The Honest Guide

to Insider Threat Detection

Prevent and Mitigate Data Leaks with PAI Monitoring

BABELSTREET

The digital revolution makes the leak of classified information easier and more pernicious than ever before and highlights the need for enhanced insider threat detection. Consider the recent case of a 21-year-old Air National Guard reservist who allegedly stole classified documents and posted them to his Discord channel.[1] From there, the documents discussing topics ranging from the Russian invasion of Ukraine to China's weapons program made their way to 4Chan and Twitter, where they lived for months before the Department of Defense became aware of their existence. Or contemplate the War Thunder leaks. Sensitive military information, including restricted technical manuals for the Apache Longbow helicopter and other weapons systems, has been shared on this multiplayer video game's forum 13 times.[2]

The modern leak landscape

Since the terrorist attacks of September 11, 2001, the USG has deliberately distributed sensitive and classified information much more broadly among approved agencies — improving insight but heightening the risk of purposeful or accidental disclosure. Wider distribution of classified information merges with the ubiquitously accessible nature of social media to simplify the dissemination of classified information. As illustrated by the reservist leak, classified documents may reside on the web for months before the DoD realizes it. If the site hosting these documents is based in an unfriendly nation, the DoD and USG may have no recourse for suppressing them.

Leaks, therefore, represent a significant vulnerability for the DoD, the broader intelligence community, and for military contractors — aircraft manufacturers, weapons manufacturers, shipbuilders, and technology providers among them. Understanding this, in 2011 President Barack Obama issued Executive Order 13587. [3] The order established an Insider Threat Task Force and required the development of minimum standards for a USG-wide insider threat policy. For the DoD, this unfunded mandate accompanies Directive 5240.16, which prescribed new Department of Defense Insider Threat Management Analysis Center (DITMAC) procedures to "prevent, deter, detect, and mitigate the threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources."[4]

By issuing the Order and Directive, the USG acknowledged that existing processes for detecting personnel likely to leak intelligence — and, by implication, for detecting the presence of leaked information — remained suboptimal.

A holistic, integrated risk management program (HIRM) can help the DoD better prevent and detect leaks and spills. Developing such a program is a challenging process. The EY Insider Threat Program Framework, for example, suggests defining a governance model, identifying critical data assets, determining better ways to protect those assets, then developing and implementing strategies for detecting, responding to, and recovering from threats.[5] These programs require buy-in from organizational leadership along with improved personnel communications and training. Any risk management program must be developed in alignment with personnel's legal right to privacy.

No technology can replace HIRMs, but technology is a vital component of these programs. New, AI-powered threat intelligence platforms offer leak prevention and detection capabilities that are better, faster, more thorough, and more complete than the limited, often home-grown systems currently used.

The rest of this e-book will discuss the benefits of these platforms.

Leak prevention

Certainly, preventing leaks — rather than quickly spotting and mitigating them — is the priority of the DoD and the broader intelligence community. It makes infinitely more sense to lock the horse in the barn than to track it down after it's galloped from the paddock.

But despite every cowboy's best effort, sometimes the horse escapes. Therefore, the DoD must invest in technology to both detect the type of insider threats that may lead to leaks, and to quickly spot leaks that do occur.

A complex mix of motivations — from self-aggrandizement to money, from self-protection to belief in citizens' right to know — spurs individuals to betray the trust placed in them by the DoD and other authorities. Leaks continue despite the DoD's best and evolving efforts. The background screenings and psychological assessments mandated by Trusted Workforce 2.0 haven't stopped leaks. Neither have the increasing implementation of zero-trust policies; improved surveillance and physical security at SCIFS and other facilities; and the prevalent use of user activity monitoring (UAM) software.

Too often, when the DoD thinks of UAM, it thinks about tracking keystrokes on an organization's computers or networks. This type of tracking alone is insufficient for spotting personnel likely to leak intelligence: it provides information only on the use of DoD-issued or authorized devices. Supplementing the information obtained from UAM systems with AI-powered OSINT technology that actively scans publicly available information (PAI) and commercially available information (CAI) is a better choice. It enables the DoD and others to examine personnel's online behavior regardless of the device employed.

