NEXUS OF MANIPULATION

Anatomy of Influence Operations in the Philippines

USAID
FROM THE AMERICAN PEOPLE

Internews

Nexus of Manipulation: Anatomy of Influence Operations in the Philippines

Executive Summary

Influence operations (IOs), conducted by both domestic and foreign actors, have increasingly threatened information ecosystems. In recent years, research and investigations have documented how IOs seek to manipulate public opinion, disrupt democratic processes, and advance specific geopolitical or ideological agendas. Focusing on key incidents and collaborative efforts, this playbook examines the nature and impact of IOs, and explores tools and responses to protect the media and information environment in the Philippines.

In September 2020, Facebook dismantled fake accounts from the Philippines and China that supported then-President Rodrigo Duterte and his daughter while promoting Beijing's interests in the South China Sea. In January 2022, Twitter (now X) suspended hundreds of accounts promoting presidential candidate Ferdinand "Bongbong" Marcos Jr. for violating spam and manipulation policies. By mid-May of that year, Meta had removed 15,000 accounts for inauthentic behavior. Pro-Marcos accounts coordinated hashtags and manipulated public perception during the election season.

These operations show the sophisticated strategies used to capture public attention and manipulate opinions through seemingly organic, locally produced content. They also underscore that IOs in the Philippines do more than spread false information. They use hyper-partisan narratives to capture attention, mobilize audiences, and shape political discourse, including influencing elections. The divisive information they promote undermines trust, heightens polarization, and disrupts and weakens democratic processes in the Philippines.

In response to the threat from disinformation campaigns and IOs, including foreign information manipulation and interference (FIMI), the Initiative for Media Freedom (IMF) established a network of Philippine and global civil society and media organizations in mid-2023 to identify, analyze, and investigate IOs in the Philippines. IMF is a five-year program implemented by Internews and funded by the United States Agency for International Development (USAID). Its objectives include supporting an environment for a free press, enhancing the capacity of institutions to counter disinformation, and supporting media self-regulation. Under the IMF activity called PH-PROTECT, this collaboration has facilitated rapid information-sharing, comprehensive investigations, and public access to findings. It has enhanced the verification and digital investigation skills of local newsrooms, which are crucial in promoting information integrity and fostering societal trust and resilience.

The network has developed a broad framework for detecting IOs, which integrates guiding principles and existing literature from Meta, the European Union's European External Action Service (EEAS), and counter-IO experts like the DISARM Foundation, among others. This framework defines influence operations as coordinated efforts by state, nonstate, and proxy actors to manipulate information in pursuit of financial, geopolitical, cultural, ideological, or policy goals. IOs use disinformation, propaganda, and harmful content spread through deceptive and inauthentic methods in various media to disrupt democratic values, sociopolitical stability, and public safety. Techniques such as distributed denial of service (DDoS) attacks and hacking may be used to undermine reliable information.

The network's approach is grounded in a "learning by doing" methodology. This year-long partnership has collected various cases of domestic and foreign IOs, which have helped build understanding of these issues. These cases have served as a launchpad for a more detailed review of incidents affecting the Philippine information ecosystem.

The Philippines has a remarkable diversity of IO actors employing specific behaviors, content strategies, and varying degrees of reach to achieve their objectives. IO actors often use multiple platforms such as YouTube channels, Facebook pages, hyper-partisan content creators, and vloggers. They repurpose content from other malign actors, leveraging entertainment to forge links with political figures.

These operations use a wide range of tactics, including cross-platform coordinated inauthentic behavior (CIB), creation of dubious sites and accounts, impersonation of legitimate entities, and cyberattacks. Domestic IOs often follow a cascading pattern: hyper-partisan vloggers post content on YouTube, which is then embedded on dubious websites and amplified by Facebook accounts. Foreign IOs typically start with state media narratives echoed by experts, leading to a flood of content across platforms.

The IMF partners have observed a growing trend of using lesser-known websites and social media to disseminate false claims and propaganda. Malign actors mirror content on platforms like Bilibili and ViralPitch to maximize monetization and broaden their reach, increasingly using TikTok/Douyin, WeChat, Weibo, Baijahao, NetEase, and Guancha.

The network has tracked several prominent narratives in the Philippine information ecosystem. These include efforts to support or discredit the Marcos and Duterte families, undermine ties between the Philippines and its allies, challenge the 2016 Hague ruling on maritime rights favoring the Philippines, and defend China's aggression in the West Philippine Sea. Chinese state media have also attacked the IMF, its donor, Internews, and partners.

Given the complex nature of IOs in the Philippines, effective countermeasures require a well-defined plan and a whole-of-society approach. This involves investing in social media monitoring tools, fact-checking platforms, open-source intelligence (OSINT), and investigative journalism to monitor and detect these operations. Developing defensive communication strategies is essential for disseminating accurate information and preempting IOs. Public awareness and media literacy programs are crucial for equipping citizens with the critical thinking skills needed to identify and resist IO narratives.

Utilizing technology, including high-quality translation services, gamification, and centralized repositories for tracking IO actors, can enhance efforts to counter IOs. Collaboration and information-sharing among public and private stakeholders are vital for addressing emerging narratives and tactics. Regulations targeted at malign IOs should be balanced to protect free expression.

As IOs continue to evolve, it is essential to continually adapt and refine countermeasures so the Philippines can robustly safeguard the integrity of its media and information landscape and its democratic values.

This playbook is made possible by the support of the American People through the United States Agency for International Development (USAID). The content of this playbook is the sole responsibility of Internews under the Initiative for Media Freedom (IMF) project. It does not necessarily reflect the views of USAID or the United States Government.

Table of Contents

Introduction

In September 2020, Facebook dismantled two clusters of fake accounts originating from the Philippines and China.[1] These accounts collaborated to support then-President Rodrigo Duterte and his daughter Sara while vilifying critics of his government. The network of Chinese accounts, masquerading as locals, defended Beijing's interests in the region, particularly in the South China Sea, as part of what network analysis firm Graphika dubbed "Operation Naval Gazing."[2]

In January 2022, just two weeks into the Philippines' general election period, X (then known as Twitter) suspended hundreds of accounts that were promoting the leading presidential candidate, Ferdinand "Bongbong" Marcos Jr., on the grounds that these accounts had violated Twitter's policies on spam and manipulation.[3] The pro-Marcos accounts frequently threw "Twitter parties" to cause various hashtags to trend. By mid-May, a week after the election, Meta had removed 15,000 accounts for inauthentic behavior during the election period.[4]

This proliferation of coordinated malign accounts underscores the vulnerability of the Philippine information ecosystem to both domestic and foreign influence operations (IOs). For years, efforts to expose and counter IOs targeting the Philippines and its citizens have been primarily driven by technology platforms, while various sectors of Philippine society have focused predominantly on combating disinformation through fact-checking.

Analyzing these evolving threats, scholars led by Jonathan Corpus Ong in a study for Internews Philippines observed that tactics used in the 2022 Philippine election went beyond merely producing and disseminating disinformation (deliberately false or misleading information).[5] They also encompassed IOs characterized by hyper-partisan narratives. These IOs, which craft narratives to capture public attention, mobilize audiences, and sway electoral outcomes, are not necessarily false or misleading. The strategies for their dissemination are as critical as the content itself.

Equally concerning, the expansion of the Philippines' security ties with the United States (US) and other allies, alongside escalating tensions with China over disputed islands in the West Philippine Sea, has not only led to relentless attacks on Philippine vessels on the open sea but also an unusual surge in pro-China trolls, propagandists, and IOs.[6]

IOs pose significant threats to democracy. It is well established that spreading divisive and often false information both domestically and internationally erodes trust, heightens polarization, disrupts deliberative discourse, and ultimately undermines democratic processes. Operations orchestrated by foreign entities also pose a significant national security threat. In February 2024, the governments of the US, the United Kingdom, and Canada urged countries to identify and combat foreign information manipulation in a joint statement:

> Foreign information manipulation is a national security threat that undermines democratic values, human rights, governmental processes, and political stability…Securing the integrity of the global information ecosystem is central to popular confidence in governance institutions and processes, trust in elected leaders, and the preservation of democracy.[7]

Recognizing IOs as a significant threat to the integrity of information ecosystems and the institutions supporting democratic values, sociopolitical well-being, safety, and peace, in mid-2023 the Initiative for Media Freedom (IMF) launched a network of civil society and media organizations dedicated to identifying, analyzing, and investigating IOs in the Philippines. IMF is a five-year program implemented by Internews and funded by the United States Agency for International Development (USAID) with the support of the American people. Its objectives include supporting an environment for a free press, enhancing the capacity of institutions to counter disinformation, and support media self-regulation. Under the IMF activity called PH-PROTECT, this collaboration between Philippine and global organizations has ensured rapid information-sharing about IOs, multipronged investigations, and public access to key findings. This rapid response network has also facilitated skill development for Philippine media partners, offering hands-on verification and digital investigation training provided by global experts.

The insights gained from this year-long pioneering project are distilled in this playbook.

Defining Influence Operations

Influence operations (IOs) are defined in various ways across different organizations. Meta, which regularly publishes threat reports involving IOs, defines these operations as "coordinated efforts to manipulate or corrupt public debate for a strategic goal."[8]

The European Union has introduced the term "Foreign Information Manipulation and Interference (FIMI)" to address the increasing political and security challenge posed by foreign IOs to EU member states. The European External Action Service (EEAS), which leads efforts to counter the issue, defines FIMI as follows:

> FIMI is a mostly non-illegal pattern of behavior that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or nonstate actors, including their proxies inside and outside of their own territory.[9]

As noted in the introduction, disinformation (the deliberate distribution of false or misleading information) alone does not capture the full scope of IOs, which can also involve malinformation, the strategic use of harmful but factual information.

The network has adopted a broader framework to understand, investigate, and mitigate IOs. Its expanded concept includes not only traditional IO tactics but also cyberattacks and organized attempts to compromise or exploit data and system security. The network defines IOs in this manner:

> Influence operations involve information cascades originating from state, nonstate, and proxy (entities covertly working for others) actors, whether foreign or domestic. These operations are motivated by either financial, geopolitical, cultural, ideological, institutional, or policy interests. They use narratives that disrupt the health of information ecosystems and institutions vital to democratic values, sociopolitical welfare, safety, and peace.
>
> These operations employ disinformation, propaganda, and other harmful content (such as harassment and attacks) in various formats to coerce or manipulate behavior and polarize society.
>
> Influence operations often use inauthentic, deceptive, or concealed procedures. They are executed in a coordinated manner through traditional media, social media, and other digital mechanisms such as messaging applications and over-the-top (OTT) media services, whether privately or publicly distributed.

> They also include techniques that disrupt the distribution of and undermine reliable information such as distributed denial of service (DDoS) attacks, hacking, and other forms of technical interference.

This definition can be unpacked using the “5Ws, 1H” framework (Who, What, Where, When, Why, and How) that journalists use when gathering comprehensive information.

Who	Foreign or domestic state, nonstate, and/or proxy actors
What	Cascades of information or narratives
Where	Traditional media, social media, and other digital mechanisms such as messaging applications and over-the-top media services, privately or publicly distributed
When	As the occasion warrants
How	Inauthentic, deceptive, or concealed procedures executed in a coordinated manner; technical interference that disrupts the flow of reliable information such as distributed denial of service (DDos) attacks and hacking
Why	Financial, geopolitical, cultural, ideological, institutional, or policy interests

IOs are considered malign when their origins are obscured; the information they spread is false, misleading, irrelevant, unsolicited, redundant, or low-quality; and/or their calls to action violate human rights, such as inciting violence or hatred, according to a report published by the Carnegie Endowment for International Peace.[10]

To distinguish foreign IOs from domestic ones, strategic communication experts Hedvig Ördén and James Pamment have highlighted the importance of assessing their connections to foreign states, citizens, and interests.[11]

Evaluating the involvement of foreign states requires examining state sponsorship, alignment with geopolitical objectives, and the use of sophisticated tactics characteristic of state actors. Indicators include the deployment of state-run media, government-backed agencies, or coordinated disinformation campaigns aimed at destabilizing other nations’ political or social systems. Activities often parallel acts of war and may involve violations of sovereignty or international laws.

