Echosec™
SYSTEMS LTD.

# How Real-time Social Data is Transforming National Security

# In the face of national security threats, organizations need to stay prepared and make prompt, informed decisions to protect assets and potentially save lives.

Open-source intelligence has become valuable for driving these decisions. A comprehensive all source intelligence toolkit including web and online discussion monitoring software can save organizations millions, uphold national security, and retain public trust. As online platforms evolve, critical information can be easily overlooked if security teams and intelligence agencies aren't looking beyond standard sources.

Real-time data, particularly from fringe and international sources, can play a valuable role in a variety of use cases:

## COUNTER-TERRORISM AND EXTREMISM

Jihadist groups like the Islamic State and Al-Qaeda are no longer solely responsible for the threat of terrorism and extremism. Domestic extremist movements based on conspiracy theories, right-wing ideology, and discriminatory worldviews now also pose serious national security threats. Public online spaces are leveraged similarly for both extremist types, playing a huge role in spreading propaganda, recruitment, financing, and sometimes planning. OSINT data helps governments understand how extremist groups operate so they can then predict public safety risks and protect citizens and assets from domestic and global terrorism.

Fringe social networks and deep web sites have historically been used by perpetrators of violent crimes to make announcements and discuss plans. Following such events, like-minded users turn to sites like 8kun, 4Chan, Telegram, and Gab to express their support in these communities within groups and boards.

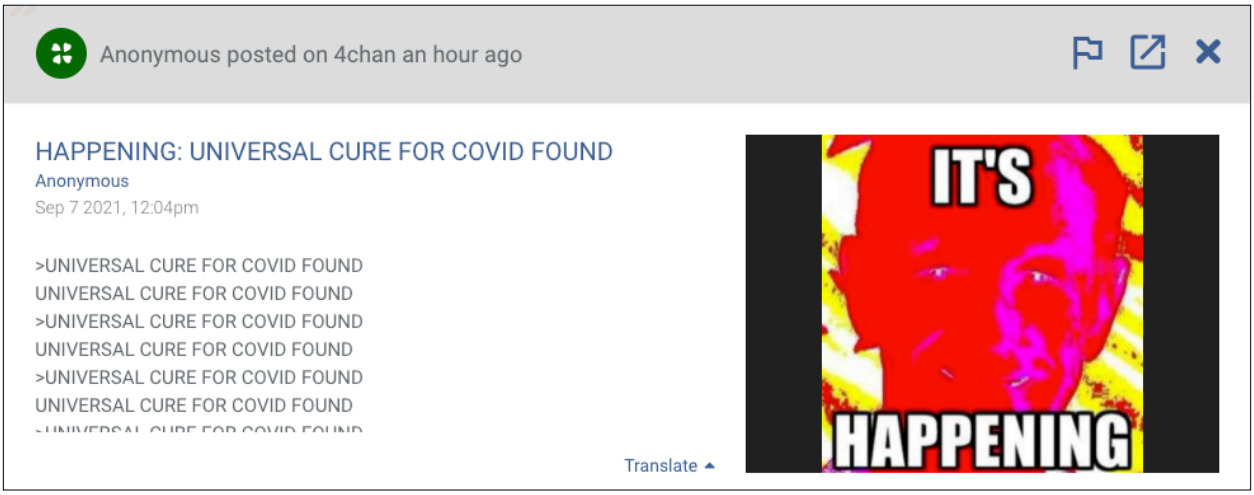
## DISINFORMATION MONITORING

National security threats have expanded to include online influence campaigns, which can compromise democratic processes and lead to real-world security risks. **Disinformation** (which is engineered to deliberately deceive) and **misinformation** (false information that is not necessarily spread with malicious intent) is widely prevalent online. Monitoring online spaces is crucial for tracking disinformation campaigns so governments can mitigate their impact and keep the public safer and more informed.

Disinformation can take the form of:

- Impersonations of corporate or personal social media accounts
- The spread of disinformation or 'fake news' about a brand, individual, or event
- Creation of photos or videos that do not represent reality
- Reposting of false content on legitimate sources
- The emersion of phrases or hashtags that quickly gain popularity.

