BABELSTREET

USE CASE

Leveraging Babel Street OSINT Tools to Investigate China's Global Strategy

In its attempt to fulfill the Chinese Dream of global supremacy, the People's Republic of China (PRC) has embarked on a series of military campaigns against its neighbors in the Pacific. It has waged disinformation campaigns against the United States. It has sought to steal intellectual property by infiltrating the supply chains of adversarial countries.

To better predict China's political, economic, and military maneuvers — and to plan and react accordingly — the United States Department of Defense and broader intelligence community need solutions for open-source intelligence (OSINT). OSINT is the practice of obtaining insight from publicly and commercially available information (PAI/CAI) to address specific intelligence priorities, requirements, or gaps.

Babel Street Products

To learn more about the Babel Street products discussed in this use case, visit:

- Babel Street Insights
- Babel Street Insights Synthesis
- Babel Street Secure Access
- Babel Street Raw Collections
- Babel Street Refined Information

The following scenarios illustrate how intelligence officers, analysts, and others can use the Babel Street Ecosystem of OSINT products to investigate China.

Scenario 1: Improving insight into Sabina Shoal tensions

Sabina Shoal is part of the Spratly Islands, a disputed South China Sea archipelago consisting of islands, islets, and more than 100 reefs. China, the Philippines, Malaysia, Taiwan, and Vietnam all assert ownership.[1] Sabina Shoal is strategically important because it sits near fisheries, oil deposits, natural gas deposits, and other resources.

Vying for control of the reef, the Philippines recently increased its naval presence there: reportedly docking a coast guard vessel within the reef's lagoon. China sees this as the Philippines' intended "long-term presence" on the reef, a presence Beijing views as violating its territorial sovereignty.[2]

In support of their own key intelligence requirements, analysts who want to learn more about Sabina Shoal may start with Babel Street Insights. Insights' user-friendly Boolean keyword search enables analysts to examine a huge array of documents for terms such as "Xianbin Reef" (China's name for Sabina Shoal) and "military" and "China" and "Philippines" and "sovereignty." (See Figure 1.) Reading the material returned, analysts will find new key words to add to their searches, further refining results. These terms may include "Declaration on the Conduct of Parties in the South China Sea," "Chinese maritime militia," and "Chinese coast guard."

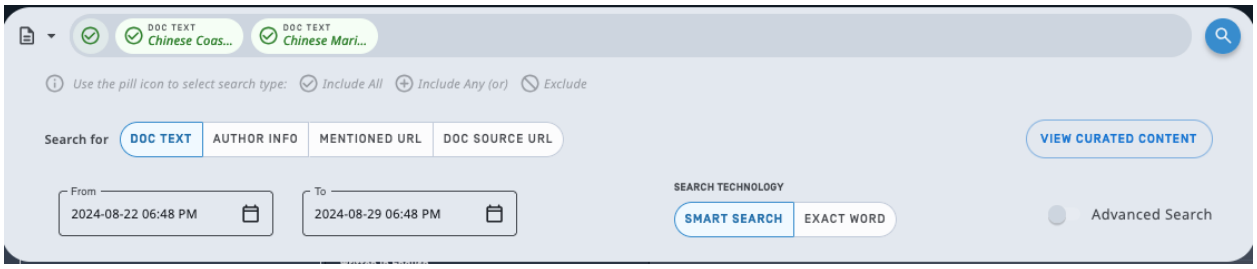

Figure 1: Insights' user-friendly interface makes Boolean searches easier

From this research, analysts will learn that multiple narratives surround Sabina Shoal. China and the Philippines view the situation very differently. In a county where professional reporting is tightly controlled by the Chinese Communist Party (CCP), analysts need only limit their Insights searches to Chinese media to uncover the PRC's view of Sabina Shoal incursions. Conversely, analysts can search Philippine media for the views espoused by journalists in that country.

Social media is as important a source of intelligence as traditional media. Analysts wishing to know what Philippine citizens think of the Sabina Shoal situation can use Babel Street Insights to search for Sabina Shoal-related posts on popular social media platforms.

Extracting insights from Chinese social media platforms is more challenging. The country's "Great Firewall" (a comprehensive technological system censoring and surveilling internet traffic) bans access from international users. Babel Street Insights' managed attribution capabilities help analysts penetrate the Great Firewall to access Chinese-grown platforms — including WeChat (known as Weixin in China), Weibo, and Douyin. The PRC monitors and censors anti-government sentiment posted on these sites, making it difficult for analysts to determine what the Chinese populace is thinking. However, since the PRC also employs operatives to flood these sites with posts supporting communist-party narratives, Chinese social media platforms can provide analysts with an in-depth understanding of what the Chinese government is telling its citizens.

Examining both Chinese and Filipino social media, analysts may find certain accounts particularly valuable. As they delve deeper, they may choose to narrow their searches to certain authors. Using Babel Street Insights, they can link one user to his or her screen names and associated posts across various social media platforms. They can also link screen names to real-world entities and find contact information for those people.

