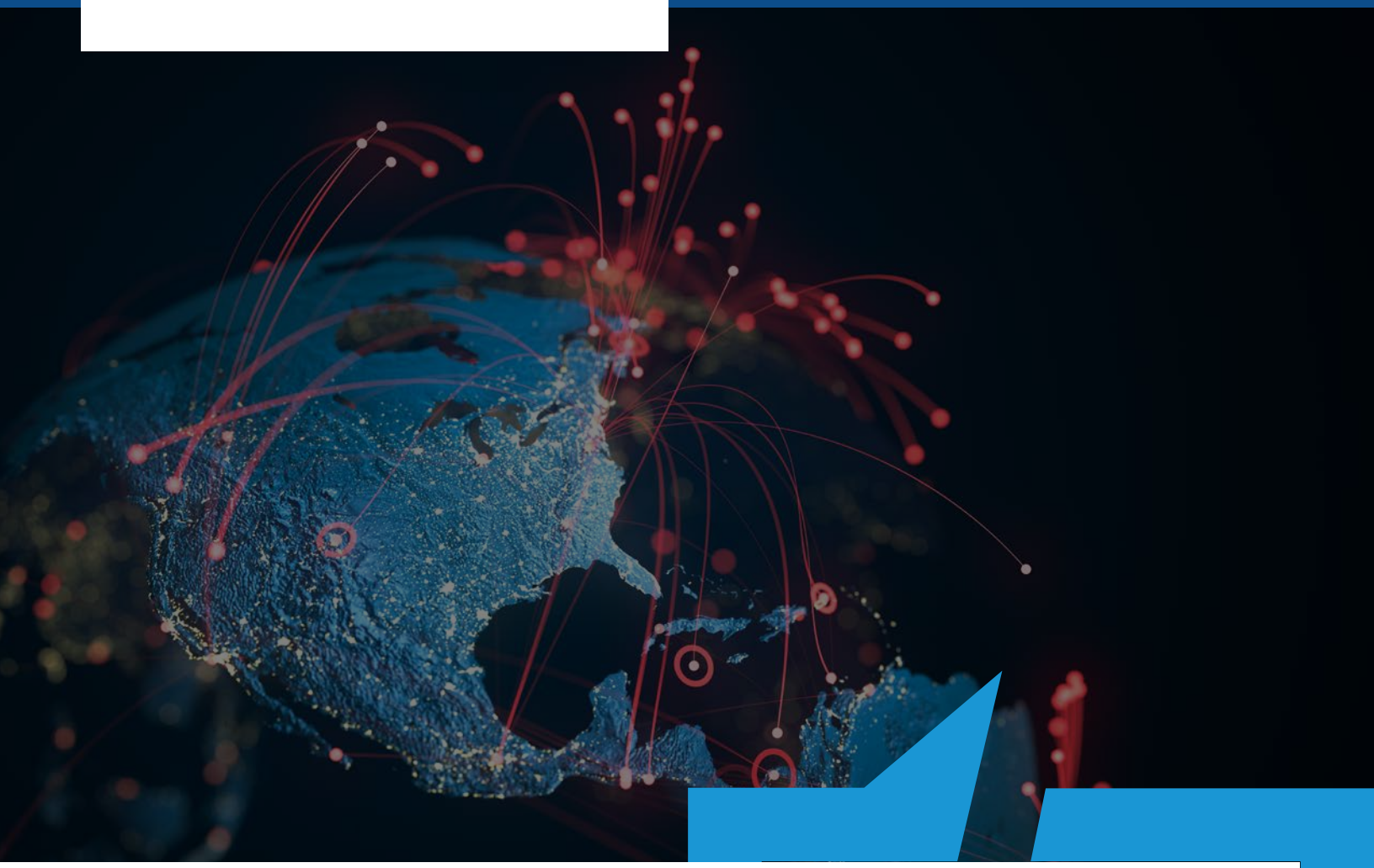
BABELSTREET



The Key to Countering Risk

How to:

- ✓ STAY AHEAD OF THREATS
- ✓ RESPOND FASTER
- ✓ POWER YOUR COMPETITIVE EDGE

Table of Contents

Introduction

From supply chain disruptions to localized disasters to criminal activities, the threats to public safety, national security and the free flow of commerce are constantly evolving. While risk is a factor in every activity, it's not always obvious just how much risk exists at a given time—or what can be done about it.

What if you could identify obstacles and threats early on, while fueling strategies to counter them and position your organization to be more secure and more competitive? By distilling the right data into actionable knowledge, you could track and analyze trends and activity that may indicate risk, allowing you to sidestep threats.