IO actors are citizens or residents of another country who engage in activities that influence the political or social discourse of a targeted state. Key factors include their citizenship and residency, exclusion from domestic rights such as voting, and the legal context of their participation in domestic affairs. Common examples are foreign nationals orchestrating social media campaigns or funding political advertisements to sway domestic opinions and actions in the targeted state.

IOs are driven by foreign interests and motivated by the strategic, economic, or political goals of foreign entities, which can include states, organizations, or individuals. These operations often use proxies or third parties to mask direct involvement and may employ soft power tactics such as cultural diplomacy, economic influence, and/or strategic communication.

The ABCDE of Influence Operations

The ABCDE Framework developed by Pamment breaks down the issue of IOs, specifically foreign interference, into five smaller operative factors to help devise countermeasures.[12] This playbook uses the ABCDE Framework as its guiding structure for presenting the network's key findings. It provides various examples to demonstrate each factor, capped by a case study that shows all five factors in action.

Factor	Question	Indicator
Actors	What kinds of actors are involved?	Individuals, nonstate actors, media platforms, political actors, foreign states
Behaviors	What activities are exhibited?	Transparency, dependency, authenticity, infrastructure, intent
Content	What kinds of content are being created and distributed?	Truthfulness, narrative, language, organic/synthetic, expression, harm
Degree	How is the content distributed? Which audiences are targeted and reached?	Audience, platform, virality, targeting, scale
Effect	What is the overall impact of the case and whom does it affect?	Climate of debate, trust/reputation, fundamental freedoms, public health, public safety, election integrity, national security

Actors

Under IMF, "malign actors," also known as threat actors, are defined as individuals or groups that maliciously spread false or manipulated information to distort public discourse as part of an IO. They include both the instigators or sources of IO narratives and the amplifier accounts that cascade the information across various social media platforms.

IO actors tracked by the network frequently draw from typical sources of disinformation, including YouTube channels and Facebook pages that self-identify as media or news outlets, as well as hyper-partisan content creators or vloggers. On Facebook and X (formerly Twitter), fan pages of political figures often amplify video content from YouTube.

Both foreign and domestic actors use similar methods, echoing certain sources and disseminating information across various platforms. Many of these actors repurpose content from other malign actors and use entertainment to forge links with political figures.

Certain organizations are vocal about geopolitical tensions in the West Philippine Sea, mirroring a pro-China stance and using experts and think tanks to project credibility. These local actors are often featured in China-controlled media such as the China Global Television Network (CGTN) and the Global Times in addition to their domestic platforms.

Category	Description
Individual(s)	Hyper-partisan influencers/content creators/“experts,” inauthentic profiles
Nonstate actor(s)	Pseudo-academic organizations/think tanks, defense/military analysts, network affiliates on crypto-scams, fan accounts and pages
Media platform(s)	Far-right media, media-styled social media pages and websites, dubious websites
Political actor(s)	State-media, government agencies/officials

Malign actors pursue various objectives encapsulated in the 5D model, an extension of Ben Nimmo’s 4D model[13] [14]. The five D’s are as follows:

- Dismiss allegations and denigrate the source
- Distort the narrative and twist the framing
- Distract to shift attention and blame to a different actor or narrative
- Dismay to threaten and frighten opponents
- Divide to generate conflict and broaden divisions within or between communities and groups.

The network has identified Facebook accounts engaged in coordinated inauthentic behavior (CIB), amplifying polarizing and often fabricated narratives from YouTube channels and dubious websites about the alliance between President Ferdinand Marcos Jr. and Vice President Sara Duterte, including allegations of electoral fraud and a supposed term-sharing agreement, to further **divide** Philippine society.

A Philippine Coast Guard (PCG) official has been repeatedly denigrated by those seeking to **dismiss** the Philippines' territorial claims in the West Philippine Sea. **Distorted** narratives, such as the alleged “Ukrainization” of the Philippines by the US, have been pushed to cast the latter in a negative light.

Dismaying strategies have targeted news organizations covering potential foreign IOs. Websites like Inquirer.net and MindaNews have been cloned to spread fabricated stories, potentially damaging the reputation of these news outlets. To **distract** the public from pressing concerns on sovereignty, malign actors have shifted attention onto other fabricated issues such as alleged collusion between the Central Intelligence Agency (CIA) and the PCG.

Behaviors

Foreign Information Manipulation and Interference (FIMI) focuses largely on behavior and draws extensively from the DISARM Framework developed by the DISARM Foundation.[15] This framework outlines the tactics, techniques, and procedures (TTPs) that malign or threat actors are likely to employ at various stages of an IO: planning, preparation, execution, and assessment.

> Tactics: Operational goals the actors try to achieve (See the 5D model)
> Techniques: Actions depicting how they try to accomplish the tactics
> Procedures: Specific combinations of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different actors

The EEAS has adopted the DISARM Framework (Red) to describe incident behaviors and the Structured Threat Information Expression (STIX), an open-source language and format for exchanging cyber-threat intelligence (CTI), when collecting data on FIMI incidents. In turn, the Taiwan-based Doublethink Lab, which researches malign Chinese IOs, has modeled its codebook on the EEAS approach and introduced it to the network partners to help them better identify and describe IOs, particularly attack patterns.

The network has identified multiple TTPs or attack patterns in domestic and foreign IOs. This playbook explores four patterns, including two that have specifically targeted media outlets and network partners. These patterns involve cross-platform coordinated inauthentic behavior (CIB), the creation of fake websites and news sites, and the impersonation of legitimate entities.

DISARM FRAMEWORK

PLAN

Plan Strategy

- Determine Target Audiences
- Determine Strategic Ends

Plan Objectives

- Facilitate State Propaganda
- Degrade Adversary
- Discredit Credible Sources
- 5Ds (Dismiss, Distort, Distract, Dismay, Divide)

Target Audience Analysis

- Segment Audiences
- Geographic Segmentation
- Demographic Segmentation
- Economic Segmentation
- Psychographic Segmentation
- Political Segmentation
- Map Target Audience Information Environment
- Monitor Social Media Analytics
- Evaluate Media Surveys
- Identify Trending Topics/Hashtags
- Conduct Web Traffic Analysis
- Assess Degree/Type of Media Access
- Identify Social and Technical Vulnerabilities
- Find Echo Chambers
- Identify Data Voids
- Identify Existing Prejudices
- Identify Existing Fissures
- Identify Existing Conspiracy Narratives/Suspicions
- Identify Wedge Issues
- Identify Target Audience Adversaries
- Identify Media System Vulnerabilities

Source: https://disarmframework.herokuapp.com/

PREPARE

Develop Narratives

- Leverage Existing Narratives
- Develop Competing Narratives
- Leverage Conspiracy Theory Narratives
- Amplify Existing Conspiracy Theory Narratives
- Develop Original Conspiracy Theory Narratives
- Demand Insurmountable Proof
- Respond to Breaking News Event or Active Crisis
- Develop New Narratives
- Integrate Target Audience Vulnerabilities Into Narrative

Develop Content

- Create Hashtags and Search Artifacts
- Generate Information Pollution
- Create Fake Research
- Hijack Hashtags
- Distort Facts
- Reframe Context
- Edit Open-Source Content
- Reuse Existing Content
- Use Copypasta
- Plagiarize Content
- Deceptively Labeled or Translated
- Appropriate Content
- Develop Text-based Content
- Develop AI-Generated Text
- Develop False or Altered Documents
- Develop Inauthentic News Articles
- Develop Image-based Content
- Develop Memes
- Develop AI-Generated Images (Deepfakes)
- Deceptively Edit Images (Cheap fakes)
- Aggregate Information Into Evidence Collages
- Develop Video-based Content
- Develop AI-Generated Videos (Deepfakes)
- Deceptively Edit Video (Cheap fakes)
- Develop Audio-based Content
- Develop AI-Generated Audio (Deepfakes)
- Deceptively Edit Audio (Cheap fakes)
- Obtain Private Documents
- Obtain Authentic Documents
- Create Inauthentic Documents
- Alter Authentic Documents

Establish Social Assets

- Create Inauthentic Social Media Pages
- Cultivate Ignorant Agents
- Create Inauthentic Websites
- Prepare Fundraising Campaigns
- Raise Funds from Malign Actors
- Raise Funds from Ignorant agents
- Prepare Physical Broadcast Capabilities
- Create Inauthentic Accounts
- Create Anonymous Accounts
- Create Cyborg Accounts
- Create Bot Accounts
- Create Sockpuppet Accounts
- Recruit Malign Actors
- Recruit Contractors
- Recruit Partisans
- Enlist Troll Accounts
- Build Network
- Create Organizations
- Use Follow Trains
- Create Community or Sub-group
- Acquire/Recruit Network
- Fund Proxies
- Acquire Botnets
- Infiltrate Existing Networks
- Identify Susceptible Targets in Networks
- Utilize Butterfly Attacks
- Develop Owned Media Assets
- Leverage Content Farms
- Create Content Farms
- Outsource Content Creation to External Organizations

EXECUTE

Conduct Pump Priming

- Trial Content
- Bait Legitimate Influencers
- Seed Kernel of Truth
- Seed Distortions
- Use Fake Experts
- Use Search Engine Optimization
- Employ Commercial Analytic Firms

Deliver Content

- Deliver Ads
- Social Media
- Traditional Media
- Post Content
- Share Memes
- Post Violative Content to Provoke Takedown and Backlash
- One-Way Direct Posting
- Comment or Reply on Content
- Post Inauthentic Social Media Comment
- Attract Traditional Media

Maximize Exposure

- Flooding the Information Space
- Trolls Amplify and Manipulate
- Hijack Existing Hashtag
- Bots Amplify via Automated Forwarding
- Utilize Spamoflauge
- Conduct Swarming
- Conduct Keyword Squatting
- Inauthentic Sites Amplify News and Narratives
- Amplify Existing Narrative
- Cross-Posting
- Post Across Groups
- Post Across Platform
- Post Across Disciplines
- Incentivize Sharing
- Use Affiliate Marketing Programs
- Use Contests and Prizes
- Manipulate Platform Algorithm
- Bypass Content Blocking
- Direct Users to Alternative Platforms

ASSESS

Assess Effectiveness

- Measure Performance
- People Focused
- Content Focused
- View Focused
- Measure Effectiveness
- Behavior Changes
- Content
- Awareness
- Knowledge
- Action/Attitude
- Measure Effectiveness Indicators (or KPIs)
- Message Reach
- Social Media Engagement

Tactics

Techniques

DISARM FRAMEWORK

PLAN

Plan Strategy

- Determine Target Audiences
- Determine Strategic Ends

Plan Objectives

- Facilitate State Propaganda
- Degrade Adversary
- Discredit Credible Sources
- 5Ds (Dismiss, Distort, Distract, Dismay, Divide)

