SIPA | IGP Institute of Global Politics

Working Paper

Margot Fulde-Hardy

Foreign Information Manipulation and Interference (FIMI) Activities Targeting Elections (2014-2024):

Presenting a dataset, a methodology, and a codebook to guide future applications of structured frameworks enabling threat assessment

Abstract

In 2016, large-scale information operations on social media orchestrated by the Russian Internet Research Agency, a Kremlin-aligned troll farm, shook the US Presidential election, creating shockwaves of reckoning with the modern shapes of foreign interference. This event catalyzed new fields of study and practices, and since then many such campaigns targeting elections have been exposed around the world. *How prevalent and consistent are the tactics used throughout these campaigns? Have their methods changed or advanced over time? Since the first incident using generative AI to target elections in 2019, how has this trend evolved, particularly amid OpenAI's recent disclosure that a number of information operations used their services? And finally, can we identify trends by examining the frequency and volume of these disclosures over time, looking at the nature of the threat and on technology companies and public institutions' disclosures of these incidents?*

These questions are fundamental for the future of democracy, and yet remain extraordinarily difficult to tackle because researchers lack a unified view and analytical framework covering these incidents across the years.

Our work with this report and dataset aims to contribute to efforts among researchers and practitioners to develop cross-FIMI campaign analysis **through the systematic application of a common behavioral framework**. Drawing upon existing databases on FIMI campaigns from 2014 to 2024, it **tests** a methodology and a codebook on **a dataset related to elections, based on** a framework commonly used by public institutions to analyze online information operations–the DISARM Framework. This work, which bridges theory and practice, will move the needle forward and spur new ideas and research projects so policymakers can tackle this growing scourge of democracy, based on knowledge and understanding about the last 10 years of election related FIMI campaigns.

Motivations and objectives

Since the 2016 US elections, growing attention has been given to electoral influence and interference conducted through digital means. However, most of the analysis has been conducted at the national level, focusing on single domestic events[1] or single threat actors[2]. A lack of common taxonomy and common framework has prevented more systematic observations, characterizations and comparisons of information manipulation over time.

Over the past few years, documentation on information campaigns targeting elections has been assembled and disseminated by several types of sources, all illustrating these threats from their specific vantage point.

Meanwhile, a taxonomy and a common framework to describe the campaign have been consolidated, with the development of the DISARM framework and its progressive use in reports by the EU External Action Service[3] and the French agency dedicated to online foreign interference threats VIGINUM.[4] Additionally, the Hybrid Center of Excellence tested and validated the adoption of the DISARM framework.[5]

It is, however, worth noting that adoption of the DISARM framework has to date been confined to the public and institutional sector, with online platforms and security vendors continuing to use other types of framework (such as the ABC framework[6]) to structure their reporting efforts on foreign interference threats.

As 2024 fills up with elections throughout the world and marks a pivotal moment for democracy globally, there is an urgent need to **consider a common taxonomy and one or several common frameworks.** Doing so will enable the drawing of a comprehensive common picture, cross-country, cross-actors, cross-platforms and cross-audiences.

[1] See Recorded Future, "Malign influence during the 2022 US Midterm Elections" (13 October 2022), https://www.recordedfuture.com/blog/malign-influence-during-the-2022-us-midterm-elections-disinformation-misinformation; and ISD, "Elections 2022: The French information ecosystem put to the Test" (June 2022), https://www.isdglobal.org/isd-publications/elections-2022-the-french-information-ecosystem-put-to-the-test/.

[2] See Charon, Paul and Jeangène Vilmer, Jean Baptiste, "Chinese Influence Operations," IRSEM (2022), https://www.irsem.fr/report.html; and Graphika, "Secondary Infektion" (2020), https://secondaryinfektion.org.

[3] See EEAS, "1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence" (February 2023), https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.

[4] See SGDSN, "RRN: A Complex and Persistent Information Manipulation Campaign" (June 2023).

[5] See Newman, Hadley, "Foreign information manipulation and interference defense standards: Test for rapid adoption of the common language and framework 'DISARM,'" Hybrid CoE (November 2022).

[6] See François, Camille, "Actors, behaviors, content: A disinformation ABC" (2020), https://www.ivir.nl/publicaties/download/ABC_Framework_2019_Sept_2019.pdf.

This project aims to **contribute to the reflection on current existing taxonomy and framework by testing on a dataset related to FIMI campaigns in elections the systematic application of the DISARM framework.** A methodology explaining the development of the dataset, a codebook explaining the tagging of the campaign and a presentation of the results obtained after analysis of the dataset are provided.