The problem is, the volume of available data grows exponentially every day—both the proprietary information you collect in the course of business and what's called Publicly Available Information (PAI).

PAI is the ever-expanding universe of news sources, websites, social media, blogs, chat rooms, multimedia, and public records.

PAI can provide insights to help you get ahead of threats, but only if you can find and analyze the parts that are meaningful to you.

This leads to two fundamental issues: first, how can you assess all of the relevant data—in any language, from any source—that can help you manage risk? Next, and most importantly, how can you turn that data into actionable information quickly enough to make a difference?

The answer meshes PAI with the transformative power of artificial intelligence, enabling you to **discover** relevant information, **decipher** meaningful insights and **empower** teams to take immediate action.

RISK CATEGORIES:

BUSINESS/COMMERCIAL

- Corporate IP theft
- Security (facilities, assets)
- KYC/KYV compliance
- Competitive intelligence
- Reputation management
- Business continuity
- Market sentiment

BOTH

- Supply chain interruptions
- Fraud/piracy
- Counterfeiting
- Event and venue threats
- Executive protection
- Insider threats
- Natural and human-made disasters

GOVERNMENT

- Government IP theft
- Official secrets exfiltration
- National security threats
- Terrorism (global or domestic)
- Human/drug trafficking
- Civil unrest
- Security (facilities, ports, transportation)
- Organized crime

The Domino Effect

When you look at the risks facing your organization, they often present both immediate disruption and, potentially, an even bigger impact down the line. Examples include:

CIVIL UNREST leads to interruptions in factory production, which then impacts downstream manufacturing processes

HURRICANES prevent produce from getting to market before spoiling, causing food insecurity across a region, affecting peoples' health and upending the local economy

A **TERRORIST ATTACK** on a sporting event causes people to avoid large public gatherings, impacting large and small businesses who depend on those events for their livelihoods

COUNTERFEIT PHARMACEUTICALS threaten public health as well as the reputation and business model of the manufacturer

The fact that any one of these scenarios is possible is enough to cause business and government leaders to wonder if their contingency plans are enough.

But before you can develop a response, you need a deeper understanding of the issues—and the sources of potential threats.

THIS REQUIRES A THREE STEP PROCESS

1. Discover

How to Know What You Don't Know

Before you can search for answers, you need to ask the right questions.

START WITH A BROAD VIEW.

Ask a high-level question, such as, **"What could disrupt this year's stakeholder conference?"** You can then identify possible factors that could impact this event, including:

- Venue security and crowd control
- Venue resources and utilities (electricity, water, HVAC, staffing)
- Known issues that impact the venue and the surrounding area (weather, communications interference, power and utilities concerns, access for responders, proximity to other problematic locations)
- Transportation for attendees and presenters (air travel, local travel, traffic control, construction)
- Hospitality (food service, hotel accommodations)
- VIP security and support

IDENTIFY POTENTIAL RISK FACTORS.

It's important to go further and **look at intentional disruptions** that are specific to your event and organization, including the potential for:

- Protests at the venue, guest accommodations and other places where attendees/presenters will gather
- Cyberattacks on organizer communications and presentation systems; venue communications and control systems; venue security systems; local infrastructure and services, including police, fire, and emergency response
- Physical attacks or threats against the venue (e.g., explosive devices, arson armed intruders)
- Physical attacks or threats against presenters, VIPs, or attendees

DEVELOP QUESTIONS THAT CAN BE ANSWERED.

Now you can ask a series of questions that drill down to **specific issues**:

- Have any attendees received threats?
- Does anyone have the intent to harm an attendee?
- Does anyone have the means to carry out that threat?
- Are persons of interest (POIs) physically able to reach the event or attendee?
- Have these POIs attempted or succeeded in carrying out past threats?

Knowing what to ask is just the first step. Finding the answers depends on knowing where to look—and having the tools to capture all the critical information.

PAI: A Primary Source

There are a lot of authoritative voices that will tell you "data is the answer." But raw data isn't information; instead, think of data as the building blocks of useful knowledge.

PAI is the ideal starting point. It's also the foundation of open source intelligence (OSINT), which is another way of saying "actionable information built on publicly accessible sources." **These sources include:**

NEWS, SOCIAL MEDIA AND THE OPEN WEB

These are the public-facing parts of "publicly available information"—the feeds, the sites, and the results of web searches. From social media posts to mainstream (and not so mainstream) media outlets, there are literally billions of sources online. Finding what you need—even if you don't know where to look—is essential to your risk analysis.