Misinformation can spread via social media very quickly, especially during an emergency. In some cases though, not all rumors are false or untrue; sometimes they are facts not yet verified by an official source. This can result in members of the public acting upon information before it can be verified. Misinformation could potentially spread widely very quickly due to the viral nature of social media, leading to ill-advised actions or decisions simply based on a lack of official information.

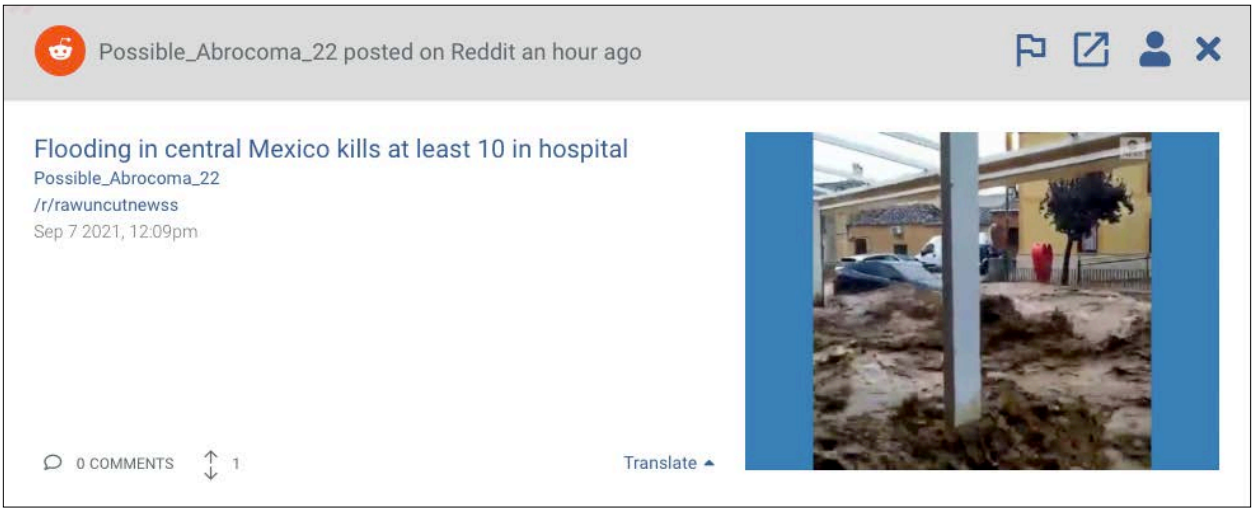


## CRISIS RESPONSE

When a national crisis occurs, governments must make timely, informed decisions to protect their data, assets, and citizens. Whether it's a natural disaster, public health crisis, or terrorist attack, intelligence teams need to know how and where a crisis is occurring, and how to allocate resources in response. Online spaces are often the earliest sources of information to provide this context—for example, social media users often post public updates and images from the scene of a crisis. Aligning this data with other feeds can help provide a faster and more informed response.

Real-time social media data, combined with information gleaned from more traditional sources, can help emergency responders gain and maintain situational awareness, and assist with decision-making, planning, and resource allocation. During response efforts following natural disasters, government officials now utilize social media to share information and connect with citizens through all phases of a crisis.

In a disaster response situation, an organization could use keyword searches and general monitoring to identify community needs, for example. Social media tools can also help aid groups, agencies and organizations advise the public about available resources during an emergency.