Think of it this way. UAM software can alert command if an Army Sergeant who typically works from 0900–1700 Monday through Friday starts accessing military networks at 2200 on a Saturday. But searching PAI and CAI for insight into the Sergeant's online behavior — regardless of whether that behavior took place over military computers or personal devices — can tell the DoD much more.

Assume the sergeant has eight years' experience, earns slightly less than $44,000 annually,[6] and has no known history of family wealth. His posting pictures of lavish family vacations and expensive new cars may lead the DoD to suspect that the sergeant is obtaining cash through illicit activities — possibly from the sale of classified information.

Similarly, a PAI/CAI search may reveal a Navy Commander taking a family trip to Beijing. She has top secret clearance, but never alerted her facility security officer of her plans for foreign travel. Could she

The difference between risks and threats

What's a leak risk? How does it compare to a leak threat?

The military often uses the phrase "left of boom" to describe a series of events occurring before a notable incident. (Originally, the incident was an explosion, hence the use of the word "boom.") The further an event from a notable incident, the further "left of boom" that event is.

How does this concept apply to leak risks and leak threats?

Leak risks are situations inherent in human dealings with confidential data. They sit further to the left of boom, and present less danger of a leak, than threats do.

A service person mistakenly distributes a memo classified "top secret" to an audience with members who have only a "secret" clearance. This is a leak risk. If a member of this distribution list, someone with only "secret" clearance, is later found to be planning the purchase of a Ferrari 488 GTB (sticker price $249,150), he presents a leak threat.

For simplicity, this e-book uses the term leak "threat" throughout.

surreptitiously be communicating with Chinese authorities? Is an Air Force Master Sergeant regularly airing his worries about his parents, three sisters, and six nephews struggling in Ukraine? Could he feel that leaking classified information on the Russian invasion would help his family? He may be vulnerable to elicitation from foreign intelligence entities (FIEs). Other personnel may be vulnerable to FIE exploitation, recruitment, or blackmail — and therefore present a leak threat.

The DoD and other authorized organizations can obtain further insight through searches of regulated PAI, including credit headers. These types of searches can help the DoD find personnel who are financially vulnerable. A reservist on the brink of declaring bankruptcy or losing his home to foreclosure is facing terrible financial pressure. This pressure may lead him to consider selling classified information.

Detection and mitigation

No single product can stop all leaks. No piece of technology can stop a service person from stealing paper documents, scanning them on his cell phone, and posting them. The DoD and broader intelligence community, therefore, need to quickly, efficiently, and discretely spot leaks wherever and whenever they appear — on social media, elsewhere on the surface web, or on the deep- or dark web.

The process starts with cutting-edge social media monitoring. AI-powered PAI/CAI platforms can scan social media sites and message boards worldwide to detect words and phrases associated with leaks of classified or sensitive information, and automatically alert DoD insider threat analysts, insider risk analysts, and other security personnel.

The best of these platforms also scour hard-to-access sites on the deep and dark web where sensitive and classified information may be offered for sale. These capabilities can quickly alert the DoD to suspected leaks, enabling the department to begin mitigation efforts more quickly.

Combating spills

Classified data is spilled — unintentionally leaked — all the time. For example:

- Classified information is transferred via the Internet, rather than through the military's designated network for classified intel.
- Retroactive classification leaves information that was legitimately shared three years ago now labeled "top secret."[7]
- An aerospace engineer working with a military contractor enthusiastically and unthinkingly writes a LinkedIn post about the exciting new military aircraft he's helping to design.

According to the Ponemon Institute, non-malicious actions account for 55% of all insider risks.[8] The same PAI/CAI platforms that help detect leaks can be deployed to detect and mitigate spills.

Averting the damage

Today's digital landscape compounds the damage leaks cause. It can make certain countermeasures — judicial relief, for example — ineffective or unavailable. Therefore, preventing and quickly detecting leaks has grown increasingly vital to national security.

