NISOS TRADECRAFT

A Framework for Tackling Influence Operations During a Busy Election Year

March 2024

RESEARCH

NISOS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Tackling influence operations (IO) in a normal year is difficult enough. This year, half the world's population heads to the polls. For social media companies, unfettered IO campaigns targeting platform users—often involving disinformation, misinformation, or malinformation—can undermine user confidence in key markets and present reputational and legal risks. In this report, Nisos breaks down why IO is so complex and explains why it is so difficult to scope, identify, and remediate these activities without dedicated analytical and investigatory support.

- **Timing:** Planning ahead is key to tracking how IO threats to elections evolve. Election campaigns can be long, which means a lot can change, including the prevailing IO narratives. Nisos analyzes the broader IO landscape well ahead of and in the direct lead up to elections to understand those shifts.
- **State and Non-State Actors:** State actors in the IO space like Russia, China, and Iran are well known, but the scope of actors running IO includes domestic actors like media outlets, influencers, and political parties.
- **From Overt to Covert and Everything in Between:** Actors involved in IO proliferate their narratives through a variety of means, ranging from very visible, attributable, and overt activities to hidden, difficult-to-attribute, and covert measures. Some IO propagators will also seek to amplify grassroots messages that sow division or further polarization in a country of interest.
- **Information Flow On and Off Platform:** IO takes place on not just one platform but usually flows across multiple platforms, including those with few or no restrictions on content, enabling violative content to spread across the information ecosystem.
- **Broader Political Context:** A country's history and recent events color the political context—understanding that background is critical in assessing the intent behind election-driven IO campaigns.

Nisos acts as an embedded part of trust and safety teams, leveraging analysts who have in-depth expertise with the IO landscape and the techniques, tactics, and procedures that IO actors use, enabling us to detect and often attribute the sophisticated adversaries behind these operations.

DISCLAIMER:

The reporting contained herein from the Nisos research organization consists of analysis reflecting assessments of probability and levels of confidence and should not necessarily be construed as fact. All content is provided on an as-is basis and does not constitute professional advice, and its accuracy reflects the reliability, timeliness, authority, and relevancy of the sourcing underlying those analytic assessments.

BACKGROUND

This year, voters across more than 80 countries will cast their ballots. Elections are particularly challenging for social media companies, as IO occurring on social media platforms can have manifold off-platform repercussions, ranging from violent demonstrations to erosion of trust in democratic processes. These events can degrade user confidence in platforms, pushing them to flee to other online communities or lead to regulatory scrutiny.

It can be overwhelming for online platforms to devise effective solutions to address IO in just one high-profile election, let alone dozens. There is a significant amount of content available focused on prominent IO actors and narratives; however, such material too often focuses on tactical concerns over broader business implications. The impact on platforms extends beyond the scope of typical IO research, and concerns a company's reach and presence into a given country, volatility in that country, and past perceptions. Nisos can help online platforms and their trust and safety teams stay ahead of and defend against the multi-dimensional threats and risks posed by election-driven IO.

To complicate the landscape further, IO actors are using AI to create deepfake videos and voice cloning audio. While AI has factored into previous elections, generative AI capabilities have significantly improved in recent years and trust and safety playbooks derived from previous election cycles are already out of date. For example, some residents in New Hampshire received an AI-generated audio recording of President Biden urging voters not to vote in the primary election.[1] The Pakistan Tehree-e-Insaf party used generative AI to create footage of Imran Khan, its founder, urging supporters to vote on election day.[2] Nisos tracks these kinds of trends to maintain an up-to-date understanding of how actors use the information ecosystem to their advantage. We contribute these insights to trust and safety workflows tasked with identifying and tracking new IO techniques and campaigns on-platform.

TIMING

Mitigating IO threats to elections requires planning ahead. A lot can change during an election cycle, including the make-up of the candidate pool and the hot issues that provide fresh fodder for new IO narratives. It is not always feasible to fully attribute the actors behind the most potentially harmful narratives—including those that may lead to an offline event or present the highest reputational risk. At Nisos, we analyze the broader IO landscape months in advance of an election, including forecasting how narratives might evolve closer to the actual vote. We continue to revisit our assessments as election day nears, highlighting more current and specific examples of overt and covert IO, including by way of coordinated inauthentic behavior (CIB) on social media platforms.