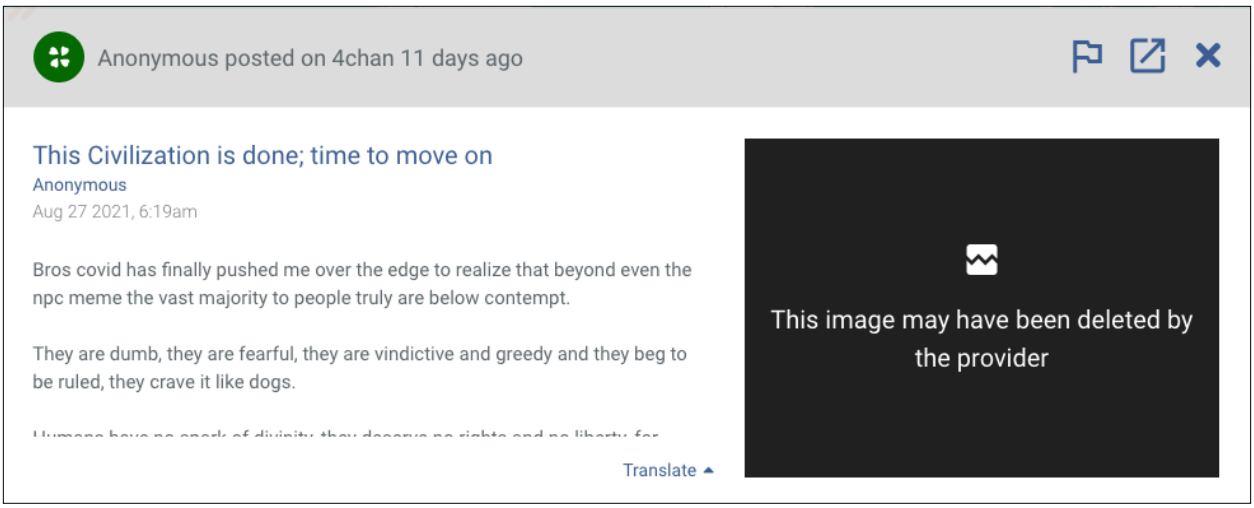
## SENTIMENT ANALYSIS

SENTIMENT ANALYSIS

Through ongoing engagement with the public via social media, organizations can "listen" for specific information or monitor for general situational awareness. Analysts can use social media monitoring and analysis to assess sentiment or popular support within a geographic area.

A U.S. RAND Counterinsurgency study in 2008 found that for the U.S. Military, "experience waging counterinsurgency operations across the globe has taught us that sentiment is fundamental in gauging success in the type of warfare the U.S. has been focused on for decades." [1]

Research performed by the US Naval Postgraduate School showed that social media data, when combined with traditional polling methods, has a positive impact on analysis, particularly where negative sentiment was concerned.




Some proponents of behaviour-based metrics believe that they can assess operational effectiveness through analyzing variables like security, economic indicators, justice indicators, and governance indicators. To do this, they gather and assess public attitudes, beliefs, atmospherics, and opinions via mass-media analysis, open-source analysis, and opinion polling. The study concluded that intelligence analysts should conduct social media analysis and combine the results with polling analysis to support operational assessments.

1 [Seth G. Jones, RAND Counterinsurgency Study, vol. 4, Counterinsurgency in Afghanistan (Santa Monica, CA: RAND Corporation, 2008), 7]

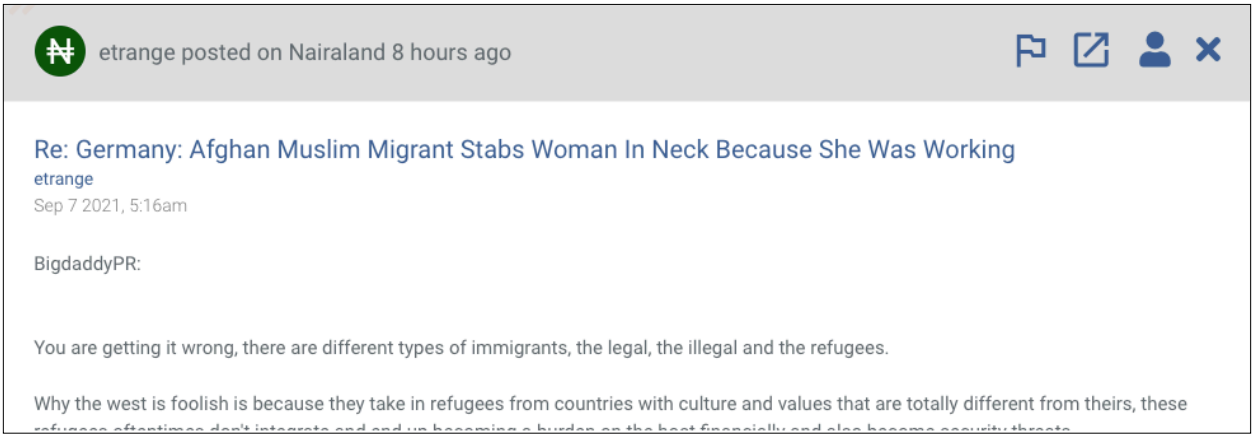
## GEOPOLITICAL RISK ASSESSMENT

Geopolitical risk can be thought of in this context as the risk associated with tensions between or within states that could potentially affect the course of international relations. Geopolitical risk encompasses both the risk that events materialize, and the new risks associated with an escalation of existing events.