Prior Efforts

The objective of developing a comprehensive global database of information influence campaigns is not new. In 2020, the Australian Strategic Policy Institute released the "Cyber-enabled foreign interference in elections and referendums" database, which reviewed both cyber and information campaigns targeting elections and referendums since the early 2010s. This report expanded the work of Cyber Policy Centre published in 2019: "Hacking democracies: cataloging cyber-enabled attacks on elections".

Incubated at the Harvard Berkman-Klein Center for Internet and Society, the "Disinfodex" project was "a database of publicly available information about disinformation campaigns," composed of "disclosures issued by major online platforms and accompanying reports from independent open source investigators."[7]

Operating on a similar scope but focused on the 2020 timeline, the "Interference 2020"[8] tracker by the Digital Forensics Research Lab of the Atlantic Council presented additional analysis on foreign interference campaigns targeting the US 2020 election, and reported and attributed by a wide range of sources (institutional, media, platforms).

In 2022, Jacob Shapiro, Diego Martin, and Julia Ilhardt introduced "the Online Political Influence Efforts database," which is comprised of cases of information campaigns beyond the elections scope and tackles not only FIMI but also domestic information manipulation and interference in political processes.

This work draws upon these databases to develop a database specifically dedicated to Foreign Information Manipulation and Interference (FIMI) in the context of elections and referendums. This database willingly excluses domestic information campaigns and cyber operations to narrow down on the specific object of FIMI. It focuses on FIMI to align with ongoing efforts at the European Union level to harmonize the scope and definition of these information campaigns.

The codebook which accompanies the database also draws upon the author's experience with the European External Action Service and VIGINUM practices regarding the integration of a systematic approach to describe information campaigns. The taxonomy chosen in this paper is taken from the EEAS and VIGINUM publications on campaigns and the integration of the DISARM Framework.

[7] See https://disinfodex.org/.

[8] See https://interference2020.org/.

Methodology

Composition of the dataset and terminology

The dataset is currently composed of 81 Foreign Information Manipulation and Interference campaigns targeting 58 electoral events from 2014 to 2024. It currently includes 23 threat actors and 18 different countries of origin. Each TTP observed is represented by a variable. The definition of a TTP and the reason to select it is described in the codebook.

An electoral event corresponds to an election or a poll in which citizens are invited to express their choice in a democratic context.

Foreign Information Manipulation and Interference (FIMI) is a pattern of behavior that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, and 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] Others have referred to the same incidents as “coordinated inauthentic behavior,” “information operations,” or “foreign-orchestrated disinformation campaigns”: the variation in terminology here, along with the differences between slightly overlapping concepts, is inherent to the difficulty of standardizing analyses on the issue.

A campaign is a series of actions perpetrated by one or more threat actor(s) pursuing specific objectives and carried out with the intent to deceive. It is composed of a combination of observables and TTPs.[10]

A country of origin is the state to which the threat actor is linked. Main states include Russia, China, Iran.

A threat actor is an individual or a group of individuals that has been politically or technically attributed to a state or non-state actor. For example, the dataset includes main state threat actors such as the IRA, Spamouflage, politically influential groups such as the Alt-right, and private companies such as Archimedes, UReputation, Estraterra, and STOIC.

Tactics, Techniques, and Procedures (TTPs): In the context of FIMI, “Tactics, Techniques, and Procedures” are patterns of behavior used by threat actors to manipulate the information environment with the intention to deceive.[11]

[9] EEAS, "Tackling Disinformation, Foreign Information Manipulation & Interference," https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

[10] See EEAS, "1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence" (February 2023), https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.

[11] See EEAS, "1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence" (February 2023), https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.

DISARM Framework: DISARM is the open-source, master framework that was constructed based on both historical and hypothetical TTPs.

2014 corresponds to the first known FIMI campaign in the context of an election.

2024 is the year when this dataset ends, but campaigns continue to appear and be documented.

Identifying and selecting the cases

The campaigns were identified through reviewing previous dataset[12] documenting FIMI campaigns from 2014 to 2021 and conducting complementary research in publicly documented campaigns by credible actors in order to cover the period ranging from 2021 to 2024.

The campaigns were selected based on the following three criteria:

- The campaign must have a foreign component, whether the country of origin or the threat actor, which is supported by evidence. This evidence can be found in administrative reports, academic research, companies' reports, platforms' reports, and/or news articles.
- There must be open-source allegations that the campaign aims to influence or interfere with the election. These allegations are reinforced by the fact that the campaign takes place during the election cycle.
- The campaign is limited to FIMI activities. Although there may be cyber components related to the same event, the campaign's focus appears to be primarily focused on shaping the information environment.