Target Audience Analysis

- Segment Audiences
- Geographic Segmentation
- Demographic Segmentation
- Economic Segmentation
- Psychographic Segmentation
- Political Segmentation
- Map Target Audience Information Environment
- Monitor Social Media Analytics
- Evaluate Media Surveys
- Identify Trending Topics/Hashtags
- Conduct Web Traffic Analysis
- Assess Degree/Type of Media Access
- Identify Social and Technical Vulnerabilities
- Find Echo Chambers
- Identify Data Voids
- Identify Existing Prejudices
- Identify Existing Fissures
- Identify Existing Conspiracy Narratives/Suspicions
- Identify Wedge Issues
- Identify Target Audience Adversaries
- Identify Media System Vulnerabilities

Source: https://disarmframework.herokuapp.com/

PREPARE
(cont'd)

Establish Legitimacy

- Create Fake Experts
- Utilize Academic/Pseudoscientific Justifications
- Compromise Legitimate Accounts
- Create Personas
- Backstop Personas
- Establish Inauthentic News Sites
- Create Inauthentic News Sites
- Leverage Existing Inauthentic News Sites
- Prepare Assets Impersonating Legitimate Entities
- Astroturfing
- Spoof/Parody Account/Site
- Co-opt Trusted Sources
- Co-opt Trusted Individuals
- Co-opt Grassroots Groups
- Co-opt Influencers

Microtarget

- Create Clickbait
- Purchase Targeted Advertisements
- Create Localized Content
- Leverage Echo Chambers/Filter Bubbles
- Use Existing Echo Chambers/Filter Bubbles
- Create Echo Chambers/Filter Bubbles
- Exploit Data Voids

Select Channels and Affordances

- Online Polls
- Chat Apps
- Use Encrypted Chat Apps
- Use Unencrypted Chats Apps
- Livestream
- Video Livestream
- Audio Livestream
- Social Networks
- Mainstream Social Networks
- Dating Apps
- Private/Closed Social Networks
- Interest-Based Networks
- Use Hashtags
- Create Dedicated Hashtag
- Media Sharing Networks
- Media Sharing Networks
- Photo Sharing
- Video Sharing
- Audio sharing
- Discussion Forums
- Anonymous Message Boards
- Bookmarking and Content Curation
- Blogging and Publishing Networks
- Consumer Review Networks
- Formal Diplomatic Channels
- Traditional Media
- TV
- Newspaper
- Radio
- Email

EXECUTE
(cont'd)

Drive Online Harms

- Censor Social Media as a Political Force
- Harass
- Boycott/"Cancel" Opponents
- Harass People Based on Identities
- Threaten to Dox
- Dox
- Control Information Environment Through Offensive
- Delete Opposing Content
- Block Content
- Destroy Information Generation Capabilities
- Conduct Server Redirect
- Suppress Opposition
- Report Non-Violative Opposing Content
- Goad People Into Harmful Action
- Exploit Platform TOS/Content Moderation
- Platform Filtering

Drive Offline Activity

- Conduct Fundraising
- Conduct Crowdfunding Campaigns
- Organize Events
- Pay for Physical Action
- Conduct Symbolic Action
- Sell Merchandise
- Encourage Attendance at Events
- Call to Action to Attend
- Facilitate Logistics or Support for Attendance
- Physical Violence
- Conduct Physical Violence
- Encourage Physical Violence

Persist in the Information Environment

- Play the Long Game
- Continue to Amplify
- Conceal People
- Use Pseudonyms
- Conceal Network Identity
- Distance Reputable Individuals from Operation
- Launder Accounts
- Change Names of Accounts
- Conceal Operational Activity
- Conceal Network Identity
- Generate Content Unrelated to Narrative
- Break Association with Content
- Delete URLs
- Coordinate on Encrypted/Closed Networks
- Deny Involvement
- Delete Accounts/Account Activity
- Redirect URLs
- Remove Post Origins
- Misattribute Activity
- Conceal Infrastructure
- Conceal Sponsorship
- Utilize Bulletproof Hosting
- Use Shell Organizations
- Use Cryptocurrency
- Obfuscate Payment
- Exploit TOS/Content Moderation
- Legacy Web Content
- Post Borderline Content

ASSESS

Assess Effectiveness

- Measure Performance
- People Focused
- Content Focused
- View Focused
- Measure Effectiveness
- Behavior Changes
- Content
- Awareness
- Knowledge
- Action/Attitude
- Measure Effectiveness Indicators (or KPIs)
- Message Reach
- Social Media Engagement

Tactics

Techniques

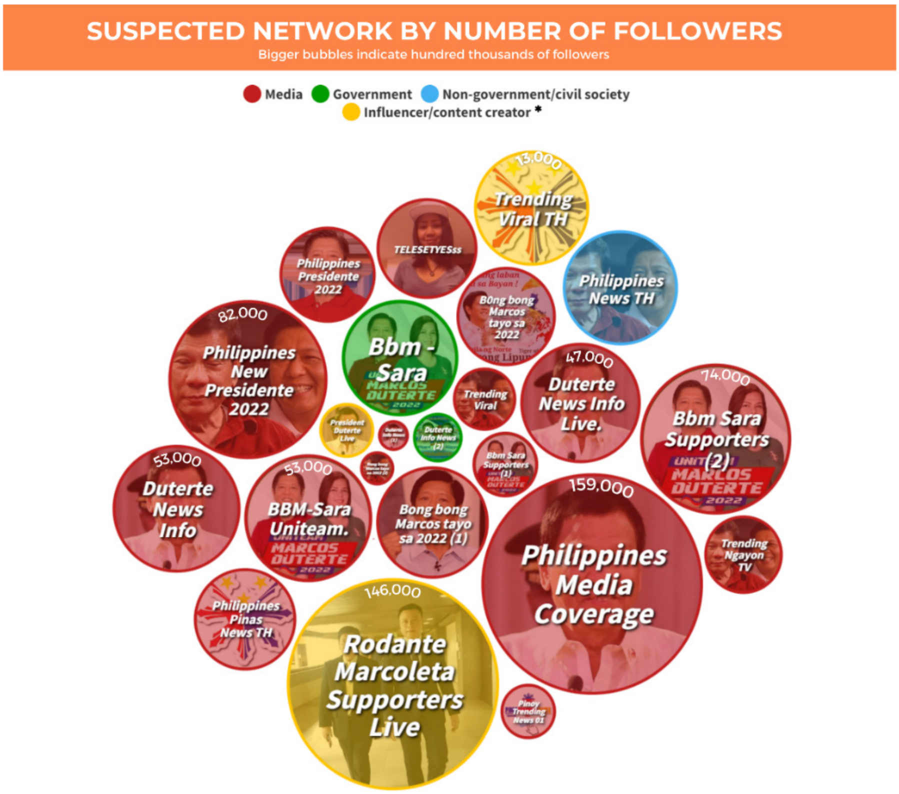
Cross-platform coordinated inauthentic behavior

Coordinated inauthentic behavior (CIB), a term coined by Facebook, refers to organized actions by a network of social media accounts and pages to artificially boost content while often falsifying their affiliations and intents.[16]

The IMF has been monitoring a suspicious network of Facebook accounts primarily located in Vietnam that disseminate and amplify content related to Philippine politics. On May 15, 2023, 33 accounts suspected to be part of this network propagated the claim that Vice President Duterte would replace President Marcos in 2025 as part of a purported "term-sharing" agreement.

Five months later, this network intensified allegations of electoral fraud against President Marcos, falsely asserting that the vote count in the 2022 election was manipulated. It also spread unverified information that Speaker Martin Romualdez, President Marcos' cousin, would run against Vice President Duterte for president in 2028 despite a lack of official announcements from either party.

The IMF traced these narratives to a verified YouTube channel, Pinoy Streamline, which seeded them through a dubious website, kankoc.info. Rather than being directly shared on Facebook, the YouTube videos were first embedded in articles on kankoc.info. The links to articles were then posted simultaneously on the same day with the exact same caption across the network of Facebook accounts and pages. The same network of accounts would use avise.info to spread content on Facebook, as observed by the IMF in July 2023.


SUSPECTED NETWORK BY NUMBER OF FOLLOWERS

Bigger bubbles indicate hundred thousands of followers

On July 28, 24 Facebook accounts self-declared as located in Vietnam shared an article with the headline "Imee is not Ferdinand Marcos Sr.'s daughter according to yellows," redirecting to a video from verified YouTube channel Pinoy Streamline.

** These categories are based on the page account's self-identification.*

At least 14 Facebook pages located in Vietnam were named after the Vice President Duterte's father, former President Rodrigo Duterte. Meanwhile, 11 pages were named after President Marcos, seven after both the president and the vice president, 50 after Sen. Raffy Tulfo, and four after SAGIP party-list representative Rodante Marcoleta.

Celebrity fan pages named after actresses Ivana Alawi and Alex Gonzaga also used kankoc.info to post entertainment content. Several pages had identical names and similar profile photos, with follower counts ranging from 2,900 to 432,000.

The IMF gathered the data based on the page account's self-identification and did not directly confirm their association with these public figures.

Philstar.com documented this pattern of content replication, amplification, and potential coordination in its report on attacks against PCG spokesperson Jay Tarriela on Facebook and X.[17] The attacks began with a verified X user accusing Tarriela of being a CIA agent. This narrative was quickly picked up by anonymous X users and Facebook bloggers.

The portrayal of Tarriela as pro-America was also echoed by columnists Penny Abad of Net25, a television network linked to Iglesia ni Cristo, and Rigoberto Tiglao of The Manila Times. Both media outlets have faced criticism in the past for spreading disinformation.

Establishing social assets through inauthentic websites

Building on the known use of suspicious websites for disinformation campaigns, the IMF's social media monitoring has identified a network of sites engaged in domestic IOs. For example, the domains kankoc.info and avise.info focus on celebrity and entertainment news, with political topics such as electoral fraud allegations absent from their homepages and search results. These websites are consistently used for CIB across platforms by seeding content from YouTube channels such as Pinoy Streamline.

Created in 2008, avise.info has had seven domain owners who registered the domain name in Ireland, Panama, California (USA), Romania, Florida (USA), and finally in Hanoi. This domain has been found to share unique identifiers such as its Google Analytics tracking ID, Facebook App ID, and IP address with kankoc.info, also known as kidstva.com.

The IMF also discovered another dubious site mirroring the website of the file-sharing application SHAREit. "wshareit.com" closely resembles SHAREit's legitimate domain name ushareit.com. The suspicious website, initially registered in Panama and years later in Denver, Colorado, was used to cascade the debunked claim that Sara Duterte had been removed as vice president by Congress, as seen in this archived post. This claim was originally posted on YouTube.

Establishing legitimacy through inauthentic news sites

Malign actors have been found to make use of a network of inauthentic or pseudo news sites that spread disinformation and propaganda worldwide. These sites may have various motives, ranging from spreading propaganda to earning click-based revenue.

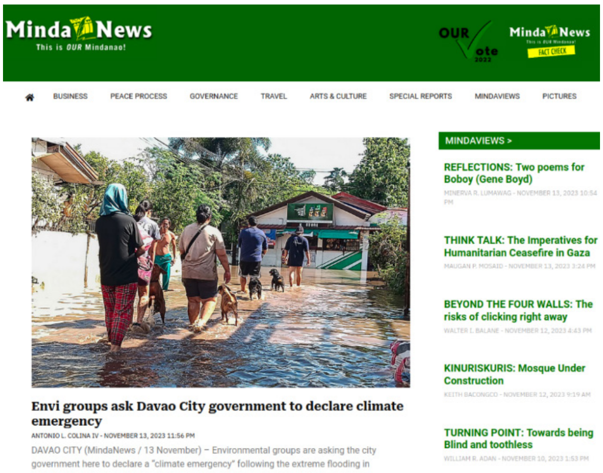
According to a report by PressOnePH, Brian Joseph Thomas Berletic, an American blogger based in Bangkok, has been writing for websites such as the New Eastern Outlook, Land Destroyer, the New Atlas, and Global Research, which the US government describes as disinformation outlets and pseudo-academic publications.[18] In a November 2023 commentary, Berletic claimed that the US was shaping the Philippines into the next Ukraine and using it as a "disposable battering ram" against China. PressOnePH found the commentary cross-posted on at least 11 websites, including the Orinoco Tribune, The Alternative World, and the Socio Economics History Blog. These websites self-identify as independent news organizations but do not disclose the identities or addresses of their editors.