In a 2017 Gallup survey of more than 1,000 investors, 75 percent of respondents expressed worries about the economic impact of the various **military and diplomatic** conflicts happening around the world, ranking geopolitical risk ahead of political and economic uncertainty. The ongoing conflicts in Afghanistan and Israel/ Palestine are just two examples where there are international political, economic and social ramifications to unrest between and within states.

**Climate change** will cause ongoing conflicts between governments, citizens, and corporations, as the general public gets caught between government commitments to reduce emissions and waste, and corporate profits. Climate change will make natural disasters more likely, more frequent, and more severe, and could potentially result in parts of the world becoming uninhabitable, displacing large numbers of people, and increasing political, social and economic instability caused by an unexpected influx of people fleeing into other areas.

**Politics** - With ongoing efforts by bad actors to influence elections worldwide, widespread disinformation or "fake news" can play a role in destabilizing entire countries, potentially even changing the outcome of a national level election. Monitoring online spaces is crucial for tracking disinformation campaigns so governments can mitigate their impact and keep the public safer and more informed.



# APIs

According to the US Intelligence National Strategy (2019), the intelligence community is increasingly challenged by growing volumes of online data available for collection, processing, analysis, and triage. The western world is also facing a data analyst shortage coupled with a growing demand for military AI. As a result, data scientists in the public sector tend to handle more complex tasks, developing tooling and data sets to support lower-level analysts on intuitive platforms.

Intelligence teams are also challenged by a lack of access to some emerging online sources. For example, fringe networks (like alt-tech platforms, deep and dark web imageboards and paste sites, etc.) do not offer their own APIs or are unavailable through commercial API providers. To gather data from these sources, analysts are often required to create dummy accounts, make group requests, and navigate networks manually. This requires a significant amount of HUMINT resources that could be allocated to other areas of the intelligence cycle.

Intelligence professionals require specialized software to collect information and generate actionable intelligence. Commercial OSINT tools help intelligence teams gather open-source data more efficiently and align with a team's unique requirements. Because intelligence teams often work with their own interfaces and tooling, they often require direct access to raw data that can be plugged into their existing systems.

Application programming interfaces (APIs) are becoming an integral part of any organization's investment in digital transformation—and intelligence and corporate security entities are no exception.

APIs help connect data with applications, saving users the resources otherwise required to integrate data inputs manually. In the context of gathering threat intelligence, the quality of an API's data and delivery is high-priority for:

- **Defense and intelligence teams** requiring access to online data feeds
- **Corporate security operations centres** using online feeds for security alerts
- **Data companies** seeking valuable online data inputs to offer their own clients

As a wider array of online spaces become relevant to security initiatives—whether it's a private or public sector environment—addressing data requirements in the coming years will rely heavily on the breadth of sources available through commercial API solutions, and security and intelligence professionals are likely to prioritize expanded data coverage in their tooling.

This can be achieved by leveraging API vendors who offer a wider variety of standard and alternative threat sources than is commonly available through commercial solutions. This looks like combining standard intelligence sources with emerging sites.

This has a number of benefits. For one, more data coverage = less overlooked information. Access to a direct API allows analysts to spend less time gathering data manually. Crawling more obscure sources also means that any posts that have since been deleted from the original site are retained for analysis—a side benefit not available through manual collection.

Additionally, combining various inputs allows for easier cross-referencing and pivoting between data sources. This is valuable since the intelligence bread crumb is becoming more convoluted as the online risk landscape diversifies and expands. As a result, analysts can glean insights that might not be obvious or available when standard and alternative data feeds are not integrated.

A more data-diverse solution can also better support machine learning development. Without access through an API, many online sources—such as content on obscure social sites and chat applications—could not otherwise be catalogued and stored appropriately for data science applications.