Intelligence officers and analysts can glean further insights through Babel Street Synthesis. For example, if they want to create a network of social media accounts covering the Sabina Shoal controversy, they need only to search for the keyword "Xianbin Reef" on Chinese sites. (Remember: In China, "Sabina Shoal" is referred to as "Xianbin Reef.") Synthesis develops an ecosystem of users employing this keyword — precisely pinpointing those who wield the most influence. Once these influencers are identified, Babel Street Synthesis empowers analysts to more deeply examine those users' online profiles, activities, and associates. In the case of the Sabina Shoal situation, these capabilities can help analysts identify Chinese sympathizers and operatives actively pushing that country's narrative.

No intelligence search is a one-and-done task. Rather, analysts and intelligence officers need continuously updated information. Babel Street's persistent search capability keeps search operations running regardless of whether someone is actively using it — recording updates and changes, then automatically appending this information to the search term. When analysts need an encapsulated view of their searches, Insights GPT summarizes pertinent results. (See Figure 2.) This capability can be particularly valuable for updating research. Analysts can ask Insights GPT to summarize any reported unrest around Sabina Shoal that has occurred since their last search.

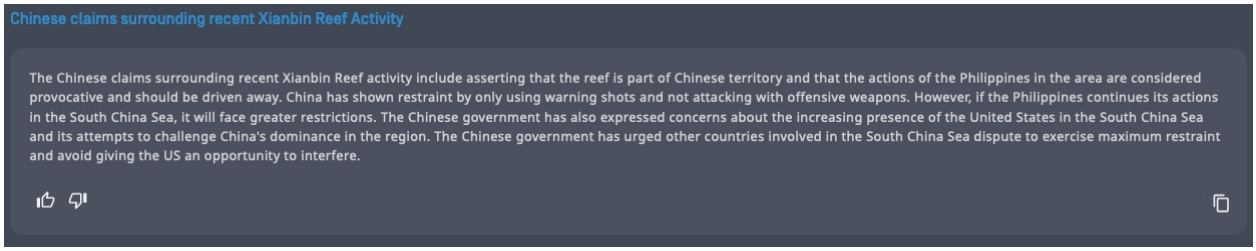

Figure 2: Insights GPT encapsulates pertinent search findings.

Scenario 2: Finding and countering disinformation

China often disseminates untrue or sensitive information to sow discord and unrest among citizens of adversary nations. For example, Chinese operatives used social media to claim that United States' tests of new weather weapons caused the devastating 2023 Maui wildfires.[3] AI-generated photographs accompanied many of these posts. More recently, posts on social media included sensitive, birds-eye images of the U.S.S. Ronald Reagan, a Nimitz-class aircraft carrier docked in Japan's Yokosuka Naval Base.[4] The security concerns raised by publication of these photos no doubt rattled those stationed on the carrier, along with their friends and family.

Disinformation tends to arise around divisive or upsetting topics. Analysts hunting disinformation originating from China may therefore begin their Insights work with searches of natural disasters, new tariffs, military skirmishes, or a host of other events. Through searches of both established and social media, analysts will begin to understand what the PRC is saying about a specific issue — comparing China's reporting on the subject against both hard facts and their own intelligence experience.

How does intelligence experience complement the search for hard facts in OSINT?

The Maui wildfires burned nearly 6,700 acres over 8 days — destroying more than 2,200 buildings and killing 102 people.[5] Analysts studying the event with Insights did not know from the outset that sparks from broken utility lines ignited the fires. (That determination was only reported in October, about two months after the conflagration.[6]) However, their own experience, training, and common sense told them there was no chance United States weather weapons caused the wildfires. The United States does not currently use weather weapons. And historically, the DoD has tested its weapons in vast, uninhabited swathes of the American desert — rather than on, say, a populated island that U.S. News & World Report lists as the sixth best vacation destination in the world.[7] Some posts on the disaster clearly contained disinformation.

Using Babel Street to examine false narratives surrounding Maui or similar situations, analysts can pinpoint sources of disinformation and begin to understand what China hopes to achieve by spreading untrue claims. To do this, they can access Chinese social media sites. When analysts uncover social media posts mentioning "weather weapons," they can use Insights' people search function to learn more about the posters' online activities and personas, and link those personas to real-life identities.

The process continues with Synthesis, through which analysts can identify networks of people mentioning "weather weapons" in their posts. Synthesis can then determine the top influencers among these social networks. From there, analysts can monitor content of posts by members of this network for disinformation, or for other red-flag themes or content.

Using similar techniques, analysts may also study how China deliberately misuses language to bolster its own narratives. On the eve of Communist China's 75th birthday, PRC President Xi Jinping reiterated his commitment to the "One China Policy," pledging to achieve "reunification" with Taiwan[8] as part of the Chinese Dream. This phrasing implies that modern-day China has some claim on Taiwan. It does not. The two nations have a complicated history of imperialism and annexation dating to the 1600s, but the current Chinese government — established by the Chinese Communist Party in 1949 after a civil war — has never governed Taiwan. Use of terms such as "reunification" (rather than more apt descriptors including "annexation" or "occupation") represents an intentional effort by an authoritarian regime to shape perceptions: to turn Chinese citizens and the broader world community to China's point of view. If China wins hearts and minds, the PRC's military incursions become more palatable.