If leaked information appears on a website based in the United States, the Department of Justice may obtain a court order to suppress it. If the hosting site is based in an allied country, diplomatic pressures can be brought to bear. However, malefactors can quickly copy, screen capture or otherwise duplicate leaked intelligence, then repost it elsewhere. While new injunctions can be obtained and new appeals made, USG officials may feel as if they're playing a game of whack-a-mole: deleting classified information from one site, only to see it pop up on another.

The situation worsens when classified information appears on web sites hosted by unfriendly nations. How would the Russian government respond to requests to remove classified intelligence from VKontakte? How helpful would the Chinese government be removing classified information from WeChat?

In a time of limited countermeasures, the DoD needs PAI/CAI monitoring software to prevent leaks, detect them, and mitigate their damage. Otherwise, leaked intelligence on military strategies, tactics, operations, and procedures jeopardizes national security and threatens the lives of military personnel and intelligence operatives. Other repercussions include:

- **Cost.** Combating leaks is expensive. At the time of the Wikileaks incident, Army Gen. Martin Dempsey, then chairman of the Joint Chiefs of Staff, estimated that the USG would need to spend billions to mitigate the damage done by the leak of that classified intelligence.[9]
- **Reputational damage.** Discussing the Air National Guard reservist leak, Rep. James A. Himes, a member of the House Select Committee on Intelligence, said, "It is almost inconceivable that this particular individual A) had access to the information and B) … was able to print this stuff out and take it away and photograph it. And then finally, in a world of very advanced technology, that apparently this stuff could live on the Internet and various chat rooms and be viewed by people quite possibly for weeks or months before the Department of Defense became aware of it …"[10] Himes was not alone in this sentiment. Rather, media reports quoted numerous officials wondering how military security could be so lax — damaging the reputation of the defense and intelligence communities.
- **Marred international relationships.** Wikileaks data indicated that the NSA had monitored phone conversations of French leaders, along with conversations of Germany's then-chancellor Angela Merkel.[11] These revelations marred the United States' relationships with its allies. In wake of the reservist leak, the United States' Five Eyes partners called for "more vigilance around security." Clearly, leaks can damage relationships between the United States and its allies.

Babel Street Insights: how it works

The Babel Street Insights platform can help the DoD and other agencies better prevent and detect leaks — providing AI-powered insights that other PAI/CAI monitoring platforms simply can't.

Babel Street Insights rapidly and persistently scans vast amounts of PAI and CAI posted on all levels of the Internet. These searches can target the online activities of personnel who may leak intelligence, and continuously scan for data already leaked. The continuous nature of Babel Street searches is significant: Delays in detecting leaks delay mitigation of the damage they cause.

Social media monitoring is a significant aspect of this process. Babel Street Insights scans dozens of social media sites worldwide — including Russia's VKontakte and China's WeChat — for keywords associated with leaked information, and for posts indicative of someone potentially leaking information. (The Navy Commander touring Beijing, for example.) It also scours real-time interactions generated on more than 30 million message boards, including Discord, 4-Chan, 8-Chan, Baidu Tieba, and Tianya Club. Once Babel Street Insights detects a suspected leaker or leak, it automatically alerts insider threat analysts and managers and other security personnel.

But Babel Street Insights searches deeper than the surface web and easily accessible social media sites. The platform also scours hard-to-access sites on the deep and dark web where classified information may be posted or offered for sale. These sites may be published in an array of languages: Babel Street Insights accommodates roughly 200 of them. Working with Babel Street, the DoD and other authorized organizations can achieve further insight through regulated PAI, including credit headers. Geolocation and telemetry data is also available to qualifying government organizations.

Finally, Babel Street provides insight not just on the messages posted, but on the handles employed by those doing the posting. This helps the DoD to learn more about the real people behind the leaks. Babel Street further coalesces screen names into the single entity. Using Babel Street, DoD investigators can learn, for example, that DadJokeMaven487, PunsRMyLife837, and NoSuchThingAsABadJoke62 all coalesce to PFC John Smith* of New York, NY.

