-based slideshow format is also widely used to enable them to circulate the narratives with lower data consumption, wider audiences more efficiently, and potential avoidance from certain platform moderation mechanisms. There are also indications that the lobby networks have encouraged greater use of TikTok, recognizing its growing reach and influence. The trend needs close attention in light of TikTok's growing role in shaping public opinion. Besides that TikTok is increasingly a site of political campaigning and election-related mobilization, which further underlines the platform's importance as an influence operation tool.

■ ■ ■

2025 EVENT TIMELINE



The graph illustrates, based on monitoring observations by The Red Flag, that misinformation and disinformation are disseminated in direct response to the armed conflict, natural disaster, and opposition group activities. This section highlights the major incidents that took place on a monthly basis and associated with online content.

Cont'd

2025 EVENT **TIMELINE**

January

- Rakhine State, escalation of ethnic hate speech
- Return of military-linked bad actors on Facebook
- Conflicting information on MNDAA (Kokant Army) and Lashio
- Conscription Law – Arrests and propaganda

February

- Rising tensions among resistance groups
- Disinformation around USAID funding suspension
- Disinformation on online scam gangs and Myanmar migrant in Thailand deportations

March

- Earthquake-related disinformation
- Overseas trips of Military leaders and election timeline narratives
- Targeted disinformation against the NLD

April

- Earthquake-related disinformation and blame-shifting
- Ethnic hate speech targeting Rakhine communities
- Disinformation on MNDAA (Kokant Army) and Lashio
- Targeted arrests, deportations, and closure of ACC Center in Thailand

May

- Ow Htain Twin School attack (Depayin) – information suppression
- Cover-Up narratives on shot downed Military Helicopters
- Disinformation following Spy allegations in MDY-PDF
- A controversial incident occurs - tamu incident involving Indian Security Forces
- Divisions among pro-military propaganda channels
- Propaganda signals during Min Aung Hlaing Russia trip

Cont'd

2025 EVENT TIMELINE

June

- Exploitation of Daw Aung San Suu Kyi's Birthday
- Increased use of AI-Generated content
- Criminalization narratives against Resistance Forces
- Peace Forum amid ongoing Military operations
- Arrests of pro-Military lobbyists - Internal power struggles

July

- Aftermath of military retaking Naung Cho and Moebya
- Surrender and defection Narratives
- Propaganda around election and National Defense and Security Council timeline
- Continued criminalization of resistance Forces
- Conflicting narratives on Kyauk Kyi Village incident (Bago Region)

August

- Gotehtake bridge damage – Heritage and ethnic incitement narratives
- Labeling of KNU as a terrorist group and Military escalation
- False claims of Military control in Karenni and Demoso
- Expansion of AI-generated video propaganda
- Framed support narratives from Sagaing - Supportive of the military-planned election
- Linkages to centralized propaganda coordination

September

- First arrest under the Election Protection Law
- Dissolution of political parties and electoral engineering
- Military re-entry into previously Resistance-Controlled Areas
- Incitement to religious and ethnic conflict

October

- Bon To Village, Chaung-U Airstrike – Information Suppression
- Retaking of TNLA-Controlled Towns
- Publicizing the actions, KK Park show arrests and framed criminalization of KNUAdvancement and spread of AI-Generated propaganda
- Election propaganda, selective protection, and arrests
- Promotion of a Facebook replacement App - We Day Social Commerce App

November

- AI-generated and scam-related disinformation
- Campaigns against ethnic organizations
- False narratives about online scam operations
- Portraying PDFs and resistance groups as criminals
- Election-related disinformation and propaganda
- International and migration-related disinformation
- Incitement to violence and hate speech

December

- Attacks on civilians and medical facilities (Bombing of Mrauk U Hospital)
- Targeting CDMs and health workers
- Targeting Journalists and international actors
- Diplomatic and international misinformation
- Election related disinformation
- Fabricated narrative about Silent Campaign (Mandalay)
- Intimidation and incitement (Silent Campaign related)

LESSON LEARNED

Rapid Fact Checking

Over the years, TRF monitoring teams, together with fact-checking initiatives such as Real or Not and the Myanmar Fact-Checking Network (local media platforms), have produced a wide range of debunking outputs, including case studies, investigative reports, and quarterly analytical reports. Despite these efforts, significant gaps remain, particularly in real-time responses to emerging harmful trends, the development of early warning mechanisms, and the prevention of atrocities against civilians. While TRF has recognized the value of high-momentum debunking through MFCN and Real or Not, civilian protection networks—such as strike committees, youth and women's organizations, and humanitarian actors—remain insufficiently engaged and require greater investment in preventive approaches, including prebunking messages and coordinated public campaigns.

Emergency newsroom and situational newsroom

Based on experiences responding to earthquakes and the spread of misinformation, disinformation, and community-level rumors, emergency coordination mechanisms have proven highly effective in enabling rapid responses to urgent situations and in supporting affected populations during crises. These mechanisms are not only vital for natural disasters but are also critically important during political events that disrupt the information ecosystem, where timely and coordinated responses are urgently needed.

Platform Accountability

Social media platforms play a critical role in moderating content and preventing coordinated disinformation campaigns. In recent years, content moderation has become increasingly complex due to diverse language use, evolving coded expressions, the involvement of multiple actors, and cross-platform coordination. At the same time, tensions persist between protecting freedom of expression and addressing hate speech or content produced by perpetrators of human rights violations. These contradictions highlight the need for stronger accountability mechanisms for platforms. One major challenge remains the absence of inclusive and shared strategies for engaging social media companies with clear policy and content moderation recommendations.

Media Literacy

After many years of engagement in media and information literacy (MIL), Myanmar's information ecosystem has become increasingly weaponized through the systematic production and framing of misinformation and disinformation. MIL has largely been delivered as a standardized subject to communities, and TRF has implemented a significant number of basic, training-of-trainers (ToT), and advanced ToT programs for education service providers, youth and women's groups, and broader community members.

However, the need for MIL has become more urgent in the current context, marked by the rapid expansion of artificial intelligence, the rise of online scamming, the widespread circulation of misinformation and disinformation across social media platforms, and the persistence of community-level rumors. Moving forward, more advanced MIL approaches should be mainstreamed across multiple thematic sectors, including health, education, natural resource governance, political economy, well-being, gender, and community organizing.

■ ■ ■

RECOMMENDATIONS

To effectively counter mis/disinformation, we recommend the following actions:

- **Strengthen Fact-Checking Initiatives:**

  Invest in and support independent fact-checking organizations globally.

- **Enhance Platform Transparency:**

  Encourage social media companies to be more transparent about their content moderation policies and algorithmic amplification.

- **Support Independent Journalism:**

  Ensure the financial viability and editorial independence of high-quality journalistic outlets.

- **Audience centered news production:**

  Research public news consumption patterns and tailor news formats accordingly to improve accessibility and impact for news presentation.

- **Promote Media Literacy:**

  Implement educational programs to equip individuals with critical thinking skills for evaluating online information.

- **Foster Cross-Sector Collaboration:**

  Facilitate partnerships between governments, tech companies, civil society organizations, and academic institutions to share insights and best practices.

- **Adopt a dual strategy against misinformation**

  Ensure prebunking and debunking are implemented concurrently to proactive prevent misinformation.

■ ■ ■

SIGNALS, NARRATIVES, AND FUTURE RISKS: **MAPPING MYANMAR'S INFORMATION ECOSYSTEM IN** 2025

Thank you to all the stakeholders for their contribution at

https://theredflagmedia.com