- In Argentina, former president Alberto Fernandez announced that he would not be running for reelection at the end of April 2023, only four months before the primaries and six months

[1] https://www.theguardian[.]com/world/2024/feb/23/ai-deepfakes-come-of-age-as-billions-prepare-to-vote-in-a-bumper-year-of-elections

[2] https://www.reuters[.]com/world/asia-pacific/how-imran-khan-is-campaigning-jail-pakistan-ai-covert-canvassing-2024-02-05/

before the presidential election.[3] As such, IO campaigns and associated narratives had to adapt to the changing cast of candidates.

- In Indonesia, then-presidential candidate Prabowo Subianto did not pick his running mate, Gibran Rakabuming Raka, son of the former president Jokowi, until 22 October 2023, only two months before the election.[4] Results for “Gibran” on the Indonesian fact-checking website Cekfakta increased tenfold between the periods of 1 January to 21 October 2023 and 22 October 2023 to 14 February 2024—election day.
- In early January, Indonesia’s General Election Supervisory determinedthat Gibran broke campaign rules.[5] Cekfakta highlighted a misleading video that appeared on social media a week before the election claiming that Gibran’s trial had already started and that he faced disqualification from running for vice president, but the footage was of another, unrelated trial.[6]

STATE AND NON-STATE ACTORS

Russia’s efforts to influence US elections and China’s attempts to change voting patterns in Taiwan are prominent examples of how state actors are active in the IO space. Most people are familiar with IO efforts by Russia, China, and Iran, but other countries are growing their own capabilities in this space. Understanding which actors are seeking to amplify election-related narratives not only helps identify the different types of IO propagators but also their varying methods and goals. During elections, we often see state actors boost one candidate or try to denigrate another to persuade the targeted country’s electorate to vote accordingly.

- A declassified State Department cable released in October 2023 said the US intelligence community found evidence that Russian actors made a concerted effort to undermine faith in the voting process in at least nine countries between 2020 and 2022.[7]
- Taiwan earlier this year said it was documenting its experiences countering Chinese interference in its January election and would make its analysis public.[8]
- The Indian military backed an IO campaign in 2019 that sought to convince Kashmiris that they would be better off under Indian authority.[9]

State actors are just part of the story—domestic and non-state actors play a role in the IO landscape as well. Such actors could include journalists, influencers, political parties, or other individuals or groups focused on pushing certain perspectives to the public. Overlap between groups of actors is also common, as some domestic and nonstate actors often share viewpoints with state actors and

[3] https://apnews[.]com/article/argentina-fernandez-president-reelection-wont-run-31782993f581915f30f6106fb00f7fe7

[4] https://www.reuters[.]com/world/asia-pacific/indonesia-presidential-candidate-prabowo-picks-jokowis-son-running-mate-2023-10-22

[5] https://www.reuters[.]com/world/asia-pacific/indonesia-election-watchdog-summons-presidents-son-over-alleged-violation-2024-01-03

[6] https://cekfakta[.]com/focus/16012

[7] https://www.reuters[.]com/world/us/us-intelligence-report-alleging-russia-election-interference-shared-with-100-2023-10-20/

[8] https://www.reuters[.]com/world/asia-pacific/taiwan-will-publish-analysis-chinas-alleged-election-interference-post-vote-2024-01-04/

[9] https://www.washingtonpost[.]com/world/2023/09/26/india-facebook-propaganda-hate-speech/

knowingly or unknowingly propagate the same material. In some cases, these actors have also incited violence.

