carahsoft

SILOBREAKER

Blog: Connecting geopolitical events with cyber threats through real-time OSINT

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Silobreaker, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/SilobreakerResources

Join Events & Webinars:
carah.io/SilobreakerEvents

Discover Technology Solutions:
carah.io/SilobreakerSolutions

Learn About Procurement:
carah.io/SilobreakerContracts

Connect With Our Team:
Silobreaker@carahsoft.com
844-445-5688

SILOBREAKER

Blog: Connecting geopolitical events with cyber threats through real-time OSINT

Geopolitical instability isn't just a challenge for policymakers – it's an increasingly urgent concern for intelligence teams tasked with protecting organizations from digital and physical threats. Political developments, viral misinformation, and global events can quickly escalate into targeted cyber campaigns, supply chain disruptions, or reputational damage.

Against this backdrop, real-time open-source intelligence (OSINT) is becoming an essential tool for identifying and responding to these risks.

This blog will draw on recent cyberattacks and Silobreaker's own research to explore how OSINT can help connect the dots between global events and cyber threats – and importantly, how organizations can take timely action.

Expanding the definition of "geopolitics"

Traditionally, interest in geopolitics has been confined to monitoring global conflict or diplomatic relations. But today, even routine political activity in historically stable democracies – such as regulatory changes, elections or public statements – can have significant security implications.

In this broader context, geopolitical monitoring must now include developments within previously reliable states, that may affect organizations due to their industry, location, partnerships or public profile.

The Event–Action Chain

For effective geopolitical monitoring, a key concept is the Event-Action Chain. This framework links geopolitical events to actionable steps for Cyber Threat Intelligence (CTI) analysts. It is comprised of the following:

1. **Event** – A geopolitical incident such as a political decision, election or unrest
2. **Vulnerability** – Any organizational weakness exposed by the event (technical, human or structural)
3. **Threat** – A malicious actor's intent or capability to exploit the vulnerability
4. **Risk** – The potential business impact of the threat, based on context and exposure
5. **Action** – The tactical or strategic response informed by the preceding analysis

Following this framework, CTI analysts can determine the appropriate course of action to address geopolitical events. Each step of the chain will require setup to be ready for execution each time a relevant event is captured by analysts. This setup process should start with understanding the risk profile of your organization. Although impacts relating to risk come later in the chain, risk quantification is a lengthy process that typically follows yearly cycles and involves multiple stakeholders. It should therefore be prioritized to enable threat intelligence teams to tie global developments to organization-specific risks and responses.

Understanding organizational exposure

A vital step in the risk assessment process involves mapping an organization's "crown jewels". These key assets may include essential systems, facilities, partners, products and people. Securing vulnerabilities associated with your crown jewels are key in denying actors the opportunity to interrupt and prolong business continuity. These vulnerabilities may be technical (due to software flaws), human (such as susceptibility to phishing) or structural (due to industry or geography, such as supply chain reliance on a politically unstable region).

Identifying these elements allows intelligence teams to prioritize monitoring and quickly assess whether unfolding events may present a credible threat.

From headlines to hacktivism

Several recent examples of hacktivism illustrate how politically charged events can trigger rapid cyber threats.

Cyberattacks against Indian banks following viral misinformation

On 6 June 2024, a viral video showed an Israeli missile allegedly marked "Made in India" hitting a UN refugee camp in Gaza, sparking outrage. From 7 to 22 June, hacktivist groups Rippersec, Infamous, and RADNET launched cyberattacks against Indian financial institutions. Despite the video being debunked as showing medical equipment, the attacks continued, with Rippersec targeting 18 more organizations on 15th August, Indian Independence Day.

Targeted cyber incidents against French organizations after Trump state visit

President-elect Donald Trump announced his first foreign visit to France on 2nd December 2024 for the reopening of Notre Dame. On the 5th of December, the French Parliament passed a no-confidence vote against Prime Minister Michel Barnier.

Just a few days later, the hacktivist alliance known as the "Holy League", including groups like NoName057 and People's Cyber Army, launched DDoS attacks on French municipality websites, AXA and various energy firms. The campaign also targeted private companies across multiple sectors, highlighting how geopolitical events can lead to cyber threats.