Additional research by the network members revealed that Berletic's commentary was reposted 81 times on X, including by accounts based in the Philippines, and shared by a dozen Facebook groups predominantly catering to Filipinos.

Establishing legitimacy by impersonating legitimate entities

IOs sometimes impersonate legitimate entities to obscure their network identity and lend an air of credibility to their content, according to the DISARM Foundation. The foundation states that users are more inclined to believe and less likely to fact-check information from well-known sources than from unfamiliar ones. These legitimate entities could include authentic news sites, public figures, organizations, or government bodies.

In the Philippines, since 2021 a China-based network has cloned the website of MindaNews, scraping content from its opinion section and translating it into Chinese.[19] An investigation by the Swedish nonprofit Qurium Media uncovered that the network targets diverse industries and has cloned hundreds of websites, including those of universities, libraries, and businesses.[20] The cloned sites were found to contain ads for a gambling company called 188BET. The fraudulent MindaNews website (m.mart-inn.com) is registered in Hebei, China.



Envi groups ask Davao City government to declare climate emergency
ANTONIO L. COLINA IV - NOVEMBER 13, 2023 11:56 PM
DAVAO CITY (MindaNews / 13 November) – Environmental groups are asking the city government here to declare a "climate emergency" following the extreme flooding in

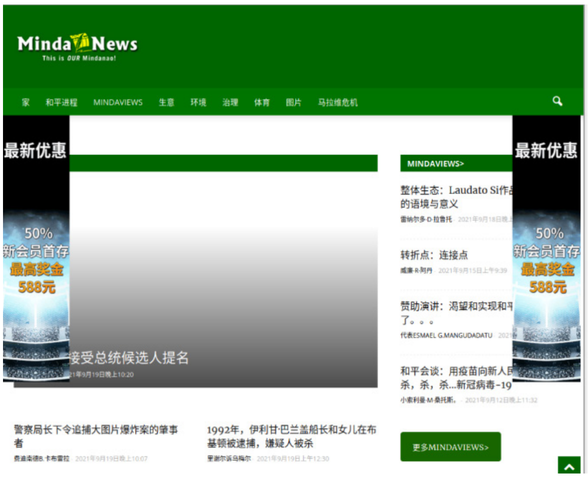
REFLECTIONS: Two poems for Boboy (Gene Boyd)
MINERVA R. LUMAWAG - NOVEMBER 13, 2023 10:54 PM

THINK TALK: The Imperatives for Humanitarian Ceasefire in Gaza
MAUGAN P. MOSAID - NOVEMBER 13, 2023 3:24 PM

BEYOND THE FOUR WALLS: The risks of clicking right away
WALTER I. BALANE - NOVEMBER 12, 2023 4:43 PM

KINURISKURIS: Mosque Under Construction
KEITH BACONGCO - NOVEMBER 12, 2023 9:19 AM

TURNING POINT: Towards being Blind and toothless
WILLIAM R. ADAN - NOVEMBER 10, 2023 1:53 PM



接受总统候选人提名
21年9月19日晚上10:20

警察局长下令追捕大图片爆炸案的肇事者
詹迪南德B.卡布雷拉 2021年9月19日晚上10:07

1992年，伊利甘·巴兰盖船长和女儿在布基顿被逮捕，嫌疑人被杀
里谢尔诉乌梅尔 2021年9月19日上午12:30

整体生态：Laudato Si作品的语境与意义
雷纳尔多·D·拉鲁托 2021年9月18日晚上

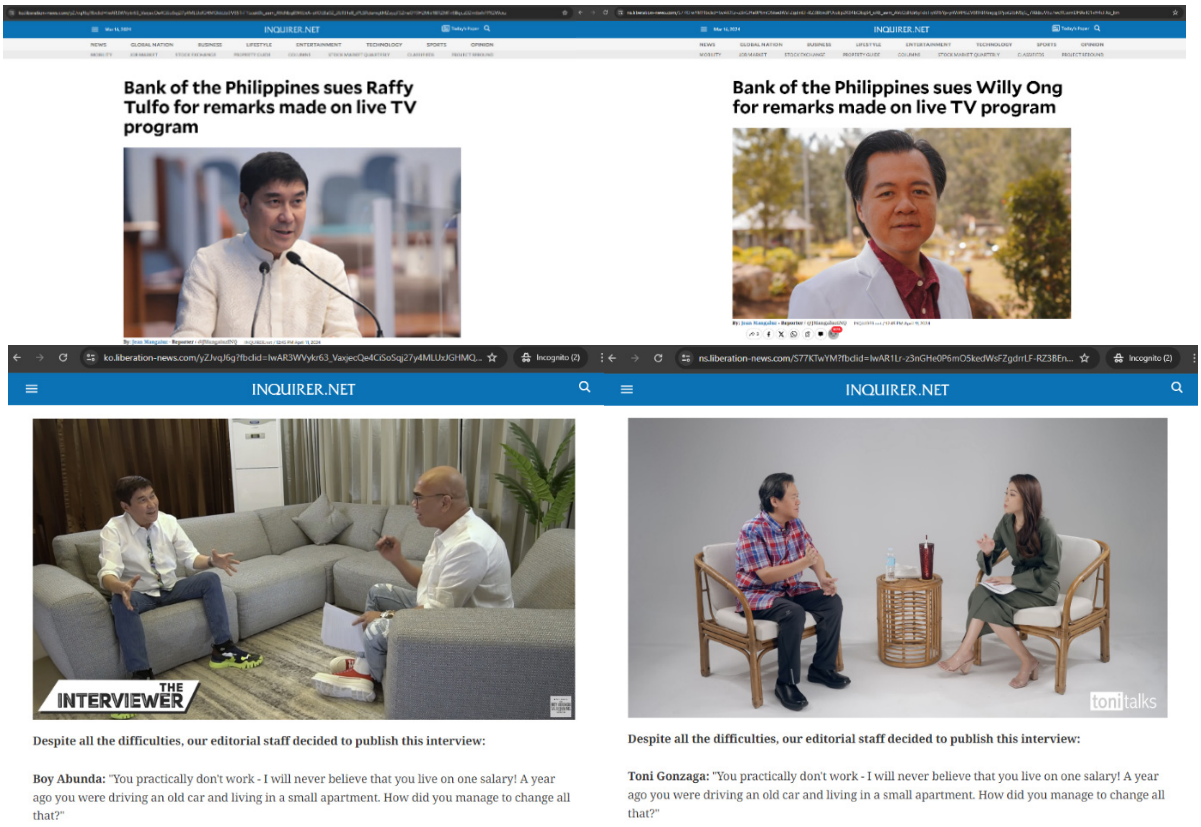
转折点：连接点
威廉·R·阿丹 2021年9月15日上午9:39

赞助演讲：渴望和实现和平了。。。
代表ESMAEL G.MANGUDADATU 2021

和平会谈：用疫苗向新人民杀，杀，杀...新冠病毒-19
小索利曼·M·桑托斯。 2021年9月12日晚上11:32

The IMF's social media monitors also found a website with the domain name liberation-news.com that has impersonated INQUIRER.net, one of the Philippines' most-respected online news outlets. On March 16, 2024, this website posted fake articles featuring Sen. Raffy Tulfo and internet influencer doctor Willie Ong with identical clickbait headlines: "Bank of the Philippines sues [Raffy Tulfo/Willie Ong] [*sic*] for remarks made on live TV program." Both articles contained fabricated interviews with television personalities Boy Abunda and Toni Gonzaga promoting the cryptocurrency platform Trade 24 Evista.

A domain age check revealed that this dupe site was only a month old at the time of its discovery. The site appeared aimed at deceiving users and stealing their sensitive data. Both the Inquirer and Tulfo have publicly denounced the site as fake and denied any involvement in the associated investment scheme. [21] [22] A Qurium investigation traced the ads on the counterfeit site to the marketing agency Supreme Media, an affiliate network based in Tel Aviv, Israel, formerly known as Media 500.[23] [24]



INQUIRER.NET

Bank of the Philippines sues Raffy Tulfo for remarks made on live TV program

Bank of the Philippines sues Willy Ong for remarks made on live TV program

ko.liberation-news.com/yZJvqJ6g?fbclid=IwAR3WVykr63_VaxjecQe4CiSoSqj27y4MLUxJGHMQ...

INQUIRER.NET

Despite all the difficulties, our editorial staff decided to publish this interview:

Boy Abunda: "You practically don't work - I will never believe that you live on one salary! A year ago you were driving an old car and living in a small apartment. How did you manage to change all that?"

ns.liberation-news.com/S77KTwYM?fbclid=IwAR1Lr-z3nGHe0P6mO5kedWsFZgdrrLF-RZ3BEn...

INQUIRER.NET

Despite all the difficulties, our editorial staff decided to publish this interview:

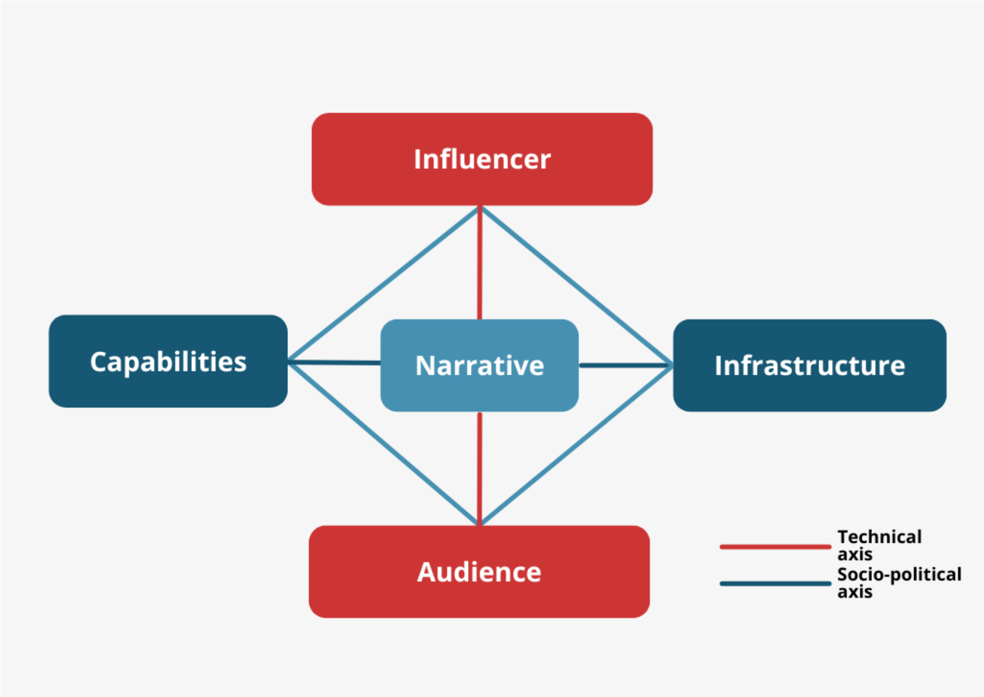
Toni Gonzaga: "You practically don't work - I will never believe that you live on one salary! A year ago you were driving an old car and living in a small apartment. How did you manage to change all that?"