Scenario 3: Protecting supply chains to prevent theft of intellectual property

In the United States, Presidential Executive Orders, national security strategies, defense strategies, and numerous legislative mandates attest to the criticality of protecting the supply chain. Supply chain threats emanating from China include competition for critical resources and exploitation of those resources, along with cyberattacks.

Increasingly, obscure Foreign Ownership, Control, or Influence of companies doing business for or in the United States is a significant concern. China's efforts at global domination include the use of cutting-edge technology, and sources ranging from the House Foreign Affairs Committee[9] to mainstream media outlets report that China often steals, rather than creates, technological intellectual property. A semiconductor manufacturer in Illinois found that a Chinese customer reverse engineered its products.[10] A Texas chemical manufacturer found Chinese clients using its proprietary technology.[11] The United States government is vulnerable to the theft of technological intellectual property — as are American corporations operating in the fields of artificial intelligence, satellite development, space exploration, nuclear energy, shipbuilding, and aviation.

Covertly inserting PRC-affiliated companies into the supply chain is one mechanism through which China effects these thefts. Chinese companies that seem to be innocuous may in fact have ties to the Chinese government or military. Information stolen may be used to bolster China's military operations.[12]

Clearly, the United States government and its vendors should screen suppliers and their ultimate beneficial owners against watchlists. But top-level screening isn't always enough. Thorough vetting of vendors is necessary to gain visibility across multiple tiers of a supply chain. Company A may receive an "all clear." But what about Company A's supplier, Company B? And Company B's supplier, Company C? Government agencies and vendors may unknowingly be working with suppliers that are only separated from sanctioned or "risk-indicated" entities by a few steps.

Babel Street Data can help analysts and intelligence officers vet vendors and protect supply chains. Analysts can use Babel Street Data to create a data collection strategy that answers questions specific to their own and vendors' supply chains. In doing so, they can produce their own watchlists of risk-indicated organizations — lists that go deeper than just naming ultimate beneficial owners. Once risk-indicated companies are identified, analysts can use Babel Street Insights and Synthesis to better understand these companies and determine whether their presence in a supply chain presents a risk to the United States.

Military incursions in contested waters, sophisticated misinformation/disinformation campaigns, and attempted supply chain dominance all result from China's pursuit of the expansionist Chinese Dream. These actions not only challenge international norms but also threaten the national security of the United States and the stability of the established global order. The ability to detect, understand, and counter these activities has therefore never been more vital. Babel Street empowers analysts with advanced solutions to monitor activity, identify emerging threats, illuminate false and biased narratives, and uncover hidden connections to inform actionable decisions.

End notes

1. CIA, "Explore All Countries — Spratly Islands," The World Factbook, September 2024, https://www.cia.gov/the-world-factbook/countries/spratly-islands/

2. Babel Street Insights, 2024

3. Sanger, David E. and Myers, Steven Lee, "China Sows Disinformation About Hawaii Fires Using New Techniques," The New York Times, September 2023, https://www.nytimes.com/2023/09/11/us/politics/china-disinformation-ai.html

4. Wilson, Alex and Kusumoto, Hana, "Navy probes apparent drone footage of USS Ronald Reagan posted on social media," Stars and Stripes, May 2024, https://www.stripes.com/branches/navy/2024-05-10/drone-footage-ronald-reagan-yokosuka-13813098.html

5. World Vision, "Maui wildfires: Facts, FAQs, and how to help," accessed November 2024, https://www.worldvision.org/disaster-relief-news-stories/maui-wildfires-facts-faqs-how-to-help#:~:text=The%20deadliest%20U.S.%20wildfire%20in,according%20to%20Maui%20County%20officials.

6. Alfonseca, Kiara and Sarnoff, Leah, "Broken power lines caused deadly Maui wildfire, new report shows," ABC News, October 2024, https://abcnews.go.com/US/broken-power-lines-caused-deadly-maui-wildfires-new/story?id=114423744#:~:text=%22The%20cause%20of%20the%20fire,had%20been%20two%20separate%20fires

7. Von Tersch, Elizabeth, "World's Best Places to Visit," U.S. News & World Report, August 2024, https://travel.usnews.com/rankings/worlds-best-vacations/

8. Gan, Nectar, "Xi vows 'reunification' with Taiwan on eve of Communist China's 75th birthday," CNN, October 2024, https://www.cnn.com/2024/10/01/china/china-xi-reunification-taiwan-national-day-intl-hnk/index.html

9. House Foreign Affairs Committee, "Egregious Cases of Chinese Theft of American Intellectual Property," accessed October 2024, https://foreignaffairs.house.gov/wp-content/uploads/2020/02/Egregious-Cases-of-Chinese-Theft-of-American-Intellectual-Property.pdf

10. Ibid

11. Ibid

12. Department of Defense, "DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021," October 2022, https://www.defense.gov/News/Releases/Release/article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/

Disclaimer: All names, companies, and incidents portrayed in this document are fictitious. No identification with actual persons (living or deceased), places, companies, and products are intended or should be inferred.