What many people think of as "the web" is just the tip of a very large iceberg. In reality, what you can find using typical search engines—mainstream sites such as Google, Bing, and Yahoo—is a small fraction of what's really available online. An overreliance on the main social media platforms can obscure the wealth of data that can support a search for threats.

While these sources can tell you a lot about trends and people, cutting-edge tools can reach more of what's posted to public channels—even more obscure ones. The results become even more powerful if you can search in native languages (more on that later).

FOCUS ON: IP THEFT / LEAKAGE

Every day new vulnerabilities are found in dozens of applications that touch your organization's most valuable intellectual property (IP), and every new application you add increases the risk. IP leaks might be due to a misconfigured cloud container, an untrustworthy former contractor or an outside hacker, but the result is the same: your IP is no longer in your control. Searching PAI for your IP can help you quickly take steps to secure it.

QUESTIONS TO ASK:

- What are the defining characteristics of your IP?
- Where might innocent or not-so-innocent discussions of this IP take place?
- Who appears to be in possession of your IP and where are they located?

PUBLIC RECORDS

The information that's available in public databases—from real estate transactions to required financial filings to international watchlists—can be incredibly useful for developing profiles of people of interest. But, since records are usually siloed by geography, agency, and department, it's always been difficult to capture complete details, especially if someone has relocated or goes by variations of their name (for example, "Amanda Thomas,"Amanda J. Thomas," and "Mandy Thomas").

With specialized tools, your team can eliminate these barriers to gain a more complete view. This allows them to quickly assemble a comprehensive profile from very little starting information, including names, aliases, phone numbers, addresses, email, web and social presences, relationships, job and educational background, and more. These elements can support deeper research into potential threats and persons of interest.

FOCUS ON: HACKING, CRIMINAL OR TERRORIST GROUPS

A key part of many investigations is tying hacker handles, noms de guerre, or nicknames back to actual people and groups. It takes just one member of a group to use sloppy operational security one time, then you can start to pierce the entire group's cloak of anonymity.

QUESTIONS TO ASK:

- Is there any overlap between the pseudonyms and real names in the suspected area?
- Were the same or similar email addresses used to register both dark and light personas?
- Is there domain or IP address overlap between dark and light actor activity?

DEEP AND DARK WEB

The stuff of movies and TV dramas, these are the fringe areas of the online universe. Think of the dark web as a series of unconnected message boards and online bazaars that can only be accessed if you know exactly where to go and have the passwords to get in. Users generally protect their identities with a Tor browser, which encrypts online activity and blocks trackers, allowing users to navigate the web anonymously.

The dark web makes up a tiny fraction of the deep web, but both are intentionally hidden from conventional search engines. The deep web is where protected information such as bank data, cloud data, email accounts, and parts of subscription services reside; the dark web is made up of encrypted online content that, all too often, is related to criminal or terrorist activity.

The ability to understand the true nature of threats against your people or organization depends on whether you can find, assess, and make use of all relevant information, especially the sensitive content that bad actors are trying to hide. Unfortunately, most organizations simply don't have the tools or proper guidance to locate it online.

FOCUS ON: COUNTERFEIT OR GRAY MARKET GOODS

From eroding profit margins to putting lives at risk, stopping counterfeit and gray market activity can feel like a frustrating game of whack-a-mole. However, armed with the right tools and an understanding of the defining characteristics to look for, the moment your opponents put up illegitimate goods for sale with any kind of digital footprint you can be there to put a stop to it.

QUESTIONS TO ASK:

- Are counterfeit/gray market goods being sold?
- Are there explicit dangers to the brand because of this activity?
- Are there genuine goods being sold in an unauthorized manner or counterfeit?
- What are the defining characteristics of these goods?
- Who is selling these goods and where?
- Who is supplying these goods and where are they coming from?

The Big Picture

Remember, it isn't just text and documents that can provide clues to risk. Graphics, images, photos, videos and even emojis can be sources of context and messages that can alert you to potential threats. Your search mechanisms should alert you to suspicious or troubling content in whatever form it takes.

Powering Up PAI with CAI and Proprietary Information

PAI can provide an incredible array of information, which can give you tremendous insight into the risks you face. But it can be enhanced even further by factoring in Commercially Available Information (CAI)—legally obtained and secured data from service providers—and your own proprietary data (the information gathered from business transactions and research performed within your organization). These additional sources can provide even greater depth to your analysis, and can spot relationships, behaviors and stressors which could indicate risk.