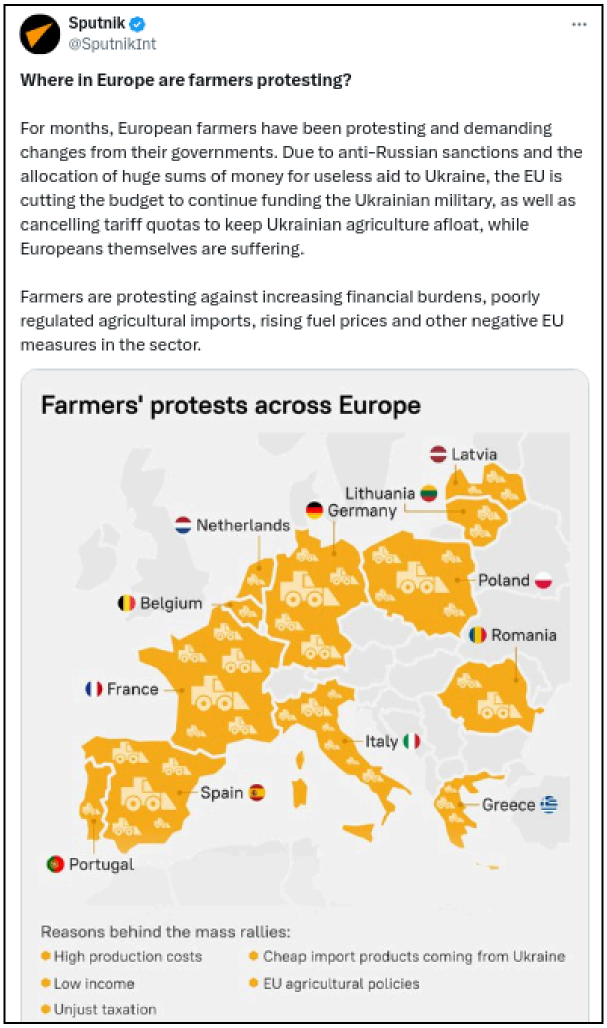
- In 2021, Nisos researchers identified a coordinated, inauthentic network of 317 Twitter accounts that aimed to discourage Honduran voters from supporting either of their two presidential candidates and to abstain from voting entirely.[10]
- The Telegram channel LexeData, which appears to be linked to the Turkish Kurdistan Workers' Party, collects and shares information on Turkish citizens and incites violence against individuals who insult or offend Kurds.[11]
- During the Colombian election in 2022, Nisos identified a Twitter disinformation campaign by Venezuelan organizations seeking to support then-presidential candidate and current Colombian President Gustavo Petro.[12]
- Some reporters from China's state-run media outlets have social media accounts where they cast themselves as influencers, posting content that counters Western perceptions, highlights positive stories about China, and amplifies Russian IO narratives.[13]

FROM OVERT TO COVERT AND EVERYTHING IN BETWEEN

IO campaigns usually employ both covert and overt means to proliferate their narratives, making them even more difficult to fully uncover. IO actors do not just spread true information that aligns with their chosen narratives or spread false information intentionally—they also coopt existing grassroots movements they have no role in and amplify their messages to sow division and further polarization.

IO propagators often seek to amplify narratives that suit their purposes, even if they originate from and are authentic to grassroots movements in a particular country. For example, in 2018 overt Russian state-sponsored accounts, including Sputnik and RT, amplified the yellow vests protests in France that started over rising prices and economic inequality.[14] In early January, Nisos observed Russian state-run media and pro-Russian outlets amplify stories surrounding the widespread farmers protests across the EU, likely to further polarize these issues ahead of the EU parliamentary elections in June 2024. France holds 79 seats in the European Parliament, the second largest share.

[10] https://www.nisos[.]com/library/hunduran-election-threat-investigation/
[11] https://t[.]me/c/1707322164/236
[12] https://www.nisos[.]com/blog/colombian-election-disinformation-venezuelan-leftists/
[13] https://apnews[.]com/article/china-tiktok-facebook-influencers-propaganda-81388bca676c560e02a1b493ea9d6760
[14] https://securingdemocracy[.]gmfus[.]org/incident/russian-state-media-including-rt-and-sputnik-amplify-and-heavily-promote-the-yellow-vest-protest-movement-in-france-on-social-media/



Sputnik
@SputnikInt

Where in Europe are farmers protesting?

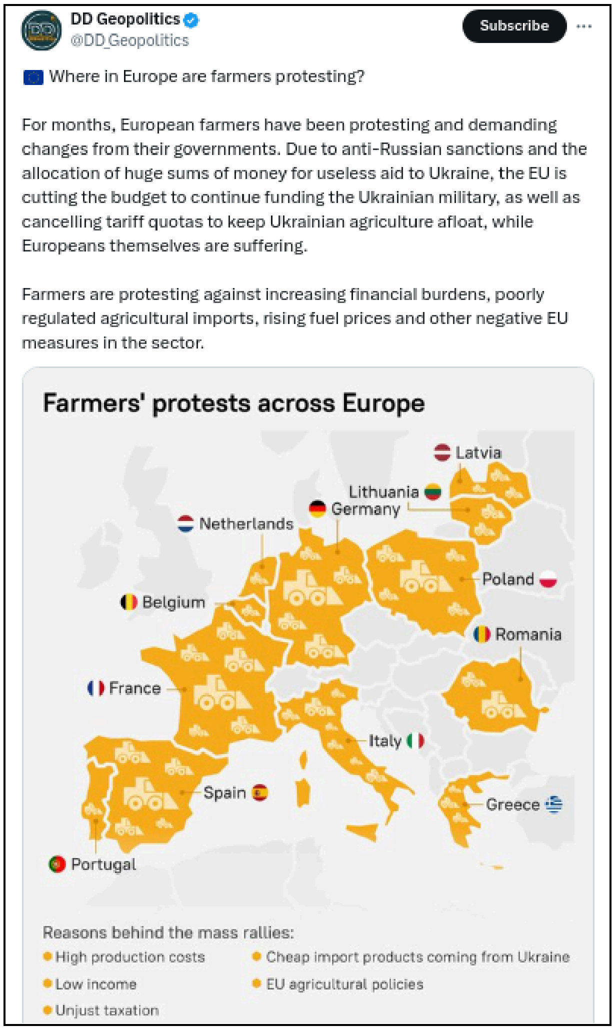
For months, European farmers have been protesting and demanding changes from their governments. Due to anti-Russian sanctions and the allocation of huge sums of money for useless aid to Ukraine, the EU is cutting the budget to continue funding the Ukrainian military, as well as cancelling tariff quotas to keep Ukrainian agriculture afloat, while Europeans themselves are suffering.