Babel Street Insights rapidly and persistently scans vast amounts of PAI and CAI posted on all levels of the Internet.

Capabilities tailored to the DoD

Babel Street is uniquely qualified to help the DoD prevent and detect leaks. While Babel Street Insights operates in the open source/unclassified space, many of our employees are former military, IC, and government professionals with USG clearances. The expertise of these professionals helps us tailor our products and services to meet the specific needs of the DoD, broader intelligence community, and related organizations. Consider the following capabilities.

Custom searching

Everyday words and phrases can often indicate an intelligence leak. But these everyday words and phrases can also indicate … nothing. Our filters cut through data noise to return only information relevant to DoD searches.

Suppose you want to search for leaked documents known to have been designated "top secret." Online, people regularly use the phrase "top secret." A search for "top[space]secret" will return a vast array of irrelevant posts. You don't want a PAI/CAI system that alerts to "Top Secret: Surprise Party for Jenny's 40th" because analysts and examiners should not waste time reviewing those types of posts. However, party planners very rarely follow DoD labeling conventions. Specifically, they don't use labels such as "top secret\\". Nor do they list "classified on" dates, "declassified on" dates, and "classified by …" lines. Babel Street understands this, and we know how to search for pertinent phraseology.

Detecting cross-domain violations

Cross-domain violations are common within the DoD. A "top secret" document stored on the Joint Worldwide Intelligence Communication System may also contain unclassified information which the DoD wants to share more broadly. But the entire document — including "top secret" passages — is mistakenly posted on the unclassified NIPRNet. Babel Street capabilities can help the DoD spot — and therefore mitigate — these cross-domain violations.

Coordinating search efforts

Currently, the agency with original classification authority assumes responsibility for tracking and mitigating its own intelligence leaks and spills. As the original classification authority for signal intelligence, the NSA assumes responsibility for signal intelligence leaks. The National Geospatial Intelligence Agency must track down and mitigate any leaked geospatial intelligence.

This makes sense. But what happens when different services collaborate? The United States Army, Navy, Air Force, and Marines may work in concert to protect Nation X from invasion by Nation Y.

Each service should be scanning the Internet for evidence that a component of the plan for which it had original classification authority has been leaked. Unfortunately, this often fails to happen. Deploying Babel Street Insights in all pertinent agencies can help the DoD coordinate efforts to track down leaks, spills, or other compromised information.

Persistent search of your choice of data

Unlike the sporadic, scheduled checks performed by other platforms, Babel Street Insights identifies and alerts analysts and investigators to leaks and leak threats continuously, as they emerge. This is accomplished via Babel Street Insights' persistent search — a technology that keeps a search operation running regardless of whether someone is monitoring it. Persistent search records updates and changes, automatically appending this information to the search term, and alerting investigators as necessary.

Babel Street Insights conducts persistent searches of data sources most germane to its clients. We also take input from clients on which additional data sources to include in our data lake for search. This capability empowers the DoD to choose the data sources most important to its mission.

Data collection aligned with DoD protocols

Leaked, spilled, or otherwise compromised information remains sensitive or classified even when it's posted "in the wild." Government agencies, therefore, are often reticent to collect sensitive and classified information, and to retain it in their organic systems. (In fact, intentionally collecting and retaining this type of information requires that the collector has both the mission and authority to do so.) Collection procedures can be established to isolate collected classified or sensitive information so as not to compromise NIPR systems and networks. This process entails essentially "sandboxing" the data collected. Babel Street can work with government agencies and the Under Secretary for Defense for Intelligence and Security to support this process.

Improved intelligence

The United States isn't the only nation to suffer leaks, spills, and other instances of compromised information. Babel Street capabilities can quickly detect leaked classified information from Russia, China, North Korea, Iran, and other unfriendly countries — potentially giving the DoD and the broader intelligence community new insight into the political and military machinations of those countries. Unfriendly countries' leaks can become the USG's intelligence gains.