DISARM, a framework to compare tactics, techniques and procedures (TTPs) used in various elections

The DISARM framework, a matrix describing information manipulation campaigns, has been used to analyze these campaigns from the planning phase to the execution phase. This method borrows from cybersecurity concepts, notably that of the "kill chain,"[13] to help extract stable indicators defining each incident.

This matrix includes a series of Tactics, Techniques, and Procedures (TTPs), which have previously been observed in cases of information manipulation by foreign actors. This matrix was used following these guidelines:

[12] Hanson Fergus, O'Connor Sarah, Walker Mali, Courtois Luke, "Hacking democracies: Cataloguing cyber-enabled attacks on elections" (2019), https://www.acs.org.au/insightsandpublications/reports-publications/hacking-democracies.html.
Martin, D. A., Shapiro, J. N., & Ilhardt, J. G., "Introducing the Online Political Influence Efforts dataset" (10 November 2022), *Journal of Peace Research*, *60*(5), 868-876. https://doi.org/10.1177/00223433221092815.

[13] On the application of the "kill chain" concept to information operations, see Nimmo Ben, Hutchins Eric, "Phase-based tactical analysis of information operations," Carnegie Endowment, (March 16, 2023), https://carnegieendowment.org/research/2023/03/phase-based-tactical-analysis-of-online-operations?lang=en.

Tagging the TTPs

- Each report or article has been qualitatively analyzed by the author,
- Sentences referring to a TTP from the matrix were extracted using the DISARM Plug-in.
- The TTPs were reviewed according to the codebook to ensure coherence and consistency over time.

Analyzing the TTPs

- TTPs were ordered according to the different variables provided: target country, country of origin, threat actor, region, year, event.
- TTPs were compared through the 75 FIMI campaigns.

Initial research questions

- How would one structure and populate a database systematically covering FIMI targeting global elections?
- Does the DISARM framework provide a robust base to systematically tag campaigns conducted by multiple threat actors targeting different countries and in different languages?
- What are the most commonly used TTPs during elections?
- Do sets of TTPs and threat patterns emerge from analyses of the resulting database?
- What are the main trends regarding the evolution of TTPs over the years and what does it suggest about the potential of this methodology and the future of FIMI in elections?

Limits of the methodology

The tagging of TTPs is based on secondary data, which are the observations drawn by investigators. These observations are directly linked to the ability of investigators to observe these TTPs, which means their ability to access data, their ability to understand the data, and their ability to get political and economic support for reporting about their observations.

These conditions result in the following limitations:

- Reports are not homogeneous in terms of granularity of the observations. Some observations focus on strategy and dissemination tactics while others focus on the content and the targeted audience. This lack of conformity results in some FIMI campaigns not entirely described or some campaigns described with a particular micro or macro layer which can prevent cross-campaigns comparison.
- Reports are also not homogenous in terms of level of confidence to assess the origin of the threat actor behind the information manipulation activities. A known difficulty in this space can be to “extricate” the source of the campaign from the target of the operation: for instance, in the context of Russian sockpuppet accounts targeting Alt-right communities, perhaps resulting in a mix of actors

involved in a campaign. This heterogeneity of level of confidence can result in potential misattribution of TTPs to certain threat actors.[14]

- The DISARM Framework is an evolving framework, which needs further elaboration. Some TTPs have been updated while this dataset was being developed while some TTPs are still missing or not precise enough. The codebook attempts to palliate these limitations.

More collaborative work from others in the field, including platforms, security companies, researchers, fact-checkers, and government, will hopefully contribute to overcoming these limitations in the future, and this project seeks to contribute to this strand of effort:

- First, the methodology used, applying the DISARM Framework, allows us to precisely describe the information manipulation activities during elections. Precise descriptions of information campaigns can contribute to the harmonization of the reporting of investigators.
- Secondly, conducting interviews with investigators can contribute to ensuring that all the details of the investigation have been correctly understood.
- Thirdly, an update of the DISARM Framework and its review by the international community may support the development of a common comprehensive picture of threat attack patterns during elections.

[14] François, Camille, "Moving beyond Fears of the 'Russian Playbook.'" Lawfare (Sep. 15, 2020), available at https://www.lawfaremedia.org/article/moving-beyond-fears-russian-playbook.