Farmers are protesting against increasing financial burdens, poorly regulated agricultural imports, rising fuel prices and other negative EU measures in the sector.

Farmers' protests across Europe

Reasons behind the mass rallies:

- High production costs
- Low income
- Unjust taxation
- Cheap import products coming from Ukraine
- EU agricultural policies



DD Geopolitics
@DD_Geopolitics

🇪🇺 Where in Europe are farmers protesting?

For months, European farmers have been protesting and demanding changes from their governments. Due to anti-Russian sanctions and the allocation of huge sums of money for useless aid to Ukraine, the EU is cutting the budget to continue funding the Ukrainian military, as well as cancelling tariff quotas to keep Ukrainian agriculture afloat, while Europeans themselves are suffering.

Farmers are protesting against increasing financial burdens, poorly regulated agricultural imports, rising fuel prices and other negative EU measures in the sector.

Farmers' protests across Europe

Reasons behind the mass rallies:

- High production costs
- Low income
- Unjust taxation
- Cheap import products coming from Ukraine
- EU agricultural policies

Graphic 1: Russian state-run media outlet Sputnik highlighted the farmers' protests in Europe on 13 February 2024 on its Twitter account; pro-Russian Twitter account and DD Geopolitics shared the same exact language and map the same date.[15] [16]

Actors involved in IO push their narratives through a variety of means, ranging from very visible, attributable, and overt activities to hidden, difficult-to-attribute, and covert measures. Potential sources of overt IO are those that have a known affiliation to an IO originator and include its official page, or the state actor's ministry of foreign affairs, or state-run media sources. Often we will see inauthentic actors boosting these overt accounts to further spread their message beyond the reach of its expected audience. These overt forms of IO typically propagate their preferred narratives regularly, even in off-election cycles, but ramp up their behavior and volume of content in the run-up to an election.

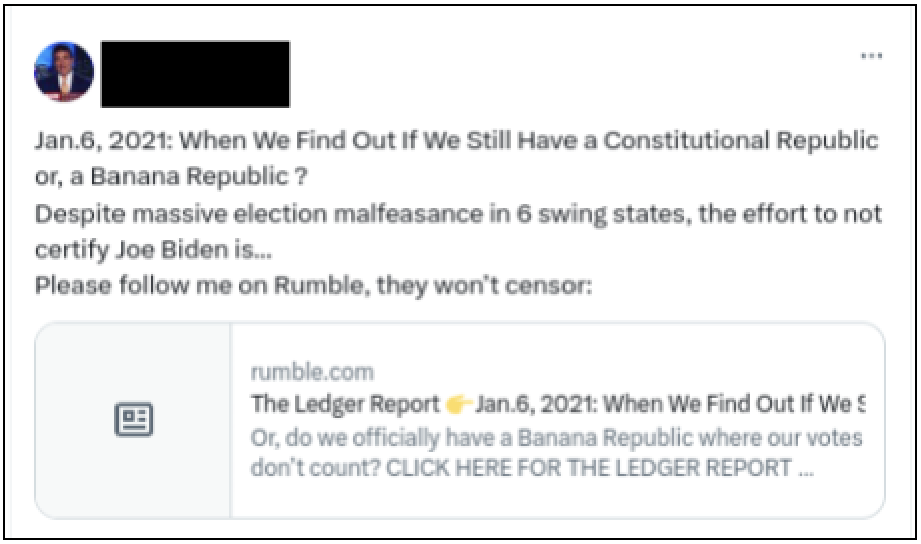
Covert IO involves a range of approaches that attempt to hide the hand of the IO originator, including using third-party services or digital media companies and leveraging bots or other inauthentic accounts