Attacks on Italian ministries and banks after Zelensky visited Rome

Ukrainian President Vladimir Zelensky arrived in Rome on 9th January 2025, to meet with Italian Prime Minister Giorgia Meloni. Two days later, the pro-Russia hacker group, NoName057 launched DDoS attacks against the Italian Ministry of Foreign Affairs, Ministry of Infrastructure and several banks and port authorities.

Each example demonstrates how public events – even those based on falsehoods – can serve as triggers for cyber campaigns. OSINT tools are vital in identifying these early signals and monitoring related threat actor activity.

The motivation for these attacks is often widely publicized, enabling threat analysts to analyze hacktivist activity, identify targeted industries, locations and associated motivations, and create playbooks for predicted outcomes.

Monitoring OSINT allows security teams to anticipate and capture relevant political statements and events, such as elections and state visits, using these insights to trigger action plans that strengthen their security posture.

Public sentiment and brand risk

There are many tools dedicated to tracking actors' capabilities; however, their specific intent will frequently remain elusive. One helpful source for actor intent, particularly in an era marked by widespread boycott movements and politically motivated brand targeting, is examining public sentiment

By using tools like Google Trends or OSINT platforms to track brand mentions in relation to protests or activist groups, intelligence teams can anticipate possible phishing campaigns, website defacements or activist-led disruptions.

These examples illustrate why proactive monitoring and broader geopolitical awareness are essential, regardless of industry or size.

Turning OSINT into action

So how can OSINT drive tangible outcomes? The process typically involves two key cycles: general threat landscape, which involves identifying relevant global events, public sentiment shifts and resultant threat actor activity in specific regions and industry sectors, and **focused threat landscape**, which consists of monitoring high-risk actors identified in the first cycle for indicators of compromise (IOCs) as well as tactics, techniques and procedures (TTPs), then feeding those insights to detection teams.

This dual approach enables CTI teams to move from awareness to actionable intelligence, helping organizations stay ahead of threat campaigns.

Collaborating across functions, such as between cyber threat and strategic risk teams, is also increasingly important. Two effective collaboration models include **shared tools**, which give geopolitical analysts access to CTI tools so they can scale their insights using advanced

OSINT capabilities, and the **provider–stakeholder model**, where CTI teams are treated as an internal service provider for strategic risk teams, fulfilling requests for information (RFIs) and supporting broader risk assessments.

Either approach enhances cross-functional visibility and ensures intelligence is distributed efficiently.

Tailoring intelligence to stakeholders is also crucial. Different stakeholders require different levels of detail. CTI teams should adapt their reporting based on the audience:

- **Executives** may prefer concise risk-focused summaries
- **SOC teams and threat hunters** need technical data, such as IOCs and TTPs
- **Strategic risk leaders** often look for geopolitical context and long-term trends

Communication channels should not be created in isolation. They need to be tailored to each stakeholder, sending notifications and information through their preferred channels, e.g., via SIEM integration, email, Slack, Teams, or responding to tickets via platforms like ServiceNow.

Silobreaker for comprehensive geopolitical and cyber threat monitoring

Effective geopolitical event monitoring follows an Event-Action Chain that starts with broad monitoring and ends with actionable intelligence. Here, real-time OSINT can play a critical role.

Silobreaker supports this entire workflow within a unified environment, allowing teams to discover events across diverse sources – from news and social media to dark web and vulnerability feeds.

By mapping vulnerabilities, threats and risks directly to sources and dashboards, Silobreaker processes information to deliver industry-specific insights to satisfy priority intelligence requirements. The platform's AI-assisted reporting capabilities and real-time threat actor profiling enable immediate response to stakeholder requests, bridging the gap between geopolitical events and analyst action.

The convergence of geopolitics and cyber threats is creating new challenges, but also new opportunities for intelligence teams. With Silobreaker, CTI teams can connect external events to internal risks, enabling organizations to act quickly, effectively and with confidence.

Contributors: Lukas Vaivuckas, Solutions Consultant, Silobreak