FOCUS ON: EXECUTIVE SECURITY

Protecting people from harm wherever they go—government officials, judges, diplomats, business leaders, and more—has become significantly more complicated in recent years. The ability for bad actors to communicate, plan and activate resources online has increased the risk level. At the same time, natural disasters and civil unrest can greatly increase risk at home or abroad. Identifying red flags early is essential to safeguarding your VIPs.

QUESTIONS TO ASK:

- Do any individuals or organizations have intent to do harm?
- Do these persons of interest have sufficient geographic proximity to do harm?
- Do they have the capability of doing harm?
- Who and where are these persons of interest?
- Is there a historic or chronic threat from natural causes for a specific location?

Automating the Search

It's just not possible for people—even a squadron of analysts and experts—to search all of the online places where relevant information lies in time for it to make a difference.

Automation—especially when powered by artificial intelligence (AI) and machine learning (ML)—is essential to this task. Properly tuned and applied, automation tools can provide expert-level knowledge to identify the relevant data from across billions of possible sources.

An alert that comes too late is the same as one that's never delivered at all.

But, there's more to it than speed. Along with enabling rapid search capabilities, an effective data-to-knowledge solution should be:

MULTI-LINGUAL.

Almost half of the web is created and maintained in languages other than English. It's imperative that your search and analysis incorporates native tongues, including dialects and slang; otherwise, nuance and local meaning could be lost. **Babel Street's Multi-Language Smart Search can deliver relevant results from across more than 200 languages. This not only accounts for the subtleties of local speech, it saves significant time.**

Nearly 50%
of the online web is created in languages **OTHER THAN ENGLISH**.

If you can't find data and insights from that massive section of the wired universe, **you're missing potentially crucial information.**

PERSISTENT.

What's true at any moment can change with every new piece of information. Persistent search keeps identifying as current data sources evolve (such as continuing discussions in online forums) and as new sources emerge (including new online users or new platforms). **Babel Street's solutions are designed to support always-on, vigilant searching to ensure you have the latest, most comprehensive information at your fingertips.**

CONCEPTUAL.

Context is essential to determining risk. So is being able to find relationships between seemingly disconnected data. By spotting the threads that link pieces of information (such as connecting screen names to real names or languages to locations), your search can yield a clearer picture of individuals, groups and actions. You can also spot keywords that are in close proximity to threatening language, or terms that are similar to—or "code words" for—threatening words or phrases. **Babel Street's AI engine is designed to quickly identify connections between disparate information and bring in new sources of relevant information, enabling a more comprehensive view of emerging situations.**

By itself, capturing enough relevant information is a formidable task. But making sense of this crucial information is the primary challenge.

2. Decipher
Making Connections, Uncovering Meaning

By asking the right questions, you can gather information that can help you identify threats and determine how likely they are to occur. But to get there, you need to zero-in on the data that matters most—and put it in context to determine the real-world impact.

Filtering Out the Noise

CAN THESE INDIVIDUALS, GROUPS OR EVENTS AFFECT THE PEOPLE, PLACES OR ASSETS YOU'RE TRYING TO PROTECT?

To get from relevant data to meaningful information, the next step is narrowing down your results to focus on what's most pressing. For example, geolocation allows you to account for where threat actors may be located, or where natural or human-generated disasters are occurring. A distant threat may change how you prioritize your response. Filtering for authors, keyword text, time and language can help you narrow the field.

Babel Street provides an array of filtering options that allow you to analyze your data from multiple angles—and clarify the results.

Analytics at AI Speed

Just as with search, automation can multiply your ability to find and understand the data you've captured. With well-designed AI capabilities, you can not only find specific information, but identify patterns and key entities (such as individual people, groups or organizations). You can also spot relationships across all of those inputs. All this can happen at machine speed, enabling you to highlight results that call for further investigation.

The AI powering Babel Street's platform delivers user-defined analysis based on multiple factors in near real-time. The system considers details that include geography, language, sentiment (more on that below), significance, reach, popularity, key influencers, concepts, named entities, trends and data types.

But there is another aspect that is critical to consider: **intent.**

Blowing Off Steam or Intending Harm?

Determining intent tells you if someone truly plans to take action—whether that means scheming to commit bank fraud or planning a consumer boycott. It's crucial to spot the differences between expressing anger or dissatisfaction and taking actual steps to harm others.

"Sentiment analysis" can identify how people are reacting to events—everything from an offensive Twitter post from a consumer brand to a military intervention halfway around the world. It can also help your analysts understand if someone is motivated to take some kind of action.