Leaks are a known security vulnerability for the DoD, the wider intelligence community, and for organizations contracting with the military. Babel Street Insights provides the AI-powered searches of PAI and CAI vital to securing information and detecting leaks. We are a trusted technology partner for the USG: More than 84 percent of United States national security agencies count on Babel Street. They use our technology for more than 500 million watchlist checks daily, among other tasks. National security agencies turn to us for their high-stakes identity and risk operations because we provide fast, unmatched insight; proactive risk identification; and always-on searches. In providing these capabilities, Babel Street Insights also helps close the Risk-Confidence Gap — the widening divide between the escalating volume and variety of data that must be examined to prevent and spot leaks, and the resources organizations have available to monitor that data.

Babel Street is uniquely qualified to help the DoD prevent and detect leaks.

Endnotes

1. "Air National Guardsman Indicted for Unlawful Disclosure of Classified National Defense Information," U.S. Department of Justice Office of Public Affairs, June 2023, https://www.justice.gov/opa/pr/air-national-guardsman-indicted-unlawful-disclosure-classified-national-defense-information

2. Schogol, Jeff, "For 13th time, sensitive military information leaked on 'War Thunder'" Task and Purpose, September 2023, https://taskandpurpose.com/news/us-military-sensitive-info-war-thunder-leak/

3. DCPD-201100732 - Executive Order 13587-Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, GovInfo, https://www.govinfo.gov/app/details/DCPD-201100732

4. United States Department of Defense, "Directive Number 5240.16," August 2012, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/524026p.pdf

5. EY, "Managing insider threat: A holistic approach to dealing with risk from within," accessed September 2023, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/EY-managing-insider-threat.pdf

6. U.S. Army, "Earn more than a paycheck," accessed September 2023, https://www.goarmy.com/benefits/while-you-serve/money-pay.html#full-time-pay-charts

7. Abel, Jonathan, "Do You Have to Keep the Government's Secrets?: Retroactively Classified Documents, the First Amendment, and the Power To Make Secrets Out of the Public Record," Stanford Constitutional Law Center, March 2015, https://law.stanford.edu/publications/do-you-have-to-keep-the-governments-secrets-retroactively-classified-documents-the-first-amendment-and-the-power-to-make-secrets-out-of-the-public-record/#:~:text=Retroactive%20classification%20means%20the%20government,elsewhere%20in%20the%20public%20domain

8. Ponemon Institute/DTEX, "Cost of Insider Risks: Global Report 2023," accessed September 2023, https://www2.dtexsystems.com/insider-risk-investigations-report-2023?Last_Touch_Campaign_ID=7013a000002hmSr&Last_Touch_Campaign_Status=Clicked&utm_source=google&utm_medium=cpc&utm_campaign=na_search_insider_threat&utm_keyword=insider%20threat&gad=1&gclid=EAIaIQobChMIw9r7msu-gQMVie7ICh22IAdZ-EAAYASAAEgIZV_D_BwE

9. NBC News, Snowden Leaks Could Cost Military Billions: Pentagon, March 2014, https://www.nbcnews.com/news/investigations/snowden-leaks-could-cost-military-billions-pentagon-n46426

10. Sonnenfeld, Jeffrey, et al, "The Discord Leak Has Shown Us Smart Ways to Fix Our Military Intelligence System," Time, April 2023, https://time.com/6272509/discord-leak-fix-military-intelligence-system/

11. Ryan, Missy et al, "Allies troubled by document leak, but need U.S. spying capabilities," The Washington Post, April 2023, https://www.washingtonpost.com/national-security/2023/04/14/us-intelligence-leak-allies/

Babel Street. Unlock the most insights that matter.

Babel Street is the trusted technology partner for the world's most advanced identity intelligence and risk operations. The Babel Street Insights platform delivers advanced AI and data analytics solutions to close the Risk-Confidence Gap.

Babel Street provides unmatched, analysis-ready data regardless of language, proactive risk identification, 360-degree insights, high-speed automation, and seamless integration into existing systems. We empower government and commercial organizations to transform high-stakes identity and risk operations into a strategic advantage.

Learn more at **babelstreet.com**

* Some 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.

BABELSTREET