RSIS COMMENTARY

21 August 2025

Social Listening Tools in Disinformation and Online Harms Analysis

Tan E-Reng

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Ponder the Improbable since 1996

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 178 – 21 August 2025

Social Listening Tools in Disinformation and Online Harms Analysis

By Tan E-Reng

SYNOPSIS

Social listening tools are a vital part of the disinformation and online harms researcher's toolkit, offering both depth and breadth in the insights they provide. However, there are inherent pitfalls that come with their use. This commentary elucidates what these pitfalls are and proposes steps to mitigate them.

COMMENTARY

Social listening tools, which are software applications that enable end-users to gather and analyse vast amounts of user-generated content propagated online on social media platforms, are a vital component of the toolkit for analysts who study disinformation and online harms. They help analysts to develop a clearer overall understanding of the disinformation and online harms landscape, and support investigations into ongoing information operations.

While these tools are undoubtedly essential for the researcher's toolkit, there are inherent pitfalls that may arise from their use, which could have negative repercussions for national security. This commentary aims to elucidate some of these pitfalls and offer recommendations to mitigate them.

Types of Social Listening Tools

The current range of software tools used to monitor online spaces for disinformation and harmful content consists of four main types: 1) free and/or open-source tools, 2) closed-source tools provided by social media platforms, 3) proprietary social listening tools developed by third-party companies, and 4) customised, bespoke tools tailor-made by research teams for specialised purposes.

Free and/or open-source tools

Free and/or open-source tools can include public databases and freely accessible, user-expandable tools, sometimes with user-friendly front-end interfaces to navigate these resources. OSINT (open-source intelligence) software tools such as SpiderFoot enable analysts to automate the collection and analysis of data about specific targets, as part of information reconnaissance efforts. They also include third-party applications and browser extensions like Twint and GetOldTweets, which allow investigators access to a wealth of valuable data for free.

Tools provided by social media platforms

Social media platforms may provide their own bespoke, proprietary tools that give users access to the analytics and metadata related to the content on these platforms. A notable example of this was the now-defunct CrowdTangle by Meta. CrowdTangle was a vital tool for academics, civic groups, and journalists to monitor viral posts and other content on Facebook in real-time, playing a key role in the investigation of disinformation and influence operations. The Atlantic Council's Digital Forensic Research Lab (DFRLab), for example, utilised CrowdTangle to provide insights for numerous studies on disinformation operations and influence campaigns worldwide.

Proprietary tools by third-party companies

Various proprietary third-party software tools for data collection, analysis, and processing are utilised in the study of disinformation and online harms. Prominent developers of these third-party tools include Meltwater, Cision, Brandwatch, Truescope, and Factiva, among others. These third-party software solutions enable researchers to analyse large amounts of user activity data across multiple social media platforms and websites, automating the process of aggregating massive amounts of user-generated textual and visual content propagated online.

Using built-in AI-driven sentiment analysis algorithms, analysts can generate insights into the overall emotional tone, personal valences, and ideological perspectives that characterise online users and groups on social media. In turn, analysts can determine, *en masse*, whether certain users or communities might be potential vectors for the conduct of malicious activities such as the propagation of hateful, harmful, or false content.

Custom Tools

Customised tools are developed by research teams and think tanks to perform specialised tasks for their specific research projects. These tools form an important part of the arsenal of research teams that specifically require social listening functionality for more fringe websites or social media services that fall beyond the scope and reach of existing social listening tools. These tools may not always be commercially available, but might allow limited access by request on a case-by-case basis. The various proprietary technologies developed by the Centre for Advanced Technologies in Online Safety (CATOS) in Singapore are examples.

Pitfalls and Caveats

As tools that are used for active monitoring and countering of online disinformation and other harms, any disruption to their functionality, efficacy, and operation could have ripple effects on the maintenance of national security.

Unfortunately, a common pitfall that affects the four types of social listening tools discussed above is that they are, to varying degrees, vulnerable to changes in the Application Programming Interfaces (APIs) of social media platforms that they trawl and monitor. Social media companies may make unexpected changes to their APIs that impair or disable the social listening tools that investigators rely upon.

For example, Twitter's API has historically been a valuable tool for OSINT researchers, enabling the development of various third-party applications and browser extensions such as the aforementioned Twint and GetOldTweets since it was made freely accessible. However, new restrictions and authentication requirements imposed on Twitter's API under Elon Musk's ownership have severely curtailed disinformation and online harms research on the platform (now renamed X). X, upon Musk's acquisition, announced that it would drop support for legacy versions of its API and discontinue free access, a move many say will negatively affect research into harmful content and disinformation on X, presumably by disrupting the functionality of these third-party tools.

In the case of proprietary tools, although private companies might ostensibly have more resources and greater financial and legal incentives to maintain their tools compared to OSINT tools, they might nevertheless still find themselves playing "catch-up" with the overall online landscape. Certain platforms might cease being "scrapable", i.e., capable of being salvaged or reused, by these third-party tools due to overhauls in their API. Additionally, some of these tools may not be able to perform certain potentially useful functions, such as trawling user comments, simply due to inherent technical limitations. In turn, the operational capabilities of research teams and analysts using these tools for their work might be adversely affected.

Managing Caveats and Risks

The common thread behind all the caveats and risks outlined above is that these tools could, for any reason, spontaneously cease to function as expected. To mitigate this, a policy of redundancy should be adopted. Research teams could ensure that multiple tools from different developers are used in parallel, and insights are drawn not from the singular output of any one tool, but rather aggregated and triangulated from all of them.

Complementing such a redundancy policy could be the conduct of periodic reviews of the tools used. Research teams could carry out routine risk-oriented assessments of their tools to determine if they can meet operational requirements, or if the third parties maintaining them show any signs, tacit or explicit, of undergoing unfavourable changes that could affect product functionality. Examples of such "signs" could include what was observed with X, as described above, where free access to the previously highly regarded API was curtailed and placed behind a paywall, leaving the future of tools relying on this API uncertain and therefore riskier to continue relying on.

It is undeniable that using social media monitoring tools, whether proprietary, free, or otherwise, will continue to be an essential and unavoidable part of studying disinformation and misinformation operations. However, no tool is ever entirely infallible, and various factors could cause them to become suddenly obsolete. Therefore, researchers using these tools must have sufficient awareness of the potential pitfalls associated with their use and how to manage them.

Tan E-Reng is a Research Analyst at the Centre of Excellence for National Security (CENS), within the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. E-Reng's current research interests encompass the diverse domains of cyber, online harms, disinformation and misinformation, and emerging technologies.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.