If that person also has the capacity to do harm, and is close enough to physically attempt it, you may choose to elevate your threat stance.

You may be launching a new product, managing a PR crisis or trying to protect a controversial figure. In each case, understanding what people feel as well as the evolving trends that are transforming public opinion can enable you to go from a reactive to a proactive stance. This level of detail allows you to get ahead of negative situations.

Babel Street delivers sentiment scoring and analysis in 50+ languages, providing nuanced insights into the views of people around the world. Our unique approach engages natural language processing, text analysis and computational linguistics—effectively quantifying something that is naturally subjective.

3. Empower
From Decision to Action

The search and analysis tools you choose are designed to speed up the process of finding and sorting through essential information—but humans still make the final decisions. Technology can enable more informed conclusions, supporting better informed responses to threats.

This knowledge also positions you to make long-term, data-driven choices that can keep you ahead of your competition. If you can see what's coming more clearly, you can take action sooner and stay ahead of the curve.

AI-powered Support for Human-powered Decisions

Risks to your people and operations are usually fast-evolving, with potentially global origins. Risk assessments and responses are frequently supported by an array of people who may be scattered across the globe, so real-time collaboration is a must. An ideal system provides:

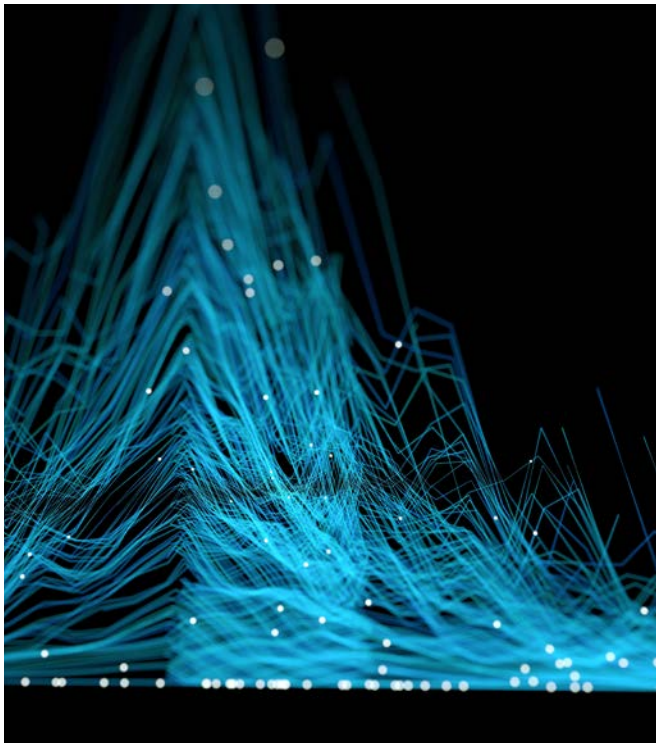
- A single platform with single log-in
- Comprehensive, customizable dashboards
- Document standardization
- Managed attribution
- Customizable visualization by geography, sentiment, volume, authors, languages or trends
- Collaboration within and across teams or organizations
- Powerful tagging features
- Accessibility for both remote and local users, including mobile applications
- Customizable options for specific compliance requirements

Babel Street's AI-powered approach enables teams to visualize the information in whatever way provides the greatest clarity, so they can focus on the knowledge they've acquired. With the insights Babel Street's suite of tools provides, teams can quickly move from reactive to proactive.

Where to Go From Here

The right tools ensure you can continuously capture, filter, sort and analyze PAI, CAI and your own proprietary data to identify actionable information—fast enough to make a difference.

Babel Street's comprehensive technology suite enables you to ask the right questions, collect and analyze relevant results and uncover deep insights to power your next moves. Our Multi-Language Smart Search breaks down language barriers, with a "thesaurus" that identifies words, phrases, slang, and subtext in more than 200 languages. This is much more than translation; this is understanding the context and meaning behind the words.



Staying Ahead of Risk

With fast, easy deployment and scalability, exceptional support and in-depth training, your teams will quickly get up-to-speed—and stay there, ready to identify and mitigate risks before they impact your essential operations.

This kind of knowledge and insight lets you do more than just defend against threats; it positions you to take advantage of changing situations, giving you a competitive edge that can open up new opportunities.

Asking the right questions. Understanding the value of the answers. Putting that knowledge into action. Babel Street gives you the unmatched ability to discover, decipher, and empower your teams to manage risk, whatever the source.

Learn how Babel Street can enable greater awareness of threats, giving you the knowledge—and the confidence—to act decisively.

BABELSTREET