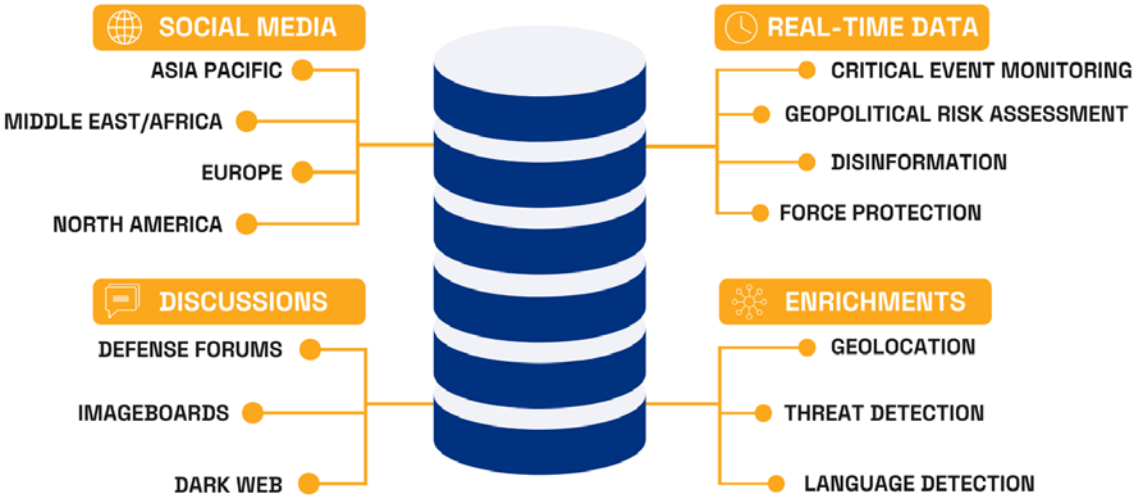
# Echosec Systems API

Many of today's most significant security threats originate in online discussions. Alt-tech platforms, imageboards, and deep web forums hold a wealth of information critical for counterterrorism, geopolitical risk monitoring, and sentiment analysis. The Echosec Systems API delivers streamlined access to this information in real-time and enriches data for enhanced security and intelligence.

The API is valuable for intelligence professionals, security operations centres, or other data companies who don't necessarily require a pre-built Platform UI—but access to high-quality data from a wide range of sources. The API serves as a complement to existing threat intelligence feeds, such as technical data.

The Echosec Systems API indexes data and leverages proprietary machine learning models to classify threats, speeding up the information gathering process. It also prioritizes real-time data over historical data, so you get the most up-to-date information possible. It provides access to a broad range of lesser-known data sources, including international networks, to deliver a powerful layer of information to enrich existing feeds. Increased data coverage means that users are less likely to overlook critical risks online—especially on fringe sites that are not commonly offered via commercial API.

The API integrates seamlessly into external interfaces and tooling to improve data coverage and enrich the value of existing feeds, without the need for a separate interface. Proprietary machine learning models are integrated within the API to help organizations process, analyze, and triage data more efficiently.



The Echosec Systems API can help analysts:

- Access invite-only and semi-closed groups that would otherwise require account creation
- Access text content that has since been deleted from sites like 4Chan
- Identify networks of users participating in hate speech and physical threats online
- Identify users across multiple sites
- Identify influential users within topics and groups online
- Discover plans of physical violence

The Echosec REST API is built with a data lake to support more advanced data science applications like integrations, analytics, visualizations, and AI.

The SOCIAL FIREHOSE API offers a scalable alternative to the current REST method of interacting with our API. With firehose access, users simply open a connection to our servers and receive all of our social data, in real-time and within seconds of when we process it. It guarantees full data fidelity for customers.

A comprehensive threat intelligence solution can save organizations millions, uphold national security, and retain public trust in the target organization. As online platforms evolve, critical information can be easily overlooked if security operations centres and intelligence agencies aren't looking beyond standard sources. Real-time and location-based situational awareness can help organizations assess risk in a timely manner, and act quickly to mitigate a situation if necessary.

*Screenshots provided by Echosec Systems*