Another impostor website appropriated the name and logo of the now-defunct CNN Philippines to falsely advertise a cream purported to treat bone and joint diseases. This fake site features an article that misuses the name and image of global orthopedic expert Ramon Gustilo, fabricating quotes by him to endorse the product's effectiveness.[25] The servers hosting the impostor site are involved in the registration of thousands of domains associated with fraud and phishing attacks, according to Qurium.[26]

Content

The EEAS emphasizes the need to examine a pattern of behavior when analyzing IOs. The US-based cybersecurity company Recorded Future advocates for the Diamond Model framework which places content at the core of every IO.[27] It highlights that narrative, which is overlooked in some IO frameworks, is essential for understanding the intentions and objectives of the influencer.

In the Diamond Model, narrative is positioned at the center of the diamond, intersected by two key axes. The sociopolitical axis consists of the influencer, meaning the individual or organization conducting malign influence activities, and the audience, meaning the intended target of the IO. The technical axis comprises capabilities, or the influencer's TTPs, and infrastructure, including the media used by influencers such as print media, television, and digital platforms.



Source: Recorded Future

The most prominent narratives tracked by the network include efforts to discredit the Marcos and Duterte families; support the Dutertes; challenge the 2016 ruling on maritime rights by the Permanent Court of Arbitration in The Hague; undermine ties between the Philippines, the US, and other allies; and defend China's aggression in the West Philippine Sea. The Hague ruling affirmed the Philippines' territorial claims within its exclusive economic zone in the West Philippine Sea, in opposition to China's assertions.

Campaigns against Marcos

In December 2023, the IMF detected a potential IO targeting President Marcos by sources known for disseminating inaccurate and biased information. Notably, the vlogger Maharlika (real name: Claire Eden Contreras) threatened to release a controversial video dubbed the "polvoron video," which allegedly implicates the president in drug use. Polvoron is a sweet, milky, and powdery Filipino-style shortbread. Maharlika, previously a Marcos supporter, has been cited in several fact-check reports by Philstar.com and VERA Files, and faced cyber libel charges in 2022. [28] [29] [30]

That same month, former broadcaster Jay Sonza claimed on his Facebook page that President Marcos wanted to shut down Sonshine Media Network International (SMNI) despite its support for his campaign. Sonza's post garnered over 300 shares and 4,000 reactions. SMNI, owned by Duterte ally and religious leader Apollo Quiboloy, was at the time being investigated by the House of Representatives for disinformation and "red-tagging," or labelling individuals or groups as communists or terrorists. Sonza's assertions about the supposed achievements of former President Duterte and the late dictator Ferdinand Marcos Sr. have been debunked by reputable fact-checking organizations.[31] [32]

Pro-Duterte social media accounts

In November 2023, Philstar.com noted potentially coordinated behavior among pro-Duterte social media accounts promoting survey findings that positioned the former president as the leading senatorial candidate for the 2025 elections.[33] Even before the market research firm Tangere released the results of its survey, the prominent pro-Duterte page "Krizette Laureta Chu" highlighted Duterte's popularity, claiming that people were "longing for his leadership." After the survey results were published exclusively by Manila Bulletin, where Chu is a former editor, pro-Duterte figures like Mark Anthony Lopez and Pebbles Duque, niece of Duterte's former health secretary Francisco Duque, shared the findings with their favorable commentary. Various social media pages and YouTube channels amplified the survey results, emphasizing Duterte's potential political comeback.

In December 2023, MindaNews flagged an apparently coordinated action to misleadingly promote survey results about Vice President Sara Duterte's trust rating.[34] A Publicus Asia survey showed this rating declining to 53% in December from the previous quarter's 55%. Pro-Duterte accounts omitted the drop in their posts, focusing instead on the detail that Duterte had received the highest trust rating among the country's top five officials. This angle was widely circulated across Facebook pages and accounts, accompanied by the narrative that the vice president should run for president in 2028.

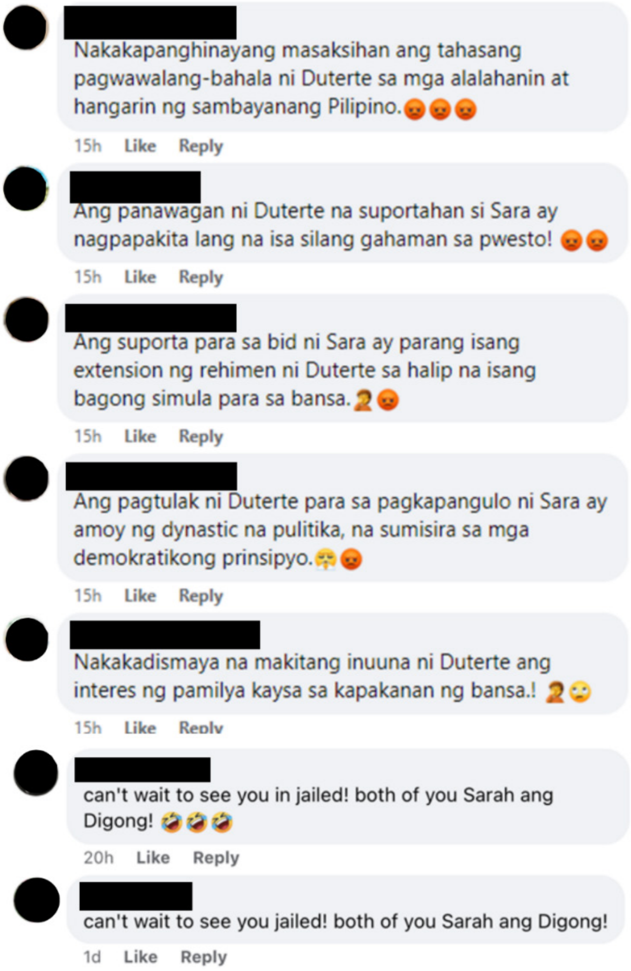
Coming to the vice president's defense, X and Facebook accounts circulated a screenshot of a tweet by political blogger Sass Sasot referring to "Oplan Destroy Inday," a purported campaign to tarnish "Inday" Sara Duterte's image. Sasot has been flagged for spreading falsehoods and her Facebook page was temporarily removed in January 2024.

Anti-Duterte narratives

Narratives against the Dutertes were also amplified through seemingly coordinated means.

In February 2024, Philstar.com found hyper-partisan vloggers across YouTube and Facebook pushing the malicious claim that Vice President Duterte had intimate relations with Philippine Basketball Association (PBA) rookie John Amores. [35] These vloggers and Facebook accounts, which appear to have acted in coordination, also said Duterte used public funds to support Amores. The involved vloggers have been known to post hyper-partisan content favorable to the Marcoses.

MindaNews' Facebook page was flooded with comments criticizing the Dutertes after it published an article about former President Duterte's call to support his daughter Sara's potential bid for the presidency in 2028.[36] The comments, which leveraged existing narratives against political dynasties and referenced the alleged criminal involvements of the Dutertes, were posted at regular intervals. They were traced to inauthentic accounts created between December 2023 and January 2024 that used images of public personalities as their profile pictures.



[redacted] [redacted]
Nakakapanghinayang masaksihan ang tahasang pagwawalang-bahala ni Duterte sa mga alalahanin at hangarin ng sambayanang Pilipino.😡😡😡
15h Like Reply

[redacted] [redacted]
Ang panawagan ni Duterte na suportahan si Sara ay nagpapakita lang na isa silang gahaman sa pwesto! 😡😡
15h Like Reply

[redacted] [redacted]
Ang suporta para sa bid ni Sara ay parang isang extension ng rehimen ni Duterte sa halip na isang bagong simula para sa bansa.🤦😡
15h Like Reply

[redacted] [redacted]
Ang pagtulak ni Duterte para sa pagkapangulo ni Sara ay amoy ng dynastic na pulitika, na sumisira sa mga demokratikong prinsipyo.😤😡
15h Like Reply

[redacted] [redacted]
Nakakadismaya na makitang inuuna ni Duterte ang interes ng pamilya kaysa sa kapakanan ng bansa.! 🤦🙄
15h Like Reply

[redacted] [redacted]
can't wait to see you in jailed! both of you Sarah ang Digong! 🤣🤣🤣
20h Like Reply

[redacted] [redacted]
can't wait to see you jailed! both of you Sarah ang Digong!
1d Like Reply

Pro-China, pro-Russia content

Research conducted by Rappler and The Nerve shows that the Philippines' foreign relations significantly influence online engagement among Filipinos. Historically aligned with the US, most Filipinos have long distrusted China due to territorial disputes, notably during Benigno Aquino III's presidency. Aquino filed a case with the Permanent Court of Arbitration in The Hague challenging China's extensive maritime claims in the South China Sea, and obtained an overwhelmingly favorable ruling in 2016, just 12 days after transferring the presidency to Rodrigo Duterte.

Under President Duterte, warmer relations with China and Russia developed, subsequently reflected in a rise of pro-China and pro-Russia sentiment online. Rappler's investigations revealed foreign IOs by both Russia and China during this period, with local networks amplifying their messages. Various governments and organizations consider Russia and China the biggest threat actors involved in IOs.

In early 2019, Rappler reported that a Russian disinformation network had penetrated Philippine social media, using "experts" to legitimize false information. Rappler linked the network to Russia's Internet Research Agency (IRA), identifying Adam Garrie as a key figure spreading misleading claims.[37] Research by New Knowledge and a US Senate report connected Garrie's activities to the broader Russian disinformation network. His views were prominently featured by The Manila Times and the website of a self-identified think tank called Eurasia Future, and were disseminated on pro-Duterte pages like those managed by Sasot.

Pro-Russian and pro-Chinese sentiments persisted among social media personalities and networks even after President Marcos' decision to align with the US and its other allies.

Amid escalating geopolitical tensions and territorial disputes in the South China Sea and West Philippine Sea, the pro-Duterte TikTok account @paglinawanestenzo posted pro-China and pro-Russia content in July 2023, according to an IMF report. The account shared a deepfake video of Russian President Vladimir Putin misleadingly warning Americans about election interference and another misleading claim about China deploying robot soldiers, originally from a 2021 report about China's border with India.[38] Although the account was disabled in September 2023, it quickly reappeared as @paglinawanestenzo4, featuring Putin in its profile picture. The new account continued to criticize President Marcos while supporting former President Duterte. It endorsed Duterte's call for Mindanao's independence in February 2024 and claimed Russian support for the secession movement.

Since 2016, Rappler and The Nerve have monitored a pro-China network spreading propaganda among Filipino communities online. The Nerve traced the network's activities back to 2018, during the Duterte administration. The Nerve detected a shift within pro-China networks in 2023. Previously aligned with both pro-Duterte and pro-Marcos groups, these networks distanced themselves from supporters of Marcos after his decision to strengthen ties with the US. After the expansion of the Enhanced Defense Cooperation Agreement (EDCA) on American bases and the Chinese Coast Guard's water cannon attack on the PCG, the network downplayed the water cannon incident, dismissed Chinese harassment, discredited the 2016 arbitral ruling against China, and condemned the expansion of EDCA sites as US militarization.[39]

Led by the self-styled think tank Integrated Development Studies Institute (IDSI) and social media personalities Sasot and Anna Malindog-Uy, the network promoted "pro-authoritarian, anti-liberal content that is skewed favorably toward China," according to Rappler. This was then funneled into hyper-partisan Facebook groups such as the Philippines-China Friendship Club (PCFC). Sasot and Malindog-Uy's pro-China positions were also given a platform on The Manila Times and on various segments on SMNI.