[15] https://twitter[.]com/SputnikInt/status/1757305313504469122
[16] https://twitter[.]com/DD_Geopolitics/status/1757500239207096691

to amplify the messaging across social media. Identifying covert actors and networks is more difficult and requires expertise and a deep understanding of how actors spread narratives on social media and the ways individual accounts interact. At Nisos, our analysts regularly surface new and existing tactics, techniques, and procedures that inauthentic accounts and other amplifiers of mis/dis/malinformation employ. Nisos' expertise in uncovering these activities goes beyond the superficial and includes more complex network analysis and identification of technical signatures. The more sophisticated the actor, the greater the chances their networks will require more work to disentangle and expose.

INFORMATION FLOW ON AND OFF PLATFORM

For trust and safety teams, identifying IO propagators, hashtags, and narratives on their own platforms is important—but equally important is having a sense of how those hashtags or narratives intersect with activity on other platforms. Broadening the scope of inquiry to multiple platforms offers a richer understanding of the IO ecosystem that can inform mitigation efforts. Users can link to content on platforms like Telegram, Gab, and Rumble that have few or no restrictions on content, enabling violative content to spread. For example, a Hamas-aligned group posted graphic images of their October 7 attacks on a Telegram channel; users subsequently shared the content widely across social media.[17] Nisos maintains cross-platform visibility and has experience tracking how these narratives move from one platform to the next. Our work to track IO, which can include closed group infiltration and monitoring, helps trust and safety teams better predict how such content might appear on and influence activity on their own platforms.



[redacted]

Jan.6, 2021: When We Find Out If We Still Have a Constitutional Republic or, a Banana Republic ?
Despite massive election malfeasance in 6 swing states, the effort to not certify Joe Biden is...
Please follow me on Rumble, they won't censor:

rumble.com
The Ledger Report 👉 Jan.6, 2021: When We Find Out If We S
Or, do we officially have a Banana Republic where our votes don't count? CLICK HERE FOR THE LEDGER REPORT ...

Graphic 2: An X (formerly Twitter) user directs viewers off-platform to an alternative social media site to view additional content.[18]

[17] https://www.wired.com/story/telegram-hamas-channels-deplatform/
[18] https://twitter[.]com/GrahamLedger/status/1344086018115309568

BROADER POLITICAL CONTEXT

Familiarity with the political context in which elections are occurring is key to seeing the nuance and assessing the intent behind IO campaigns. Venezuela is slated to hold elections on 28 July 2024,[19]but the winner of last October's opposition primaries, Maria Corina Machado, is still banned from running.[20] Journalists and activists have also been arrested, or in the case of officers working in the local UN human rights office, expelled from the country.[21] This is despite an agreement between representatives of Maduro and Venezuela's opposition to hold free and fair elections this year, which led Washington to provide oil and gas sector sanctions relief to Venezuela through General License 44.[22] The US government does not intend to renew the license on 18 April when it expires absent any progress on allowing presidential candidates to run in the elections.[23]

Efecto Cocuyo, which is part of C-Informa, a Venezuelan coalition of media and digital rights organizations against disinformation,[24] tracked narratives against the opposition primaries to the television program *Con el Mazo Dando*, run by Maduro representative Diosdado Cabello. A coordinated inauthentic network of social media accounts amplified the narratives and included the hashtags *MegaFraude*, *NiPorLasBuenasNiPorLasMalas*, and *AsiChillesOPataleesNoVas*—the last one specifically targeting Machado after she won the primaries. As part of this IO campaign, Cabello referenced Machado's ban from running to stress that no matter how much she "kicked or screamed'' (*asi chilles o patalees*) she would not be participating in the election (encapsulated in *no vas*; see graphic below).[25]

[19] https://www.nytimes[.]com/2024/03/05/world/americas/venezuela-maduro-election-date.html

[20]https://apnews[.]com/article/venezuela-opposition-candidate-ban-machado-maduro-548531e6db1dca250dc784f0dc2374c5

