Use Case: Cybersecurity

Identify harmful cyber threats

The situation

The interconnectedness of critical systems and the sheer volume of sensitive information running through them have created cyber vulnerability and given rise to cyber threats worldwide. Russia, China, Iran, and North Korea are all using disruptive technologies to gain military advantage over their adversaries. Non-state actors such as terrorist groups or hackers also aim to inflict serious harm through cyber campaigns against nations and their citizens.

Cyberattacks are designed to maliciously disrupt the operations a nation's critical infrastructure, such as military computer systems or equipment, energy grids, and power stations. These attacks have huge impacts — ranging from causing financial damage to businesses or citizens, endangering lives, paralyzing a community, or exposing national security secrets.

Our PAI solution

Open source intelligence discerned from publicly available information (PAI) is highly effective in the detection of damaging cyber threats. PAI can enable a paradigm shift that allows teams to be predictive versus reactive when used as a first resource for continuous cyber threat intelligence in an operational, tactical, or strategic capacity.

Are there any indications or warnings in cyberspace that pose a threat to national security?

Babel Street empowers teams with actionable insights to identify harmful cyber threats from adversaries.

Babel Street's analytics platform offers an AI-enabled cross-lingual, persistent search of thousands of global and regional PAI sources in over 200 languages to rapidly discover and decipher insights on potential cyber threats from adversaries. Constant access to hyper-local news, the deep and dark web, message boards, blogs, social media, and public record information is essential to identify both hidden threats or those "hiding in plain sight." Machine learning algorithms offer insights that include identifying cyber trends and patterns to tracing extensive digital footprints — from the type of threat to the originating countries, hostile governments, or the other threat actors potentially involved in a broader network. All these insights are translatable into your native language in seconds and organized on a single pane of glass for analysis and action.

Mission impact

Cybersecurity is vital to the safety, stability, and economic viability of all nations and allies.

PAI DATA SOURCES	DATA STREAMS	FILTERS	KNOWLEDGE
• 50,000+ hyper local & global news sites • Billions of blogs & message boards • 50+ social media/ geographic specific sites • Public records • Watchlists • Commercial telemetry data (restrictions apply)	• Entity name variants • Executives • Domains • Geolocation • Relevant user handles • Emails • Specific news agencies • Specific influencers	• Temporal • Keywords • Exclusions • Intent • Geo vernacular • Language • Regular expressions	• Emerging threats from nations of interest/bad actors • POIs and GOIs • Indications & warnings • Data breaches • Hack & dump tactics • Evidence of cloaking • Source of misinformation