A study done for the US-based International Republican Institute found that self-interested businesspeople in the Philippines have developed a "dependency relationship" with China and have launched think tanks and centers dedicated to promoting friendly views of China. These include IDSI, PCFC, and Herman Tiu Laurel's Philippine–BRICS Strategic Studies.[40]

Rappler and The Nerve also tracked narratives disputing the arbitral ruling favoring the Philippines' claim in the West Philippine Sea as early as 2018 by pro-China communities on Facebook that emerged during the Duterte administration. It identified Sasot as one of the top actors promoting narratives justifying China's joint exploration in the Philippines' exclusive economic zone.[41]

The Nerve detected a shift within pro-China networks in 2023. Previously aligned with both pro-Duterte and pro-Marcos groups, these networks distanced themselves from supporters of Marcos after his decision to strengthen ties with the US.

Straight out of China

Research conducted for this project, both published and unpublished, has indicated an increasing volume of seemingly coordinated anti-Manila and pro-Beijing narratives originating from various Chinese sources. These include the Chinese government, state media, academics, influencers, and even anonymous accounts. The narratives predominantly focus on the West Philippine Sea, security arrangements among the Philippines, the US, and other allies, and tensions between Taiwan and Mainland China.

In January 2024, Probe monitored anonymous Chinese accounts on X that disputed the 2016 ruling upholding the Philippines' sovereignty over its exclusive economic zone and invalidating China's reclamation activities in the South China Sea. The anonymous accounts circulated art cards in a potentially coordinated effort, claiming a historical Chinese presence in the Spratly Islands for 2,000 years and denying the arbitration case's legality.

According to an investigation by Philstar.com and DoubleThink Lab, a network of anonymous Chinese internet users capitalized upon recent calls for Mindanao's independence by spreading a narrative that civil war is imminent in the Philippines.[42] Speculations were also circulated across Chinese platforms that conflict was likely to arise due to President Marcos' pro-US stance. These posts fearmongered and sowed confusion on the origins of the maritime conflict, shifting the attention to a fabricated narrative.

China's state media have been at the forefront of promoting narratives in a highly coordinated manner as part of Beijing's attempt to reshape the global information environment through "discourse power." Kenton Thibaut, a senior resident China fellow with the Atlantic Council's Digital Forensic Research Lab (DFRLab), highlighted China's "media convergence" in a recent report.[43] Thibaut referred to "the integration of internal and external Chinese Communist Party (CCP) propaganda, the online and offline channels for its dissemination, and the mechanisms of oversight on which communications systems rely."

Thibaut's report explored three vectors of media convergence:

- Channel expansion: This vector focuses on increasing the presence of Chinese state media and entities across various platforms, aiming to expose a broader international audience to Chinese narratives and norms. The goal is to erode the global "discourse dominance" of the West.
- Content innovation: This entails adapting content to resonate with specific audiences through "precise communication" strategies while hiding the content's origins within Chinese state sources, or controlling local media environments through content-sharing agreements.
- Governance of technological infrastructure and digital connectivity: This vector includes promoting China-sponsored standards, norms, and governance protocols in prioritized industries, particularly information and communications technologies, ensuring their widespread adoption, especially in the Global South.

Unpublished research by network members and Doublethink Lab on potential IO incidents by Chinese state media highlights persistent pro-China narratives and derogatory portrayals of the Philippines and the US, especially after confrontations or controversial statements by Chinese officials. These multifaceted operations employ cross-posting, strategic influencer engagement, and the inclusion of "experts" from both within and outside China to shape public opinion. They leverage Chinese-language media in the Philippines and elsewhere and overseas Chinese forums to cultivate support within this demographic.

These trends were observed amid incidents such as Chinese Ambassador Huang Xilian's "veiled threat" against overseas Filipino workers (OFWs), the seventh anniversary of the Philippines-China South China Sea arbitral ruling that favored Manila, and attacks by the Chinese Coast Guard against the Philippine Coast Guard.

A June 2024 investigation by Philstar.com and Doublethink Lab highlighted a propaganda campaign by Chinese state media portraying the Philippines as the aggressor in the South China Sea confrontations. People's Daily, the official newspaper of the Chinese Communist

Party's Central Committee, and other media outlets backed by the Chinese government, framed Philippine vessels as the instigators in incidents during resupply missions to the Ayungin Shoal (Second Thomas Shoal).[44]

Aside from Beijing-affiliated accounts, Samachar Dainik from Nepal, Korea Post, and a dubious site called Subic Bay Naval Station posted articles from the People's Daily. Amid the circulation of these articles, a deepfake audio clip of President Marcos allegedly ordering an attack against China went viral, exacerbating efforts to sow confusion among Filipinos.

During the seventh anniversary of the arbitral ruling in July 2023, Chinese Foreign Ministry spokesperson Wang Wenbin reiterated China's rejection of the ruling. This position was broadcast by Xinhua, China's state news agency, which falsely claimed that over 100 countries supported China's stance. Chinese state media, including the Global Times and People's Daily, published editorials condemning the "hype" over the ruling's anniversary. Military blogger Gu Huoping echoed similar sentiments, with his commentary appearing almost simultaneously on Weibo, Tencent, Sohu, and Netease.

To deflect criticism of Chinese IOs, China's state media have accused the Philippines of orchestrating its own IOs against China over the West Philippine Sea issue to provoke regional conflict.

Unpublished research by the network noted the value of so-called experts in legitimizing Chinese propaganda and shaping public discourse. For instance, a Chinese academic and other "experts" accused the Philippines of siding with the US against China after the Philippines released its National Security Policy, which emphasized territorial defense and the Taiwan Strait situation. Military strategist Shao Yongling, who has a large following on the Chinese video-sharing platform Ixigua, further criticized the Philippines for its alleged provocations, a narrative that was amplified on Chinese social media platforms such as Baidu, Sohu, Netease, Weibo, QQ, and WeChat.

Narratives lauding and defending former President Duterte have been actively pushed by Chinese social media influencers. Attacks on President Marcos' wife, Liza Araneta, including by a leading academic, have also been identified in the Chinese information environment.

Diversionary tactic

In 2023, Filipino journalists and maritime law expert Jay Batongbacal received email and text messages alleging that Vietnam had plans to occupy the Spratly Islands, according to a Philstar.com report. These messages appeared to be aimed at diverting attention from China's regional aggression. The senders, claiming to be associated with a Vietnamese construction company, purportedly had insider information about the "confidential" militarization plans.[45]

Degree

Threat actors often aim to extend the reach of their content beyond its original platforms and communities. As mentioned above, a key tactic in IOs is cross-posting content across multiple platforms. This strategy bombards the information ecosystem with targeted narratives promoting a specific ideology.

The network has identified an emerging trend of utilizing lesser-known websites and social media platforms to disseminate false claims and potentially harmful content. Malign actors mirror their content on platforms such as Bilibili and ViralPitch to maximize monetization and broaden their reach. The network observed the growing use of relatively new platforms in cross-posting, such as TikTok/Douyin, WeChat, Weibo, Baijahao, NetEase, and Guancha.

The network has determined that domestic IOs often follow a cascading pattern. They begin with hyper-partisan vloggers or self-styled media outlets spreading content on YouTube. This content is then embedded on dubious websites, which act as buffers against platform regulations on Facebook and YouTube. These website links are amplified by various Facebook accounts, enabling the information to bypass the fact-checking measures of both platforms.

Foreign IOs, such as Chinese narrative warfare, typically start with state media or government officials. These narratives are then echoed by so-called experts through commentaries and analyses, thereby legitimizing the claims. These narratives are amplified across various social media platforms, resulting in a flood of content.

Effect

IOs can exacerbate polarization within a country. They exploit existing divisions within communities and deepen discord by amplifying divisive narratives, as shown in the examples promoting or attacking the Marcoses and Dutertes. This can destabilize the target country, making it less capable of collectively addressing external threats.

Another potential effect of IOs is the erosion of trust in democratic institutions and the media. Covert manipulation of public opinion can sow confusion, increase skepticism among citizens, and foster disillusionment in these institutions.

Chinese actors employ narrative warfare to sway Philippine public opinion, policymakers, and stakeholders to adopt a more appeasing stance toward China's claims, thereby weakening regional unity and resistance against China's pursuit of its interests. The overall aim of Chinese IOs in the Philippines is to advance China's strategic interests, expand its influence, and counter any opposition or resistance to its presence and activities in the region, according to a Freedom House study on China's global media influence.[46]

Unpacking the 'Next Ukraine' Narrative

The network's first in-depth IO analysis focused on the narrative that the Philippines would turn into the "next Ukraine" or the "Ukraine of Asia." This narrative emerged after the Marcos administration shifted its foreign policy toward closer alignment with the US after six years of the Duterte administration, which favored ties with China. This pivot resulted in an agreement between Manila and Washington in February 2023 that expanded EDCA sites to include new military sites in Cagayan, Isabela, and Palawan.

The IMF used basic strategies of monitoring and leveraging its existing database, dwelling mostly on sharing behavior combined with several tools such as CrowdTangle, search engines (Bing, Baidu, Yandex, Google), and Whopostedwhat. The table below shows how the network deconstructed this narrative using the ABCDE framework.

Actors	• Nonstate actors: Self-styled think tanks and academic institutions • Individuals: So-called political analysts and opinion columnists with unverified academic credentials

Behaviors	• Establishing legitimacy using academic, nonprofit, and media-styled accounts • Mirroring official positions and statements of government officials • Creating low-quality accounts, including personal profiles and pages • Cascading content from Global Talk News Radio
Content	• Amplification of the "Ukrainization of the Philippines" narrative via The Manila Times opinion columnists and IDSI website and social media pages • Promotion of a conspiracy theory that the COVID-19 virus originated in Fort Detrick, a military installation in Maryland, USA; calls for a probe into Fort Detrick were formally endorsed by the Chinese Embassy in Manila and echoed by a so-called political analyst and pro-Duterte account • Criticisms against President Marcos • Narratives of the "Collective West" waging all-out war on Russia because of "anti-Slavic racism"
Degree	• Potential audience: Pro-administration supporters (Duterte and Marcos)/ UniTeam supporters • Reach, engagement, and distribution strategies of websites, social media, other online platforms and events with niche audiences • Virality: Cross-posting to artificially generate online discussion on issues • Scale: Coordination of multiple "think tanks," media outlets, and social media pages, signaling ongoing influence operations
Effect	• Aggravates polarization over geopolitical tensions in the West Philippine Sea and South China Sea and the crumbling Marcos-Duterte alliance • Legitimizes China's maritime claims and positions by inviting think tank positions such as the South China Sea Probing Initiative • Erodes trust in legitimate media outlets, journalists, and subject matter experts on maritime law, including attacks against fact-checkers (VERA Files and PressOnePH) and Coast Guard spokesperson Jay Tarriela

Cyber-enabled Attacks against PH Media

In the realm of IOs, malign actors frequently attack the integrity of reputable media outlets by accusing them of bias, corruption, or partisanship. This tactic is intended to erode public trust in the credibility and integrity of legitimate news sources by spreading conspiracy theories that suggest media collusion or hidden agendas.

Malign actors often release false or twisted information to create confusion, making it difficult for the public to distinguish between credible and noncredible sources. They also amplify extreme views or promote contentious issues, polarizing public opinion, hindering the development of consensus on the reliability of information sources, and further degrading public trust.