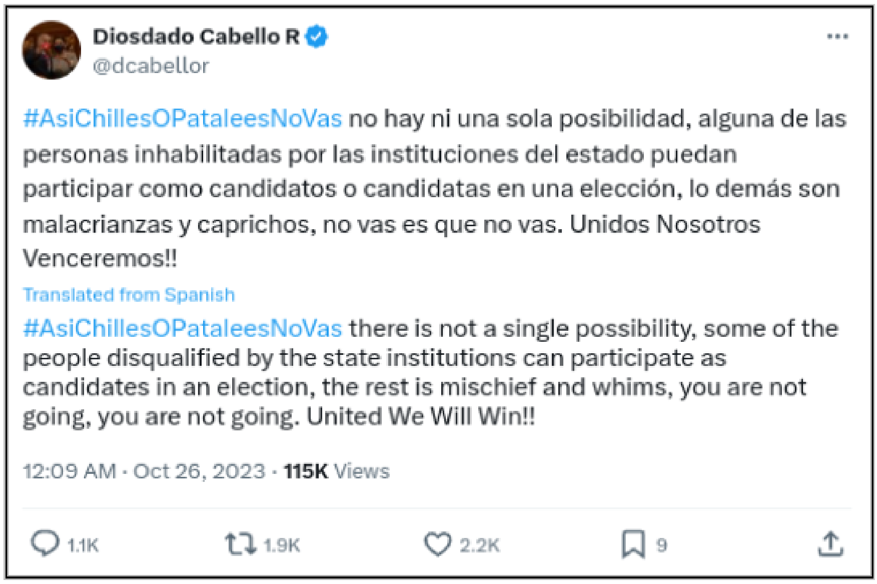
[21]https://www.washingtonpost[.]com/world/2024/02/15/venezuela-human-rights-rocio-san-miguel

[22]https://www.state[.]gov/venezuela-sanctions-actions-and-supporting-democracy

[23]https://www.state[.]gov/venezuela-sanctions-actions-and-supporting-democracy

[24]https://latamjournalismreview[.]org/es/articles/en-venezuela-crean-coalicion-informativa-para-dar-a-conocer-como-opera-la-desinformacion/

[25]https://efectococuyo[.]com/cocuyo-chequea/ciberalianzaaldescubierto-el-mazo-y-las-redes-anonimas-se-unen-para-desinformar/



Diosdado Cabello R
@dcabellor

#AsiChillesOPataleesNoVas no hay ni una sola posibilidad, alguna de las personas inhabilitadas por las instituciones del estado puedan participar como candidatos o candidatas en una elección, lo demás son malacrianzas y caprichos, no vas es que no vas. Unidos Nosotros Venceremos!!

Translated from Spanish

#AsiChillesOPataleesNoVas there is not a single possibility, some of the people disqualified by the state institutions can participate as candidates in an election, the rest is mischief and whims, you are not going, you are not going. United We Will Win!!

12:09 AM · Oct 26, 2023 · **115K** Views

Graphic 3: A tweet by Maduro representative Diosdado Cabello displaying a hashtag associated with an IO campaign targeting Venezuela's opposition.[26]

Nisos maintains a deep bench of analysts with geopolitical and open-source expertise that informs our investigations into IO and which trust and safety teams can leverage to complement their own in-house knowledge ahead of global elections.

[26] https://twitter[.]com/dcabellor/status/1717332659540492422

FINAL THOUGHTS

Nisos is here to help trust and safety teams feeling overwhelmed with tracking and responding to IO during a crowded election year. Unaddressed, IO circulates broadly, exposing online platforms to reputational damage and legal risks. We work with major platforms to help them investigate and respond to IO, acting as an embedded part of their teams to help mitigate risks to their platforms, user bases, and reputations.

- We lay the groundwork by looking at the information environment in a country well before an election and can monitor critical shifts in IO narratives as election day nears.
- We examine the range of actors involved in IO campaigns and map out CIB networks of sock puppet accounts, helping platforms stay ahead of the curve.
- In addition to covering the prominent and overt sources of IO, we uncover covert influence campaigns and inauthentic boosting of domestic issues.
- Our experience tracking, following, and anticipating the way information moves across social media networks, communications platforms, and other online forums and message boards enables us to identify IO narratives early and to provide clients with opportunities to remediate.
- Finally, our broad understanding of country-specific political context helps us quickly and efficiently triage developments, identify actors, and relay that information to our platform partners to enable rapid response and remediation.

About Nisos®

Nisos is The Managed Intelligence Company®. Our analyst-led intel investigations, assessments, and monitoring services empower your security, intelligence and trust and safety teams. We provide accurate, customized intelligence that guides your security and risk decisions – protecting your organization, assets, and people. Learn more at nisos.com.