To lend an appearance of credibility to their operations, malign actors impersonate legitimate entities, especially the media, by creating fake accounts or websites that mimic reputable organizations. They also produce maliciously crafted articles designed to spread false narratives or distort public perception on specific topics. These articles often leverage emotional or sensationalist angles to enhance their impact.

As stated earlier, MindaNews was one of many victims of a Chinese gambling network scraping content off its official website. Inquirer.net was mimicked by a dupe site promoting a crypto trading platform while the now-defunct CNN Philippines was copied by an impostor site on social media to advertise products.

A deepfake video in which Rappler founder Maria Ressa is shown talking about Bitcoin in an artificially generated voice recently spread on Facebook, including through newly created accounts, and fake news websites imitating Rappler and CNN Philippines.[47] An investigation by Qurium traced the attack to a Russian scam network and confirmed that the campaign was aimed at Philippine audiences.[48] This deepfake shows the increased sophistication of artificial intelligence (AI), which malign actors can use to sway public opinion, sow confusion and distrust, and discredit reputable organizations and personalities.

The social media pages of a Chinese state-run media outlet called Media Unlocked (also known as MediaUnlock, QidiMediaUnlocked, and China Unlocked), which describes itself as a group of "China-based journalists," released videos accusing Philippine media outlets PressOnePH and Philstar.com of biased coverage on the geopolitical tensions in the South China Sea and West Philippine Sea. PressOnePH and Philstar.com, both verified signatories of the International Fact-Checking Network's Code of Principles, were identified in two videos from the account, which is associated with China Daily, an English-language newspaper owned by the Chinese Communist Party's Central Propaganda Department.

The attacks were made after PressOnePH published an alert about the Media Unlocked account's increased engagement.[49] Counterpart accounts on X, Facebook, and YouTube posted a video refuting PressOnePH's article, highlighting its ties to Internews, the IMF, and USAID, and suggesting it was involved in disinformation campaigns. MediaUnlocked's video on X was reposted by Chinese Ambassador to Cuba Ma Hui (马辉).[50]

MediaUnlocked/China Daily targeted PressOnePH, Interaksyon, and the Philippine Center for Investigative Journalism (PCIJ) in its June 12 and 13, 2024 video series on "Information war" and "silencing voices" posted on Facebook, X, and YouTube. These videos mentioned Internews, the IMF, and USAID for allegedly "contro[lling] the narrative and influenc[ing] public perception in the South China Sea." The two-part series reacted to a CNN Global report featuring reporter Will Ripley, which called out Media Unlocked's use of AI and synthetic media enhancements and mentioned the banning of its TikTok account.[51]

Countering IOs

Influence operations, both foreign and domestic, represent a significant and growing threat as they aim to manipulate public opinion and erode trust in institutions. Dealing with these operations requires a clear framework and a multi-stakeholder approach due to their growing complexity and the need for diverse expertise. In the Philippine context, only a few organizations are equipped to manage large-scale campaigns against IOs in real time and sustain countermeasures over prolonged periods.

Drawing on the monitoring and investigation experience of the network over the past year, the following strategies and initiatives are recommended to effectively navigate and counter IOs:

Monitoring and detection

- Invest in social media monitoring tools. Support initiatives that track suspicious online activity and identify emerging foreign IO (FIO) campaigns.
- Invest in fact-checking platforms. Support fact-checking initiatives and provide reliable sources of truthful information.
- Support open-source intelligence (OSINT) initiatives. Fund organizations that leverage publicly available data to track and expose FIO networks.
- Fund training programs for journalists that teach journalists best practices for verifying information and identifying FIO narratives.
- Support independent investigative journalism. Equip newsrooms with resources to build teams dedicated to understanding and reporting disinformation and IOs.
- Fund investigative journalism focused on FIO attribution. Support investigative efforts that expose the actors behind FIOs and their financial backers.

Defensive communication

- Develop plans and create strategies for accurate and timely information dissemination during IO crises.
- Conduct initiatives that are preventive in nature and examine the effectiveness of IOs with specific audiences.
- Stress the need for newsrooms and journalists to be up to date on technology and digital security news. Improve the ability of news media organizations and workers to design and implement data and information security strategies.
- Avoid the perception of bias. Present the information and/or research in the most accurate way possible, factually and in context, and acknowledge uncertainty where it exists.

Public awareness and media literacy

- Explore areas for further investigation, such as the disinformation-for-hire industry, creator economy, algorithmic bias, or distribution strategies. Provide resources for studies that contribute to the body of knowledge and fill gaps on understanding disinformation and IOs.
- Invest in media literacy programs. Support initiatives that equip citizens with critical thinking skills to identify and resist FIO narratives.
- Develop resources for identifying bias. Support the creation of guides that help media and citizens recognize biased narratives from foreign state media outlets.
- Support research on foreign state media ecosystems. Fund research that analyzes the strategies of state-controlled media and explores how to counter foreign influence in the Philippines.
- Fund research on FIO tactics. Back research projects analyzing foreign influence techniques and developing recommendations for countering them.

Leveraging technology

- Invest in high-quality translation services. Support the development of accurate translation tools crucial for analyzing FIO campaigns in multiple languages.
- Fund the development of FIO watchlists and databases. Support the creation of centralized repositories that track FIO actors, tactics, and target countries.

- Promote gamified media literacy. Develop interactive games that educate people about the mechanics of disinformation. Teach strategies to effectively identify and counter disinformation and IOs.

Collaboration and information sharing

- Foster and enhance collaborative initiatives and coordination among public and private stakeholders, including media, legal, national security, foreign policy disciplines, and grassroots organizations, to counter emerging strategic narratives, tactics, and behaviors.
- Scale up collaboration with communities outside the capital, engaging a range of demographics including youth, the elderly, persons with disabilities, and residents of regions without internet access.
- Create a shared fact-checking database. Collaborate across response groups to compile and share fact-checking resources, tips, and counter-messages to boost trustworthy information and combat IOs.

Regulatory measures and policy development

- Empower existing regulators to oversee social media platforms. Actively monitor their decision-making process and encourage them to publicly share data.
- Make use of content moderation, upholding human rights and integrating due process at all stages.
- Integrate transparency into social media (e.g., Facebook or TikTok) policies and rule enforcement, specifically actions related to the removal of content or suspension of accounts.
- Consider the role of social media or state involvement within the broader media regulatory framework.
- Craft policies that protect free expression principles, ensure transparency, impose liability, and address noncompliance.
- Explore using fraud legislation to clean up social media.

About the Initiative for Media Freedom Partners

Internews is a nonprofit that supports independent media in 100 countries — from radio stations in refugee camps, to hyper-local news outlets, to filmmakers and technologists. Internews trains journalists and digital rights activists, tackles disinformation, and offers business expertise to help media outlets thrive financially. For nearly 40 years, it has helped partners reach millions of people with trustworthy information that saves lives, improves livelihoods, and holds institutions accountable.
https://internews.org/

Internews Philippines, funded by the United States Agency for International Development (USAID) with the support of the American people, implement the Initiative for Media Freedom (IMF) since 2019. IMF objectives include supporting an environment for a free press, enhancing the capacity of institutions to counter disinformation, and supporting media self-regulation.

Recognizing the growing threat from malign actors running disinformation campaigns and influence operations (IOs), especially of foreign information manipulation and interference (FIMI), a component was established under the IMF in May 2023 which aspired to mobilize a network of civil society and media organizations focused on identifying and investigating IO/FIMI in the Philippines. This collaboration enables rapid information-sharing, comprehensive investigations, and public access to findings. Called PH-PROTECT, this activity enhanced the capability of local newsrooms in their verification and digital investigation skills on tackling IO/FIMI, representing a vital step in protecting the integrity of the Philippine information ecosystem and upholding democratic values.

The PH-PROTECT partners include the following:

MindaNews is the news service arm of the Mindanao Institute of Journalism, which was established in 2001 by journalists who believe that the story of Mindanao can best be told by Mindanawons. It started as a cooperative and transitioned into an institute in 2016 to enhance its media services for readers and provide training for schools and journalists.
https://www.mindanews.com/

Philstar.com is one of the Philippines' leading and most recognized digital brands in journalism. Philstar Global Corp., which owns and operates Philstar.com, is the digital company under the STAR Group of Publications, whose flagship print publication is The Philippine Star, a leading national broadsheet.
https://www.philstar.com/

PressONEPH is an independent news and information website dedicated to providing news that empowers readers and helps them navigate the digital and interconnected world. It is owned and operated by PressOnePH News and Information Service Inc.
https://pressone.ph/

Probe is an independent media production company founded in 1988 and a pioneer in documentary production in the Philippines. It has digitized its extensive collection of archival material and made it publicly accessible to encourage Filipinos to revisit history and help combat disinformation. Probe is owned and operated by Probe Productions Inc.
https://probe.ph/

Rappler is a news website and social news network founded by veteran journalists from the broadcast, print, and online media. Its mission is to produce stories that inspire community

engagement and social change. The name Rappler is derived from the words “rap” and “ripple.” Rappler is owned primarily by Rappler Holdings Corp.
https://www.rappler.com/

The Nerve is a data consultancy specializing in data forensics to bridge insight and action. The group's model grew out of big data investigations aimed at mapping the information ecosystem of the Philippines and understanding how technology has transformed information cascades and their impact on behavior.
https://www.thenerve.co/

Doublethink Lab (DTL) was founded in 2019 to strengthen democracy through enhancing digital defenses. It researches malign Chinese influence operations and their impacts using internally developed digital tools and methodologies. DTL seeks to facilitate a global civil society organization (CSO) network to bolster democratic resilience against digital authoritarianism.
https://doublethinklab.org/

Qurium is a Swedish media foundation committed to defending digital rights, freedom of speech, and internet security. It has provided secure hosting and other digital security services to media websites and human rights organizations facing attacks on their communication channels.
https://www.qurium.org/

Yvonne T. Chua is an associate professor of journalism at the University of the Philippines. She has completed studies on information disorder in the Philippines and has been involved in fact-checking and news literacy initiatives.

This playbook is made possible by the support of the American People through the United States Agency for International Development (USAID). The content of this playbook is the sole responsibility of Internews under the Initiative for Media Freedom (IMF) project. It does not necessarily reflect the views of USAID or the United States Government.

Notes

[1] Gleicher, Nathaniel. "Removing Coordinated Inauthentic Behavior." Meta. July 8, 2020. https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/ (accessed June 26, 2024).

[2] Nimmo, Ben, C. Shawn Eib, and Léa Ronzaud. "Operation Naval Gazing." Graphika. September 22, 2020. https://graphika.com/reports/operation-naval-gazing

[3] Baizas, Gaby. "Twitter suspends accounts in Ferdinand 'Bongbong' Marcos Jr. network." Rappler. January 21, 2022. https://www.rappler.com/philippines/elections/twitter-suspends-accounts-ferdinand-bongbong-marcos-jr-network-january-2022/ (accessed June 26, 2024).

[4] Fenol, Jessica. "Millions of Facebook, Instagram content removed during Halalan 2022 due to violations." ABS-CBN News. August 5, 2022. https://news.abs-cbn.com/business/08/05/22/millions-of-fb-ig-content-removed-during-2022-elections-due-to-violations (accessed June 26, 2024).

[5] Fallorina, Rossine, Jose Mari Hall Lanuza, Juan Gabriel Felix, Ferdinand Sanchez II, Jonathan Corpus Ong, and Nicole Curato. "From Disinformation to Influence Operations: The Evolution of Disinformation in Three Electoral Cycles." Internews. 2023. https://internews.org/resource/from-disinformation-to-influence-operations-the-evolution-of-disinformation-in-three-electoral-cycles/ (accessed June 26, 2024).

[6] Chi, Christina and Nadie Esteban. "Chinese media pushes 'Philippines as aggressor' narrative before viral Marcos deepfake." Philstar.com. June 8, 2024. https://www.philstar.com/headlines/2024/06/08/2361039/chinese-media-pushes-philippines-aggressor-narrative-viral-marcos-deepfake (accessed June 26, 2024).

[7] Office of the Spokesperson of the United States Department of State. "Joint Statement from the United States, United Kingdom, and Canada on Countering Foreign Information Manipulation." US Department of State. February 16, 2024. https://www.state.gov/joint-statement-from-the-united-states-united-kingdom-and-canada-on-countering-foreign-information-manipulation/ (accessed June 26, 2024).

[8] Gleicher, Nathaniel, Margarita Franklin, David Agranovich, Ben Nimmo, Olga Belogolova, and Mike Torrey. "Threat Report: The State of Influence Operations 2017-2020." Facebook. May 2021. https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

[9] Hénin, Nicolas. "FIMI: Towards a European Redefinition of Foreign Interference." EU DisinfoLab. April 2023. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf

[10] Yadav, Kamya, Martin J. Riedl, Alicia Wanless, and Samuel Woolley. "What Makes an Influence Operation Malign?" Carnegie Endowment for International Peace. August 2023. https://carnegieendowment.org/research/2023/08/what-makes-an-influence-operation-malign?lang=en (accessed June 26, 2024).

[11] Ördén, Hedvig and James Pamment. "What Is So Foreign About Foreign Influence Operations?" Carnegie Endowment for International Peace. January 2021. https://carnegieendowment.org/research/2021/01/what-is-so-foreign-about-foreign-influence-operations?lang=en

[12] Pamment, James. "The ABCDE Framework." Carnegie Endowment for International Peace. September 1, 2020. https://www.jstor.org/stable/resrep26180.6

[13] Ibid., 4.

[14] Nimmo, Ben. "The 4D Model of Disinformation Campaigns." Michigan Online. August 20, 2020. Educational video, 6:54. https://online.umich.edu/teach-outs/disinformation-misinformation-and-fake-news-teach-out/lessons/4d-model-disinformation-campaigns/

[15] DISARM Foundation. "Disarm Framework Explorer." https://disarmframework.herokuapp.com/

[16] Meta. "Facebook Community Standards." https://transparency.meta.com/policies/community-standards/inauthentic-behavior (accessed June 26, 2024).

[17] Chi, Cristina. "Anonymous accounts flood WPS discourse with 'CIA agent' accusations vs PCG spox." Philstar.com. December 4, 2023. https://www.philstar.com/headlines/2023/12/04/2316405/anonymous-accounts-flood-wps-discourse-cia-agent-accusations-vs-pcg-spox/amp/ (accessed June 26, 2024).

[18] Lopez, Rommel. "Socmed personality's pro-China narrative on WPS shared across various pro-China disinformation websites." PressOnePH. November 23, 2023. https://pressone.ph/socmed-personalitys-pro-china-narrative-on-wps-shared-across-various-pro-china-disinformation-websites/ (accessed June 26, 2024).

[19] Ocampo, Yas. "Chinese network clones hundreds of websites, including MindaNews – Qurium Media." MindaNews. November 15, 2023. https://mindanews.com/top-stories/2023/11/chinese-network-clones-hundreds-of-websites-including-mindanews-qurium-media/ (accessed June 26, 2024).

[20] Qurium Media. "Hundreds of sites cloned to promote a Chinese gambling network." November 15, 2023. https://www.qurium.org/alerts/philippines/hundreds-of-clone-sites-used-to-promote-a-chinese-gambling-network/ (accessed June 26, 2024).

[21] Inquirer.net. "Fact Check: Alleged article on Toni Gonzaga and Willie Ong." April 4, 2024. https://newsinfo.inquirer.net/1926089/fact-check-alleged-article-on-toni-gonzaga-and-willie-ong (accessed June 26, 2024).

[22] Raffy Tulfo In Action. "Facebook post debunking fake websites using Tulfo's name." March 26, 2024. https://web.facebook.com/photo/?fbid=1006503384177186&set=a.298845928276272

[23] Lundstrom, Tord and Harper, Sam. "Tell of Spring – Exposing Crypto Scam Affiliate Networks." May 14, 2024. https://www.qurium.org/alerts/tell-of-spring-exposing-crypto-scam-affiliate-networks/ (accessed July 30, 2024)

[24] Arasa, Dale. “Crypto scams impersonating Inquirer.net and other news sites.” Inquirer.net. May 15, 2024. https://technology.inquirer.net/134441/crypto-scams-impersonate-news (accessed June 26, 2024).

[25] Philippine Council for Health Research and Development. “Filipino scientist recognized as global expert in orthopedics.” https://www.pchrd.dost.gov.ph/news_and_updates/filipino-scientist-recognized-as-global-expert-in-orthopedics/ (accessed June 26, 2024).

[26] Qurium Media. “The tip of the iceberg – the algorithm fraud industry.” May 1, 2022. https://www.qurium.org/alerts/the-tip-of-the-iceberg/ (accessed June 26, 2024).

[27] Wright, Charity. “The Diamond Model for Influence Operations Analysis.” Recorded Future. 2022. https://go.recordedfuture.com/hubfs/white-papers/diamond-model-influence-operations-analysis.pdf

[28] Philstar.com. “Fact check: Media actually did report on Ilocos Sur caravan for Marcos.” November 9, 2021. https://www.philstar.com/headlines/2021/11/09/2140100/fact-check-media-actually-did-report-ilocos-sur-caravan-marcos (accessed June 26, 2024).

[29] VERA Files. “New Zealand PM DID NOT express support for Marcos Jr.” January 21, 2022. https://verafiles.org/articles/vera-files-fact-check-new-zealand-pm-did-not-express-support (accessed June 26, 2024).

[30] Navallo, Mike. “'Maharlika' YouTube account in Pangilinan cyber libel complaint.” ABS-CBN News. February 25, 2022. https://news.abs-cbn.com/news/02/15/22/doj-moves-to-preserve-maharlika-youtube-account-in-pangilinan-cyber-libel-complaint (accessed June 26, 2024).

[31] Rappler. “MISSING CONTEXT: 10 multi-role response vessels delivered under Duterte.” August 29, 2021. https://www.rappler.com/newsbreak/fact-check/multi-role-response-vessels-delivered-duterte-administration/ (accessed June 26, 2024).

[32] Rappler. “IRRI and Central Luzon State University were not established during Martial Law.” September 30, 2022. https://www.rappler.com/newsbreak/fact-check/international-rice-research-institute-central-luzon-state-university-not-established-martial-law/ (accessed June 26, 2024).

[33] Malasig, Jeline. “Pro-Duterte accounts push survey showing Rody as top Senate bet in 2025.” Philstar.com. November 9, 2023. https://www.philstar.com/headlines/2023/11/09/2309596/pro-duterte-accounts-push-survey-showing-rody-top-senate-bet-2025 (accessed June 26, 2024).

[34] Sarmiento, Bong. “Pro-Duterte supporters magnify survey showing Sara with high trust rating.” MindaNews. December 20, 2023. https://mindanews.com/top-stories/2023/12/pro-duterte-supporters-magnify-survey-showing-sara-with-high-trust-rating/ (accessed June 26, 2024).

[35] Philstar.com. “Facebook post detailing coordinated content against VP Sara Duterte.” March 22, 2024. https://www.facebook.com/philstarnews/posts/pfbid09xx3fWPAYQGWonQS2gW83F2x1cPEiZBZjvW3J7nrNVg9C1boTj9jnNoL3zokFSPil

[36] Espinosa, Ian Carl. “Trolls pounce on Duterte’s call for support to Sara’s bid for the Presidency in 2028.” MindaNews. March 13, 2024. https://mindanews.com/top-stories/2024/03/trolls-pounce-on-dutertes-call-for-support-to-saras-bid-for-the-presidency-in-2028/ (accessed June 26, 2024).

[37] Rappler. “EXCLUSIVE: Russian Disinformation System Influences PH Social Media.” January 22, 2019. https://www.rappler.com/newsbreak/investigative/221470-russian-disinformation-system-influences-philippine-social-media/ (accessed June 26, 2024).

[38] The World in One News (WION). “Gravitas: China Deploys ‘Robot Soldiers’ Along the Border With India.” December 31, 2021. https://www.youtube.com/watch?v=afPbga9ooX4 (accessed June 26, 2024).

[39] Macaraeg, Pauline. “How pro-China Propaganda Is Seeded Online in the Philippines.” Rappler. November 1, 2023. https://www.rappler.com/newsbreak/investigative/ways-how-china-propaganda-seeded-online-philippines/ (accessed June 26, 2024).

[40] Lee, Lilly Min-Chen, Camba, Alvin and Loh, Benjamin Yew Hoong. “Countering China’s Information Manipulation in the Indo-Pacific and Kazakhstan: A Framework for Understanding and Action.” International Republican Institute. 2023. https://www.iri.org/resources/countering-chinas-information-manipulation-in-the-indo-pacific-and-kazakhstan/

[41] Ibid.,13.

[42] Chi, Cristina. “Chinese Accounts Pounce on Mindanao Secession Issue to Warn of ‘civil War’ in Philippines.” Philstar.com. June 10, 2024. https://www.philstar.com/headlines/2024/06/10/2361800/chinese-accounts-pounce-mindanao-secession-issue-warn-civil-war-philippines (accessed June 26, 2024).

[43] Thibaut, Kenton. “Chinese Discourse Power: Capabilities and Impact.” Atlantic Council. August 2023. https://www.atlanticcouncil.org/wp-content/uploads/2023/08/Chinese-Discourse-Power-Capabilities-and-Impact-1.pdf

[44] Ibid.,3.

[45] Chi, Cristina. “Influence Ops Target Journalists, Expert as China Vessels Patrol West Philippine Sea.” Philstar.com. January 19, 2024. https://www.philstar.com/headlines/2024/01/19/2327000/influence-ops-target-journalists-expert-china-vessels-patrol-west-philippine-sea (accessed June 26, 2024).

[46] Han, BC and Elemia, Camille. “Philippines.” Freedom House. https://freedomhouse.org/country/philippines/beijings-global-media-influence/2022 (accessed June 26, 2024).

[47] Mendoza, Gemma and Gonzalez, Gelo. “Russina scam network circulates Maria deepfake through Facebook, Microsoft’s Bing. Rappler. March 3, 2024. https://www.rappler.com/technology/maria-ressa-bitcoin-deepfake-russian-scam-network-facebook-microsoft-bing/ (accessed July 30, 2024).

[48] Qurium. “Deep Fake of Maria Ressa Connected to Russian Cyberscam Network.” March 4, 2024. https://www.qurium.org/alerts/philippines/deep-fake-video-of-maria-ressa-connected-to-cyberscam-network-in-russia/ (accessed July 30, 2024).

[49] PressOnePH. “ALERT: China Daily’s Socmed Propaganda Push Gets More Traction on TikTok.” May 4, 2024. https://pressone.ph/alert-china-dailys-socmed-propaganda-push-gets-more-traction-on-tiktok/ (accessed June 26, 2024).

[50] China Ambassador to Cuba MA Hui’s profile. https://x.com/mahuichina?s=21&t=rF8-9J8lOkHr8PuX7BCQKw

[51] Johnson, Royce. “‘This Is so Creepy’: Student Claims Someone Cloned Her Image.” CNN. May 2024. https://edition.cnn.com/2024/05/22/world/video/deepfakes-china-russia-video-ebof-ripley-pkg-digvid (accessed June 26, 2024).