Digital Crisis is Kinetic

Traditional monitoring tools can't keep pace with today's kinetic crises

By Ben Decker, Partner and Global Head of Threat Intelligence, FGS Global

FGS·GLOBAL

In 2026, crises don't announce themselves with press releases.

Instead, they erupt across platforms simultaneously—a deepfake video on TikTok is amplified by coordinated bot networks on X, leading to employee concerns spiraling in private Slack channels and regulatory scrutiny intensifying—all before your communications team has even convened. By the time a traditional social listening dashboard refreshes, the narrative has already metastasized.

Traditional monitoring tools were built for a different era: slower news cycles, centralized media gatekeepers, and clear boundaries between online and offline threats. That world is gone. In its place is an environment where:

- **Speed trumps perfection:** The first narrative to gain traction often defines the crisis, regardless of accuracy
- **Context is everything:** The same event can trigger vastly different responses depending on geopolitical timing, cultural sensitivities, and stakeholder economics and expectations
- **Silence is a strategy:** Sometimes the most effective response is no response—but only if you have the intelligence to make that call confidently

But the monitoring environment hasn't just evolved—it's been fundamentally transformed. And organizations still relying on point solutions are discovering, often painfully, that they're bringing yesterday's tools to tomorrow's fight.

The death of dashboards

For years, off-the-shelf social listening platforms promised comprehensive crisis visibility through color-coded dashboards and sentiment graphs. But AI models have rendered this approach obsolete.

The problem isn't the data—it's the delivery mechanism. Static dashboards can't adapt to the velocity and complexity of modern crises. They're designed to answer predetermined questions, not to surface the unexpected threats that define today's risk landscape. When a deepfake of your CEO announcing layoffs goes viral, you don't need a sentiment score. You need immediate context, source attribution, amplification patterns, and recommended response protocols.

When platforms became a hellscape

The content moderation landscape has deteriorated dramatically. Major tech companies have slashed trust and safety teams, with Meta alone reducing enforcement mistakes by 50% in Q1 2025, a metric that sounds positive until you realize it reflects reduced enforcement activity overall, not improved accuracy.

This retreat from moderation has created a vacuum that malicious actors eagerly exploit. Deepfake technology, once the domain of sophisticated state actors, is now accessible to anyone with basic technical skills. Organizations face coordinated disinformation campaigns, AI-generated impersonation attacks, and threats of offline violence—all with limited recourse from the platforms themselves.

The implications for corporate reputation are profound. When platforms won't moderate, organizations must monitor more aggressively and respond more swiftly and strategically. This means:

- **Expanding monitoring beyond traditional social platforms** to include fringe forums, messaging apps, and emerging platforms where threats often incubate before going mainstream
- **Deploying deepfake detection capabilities** as standard crisis infrastructure, not emergency add-ons
- **Building direct relationships with platform trust and safety teams** where they still exist, rather than relying on automated reporting systems

The era of outsourcing content governance to platforms is over.

Today's political volatility demands a proactive monitoring posture

Perhaps the most significant shift is the democratization of political risk. Reputational and physical threats to institutions are no longer confined to extractive industries, defense contractors, or politically exposed sectors like the news industry. They're industry-agnostic.

A children's toy manufacturer faces boycott campaigns over perceived political messaging. A regional bank becomes a proxy battleground for culture war debates. A pharmaceutical company's routine FDA approval triggers conspiracy theories linking it to geopolitical tensions.

This type of volatility also demands a new monitoring posture. Traditional crisis communications focused on reactive damage control, monitoring for mentions of your brand and responding to negative coverage.

Today's environment requires **proactive threat intelligence:** identifying emerging narratives before they reach critical mass, mapping influence networks that could amplify attacks, and understanding the geopolitical context that might make your organization a target.

According to the World Economic Forum's 2026 Global Cybersecurity Outlook, 70% of large employers have increased their focus on threat intelligence, compared to only 30% of small organizations. This gap represents a strategic vulnerability—smaller organizations often lack the capacity for sophisticated monitoring yet face the same threat landscape as their larger counterparts.

The interdisciplinary strike force

No single discipline can navigate this complexity alone. Effective crisis response in 2026 requires an interdisciplinary strike force: communicators who understand narrative dynamics, sector specialists with deep industry understanding, analysts who can interpret data patterns, and technologists who can deploy AI-driven monitoring tools.

This isn't about adding headcount, it's about integrating capabilities. Your communications and sector teams needs real-time access to threat intelligence. Your data analysts need to understand stakeholder psychology. Your technology infrastructure needs to support rapid response analysis and workflows, not just data storage.

The result is monitoring that scales like software but adapts like consulting.

Why this matters now

The convergence of AI-driven attacks, platform moderation failures, and geopolitical volatility has created what security researchers call a "threat environment where disruption, espionage, and influence operations are no longer isolated events, but part of sustained campaigns."

For organizations, this means crisis is no longer episodic—it's ambient. The question isn't whether you'll face a digital crisis, but whether you'll detect it early enough to shape the outcome.

The path forward

Every company in every industry needs a crisis playbook. But more importantly, they need the monitoring infrastructure to know when to activate it.

This infrastructure must be:

- **Adaptive:** Capable of pivoting from routine monitoring to crisis response without manual reconfiguration
- **Intelligent:** Leveraging AI not just for data collection but for pattern recognition, anomaly detection, and predictive analysis
- **Actionable:** Delivering insights that inform decisions, not just dashboards that display data

The organizations that thrive won't be those with the most data. They'll be those with the sharpest insights, delivered at the moment of maximum impact.

Because when crisis is kinetic, monitoring and threat detection must be too.

About the author

Ben Decker is a Partner and Global Head of Threat Intelligence at FGS Global, a leading strategic communications and stakeholder strategy firm, where he leads the firm's strategic initiatives at the intersection of digital security, information integrity, and global risk management.

Previously, Ben was founder and CEO of Memetica, a digital threat detection and intelligence consultancy acquired by FGS Global in 2026.

Prior to this, he was a technology researcher and investigative journalist at The New York Times, where he developed deep proficiency in uncovering and analyzing complex digital ecosystems.

He began his career in corporate intelligence, where he served as a crisis management specialist across MENA and Eastern Europe, advising organizations on operational security risks in complex geopolitical environments.

Ben has provided testimony before the United Nations Human Rights Council, provided policy advice to Ofcom, and served as a member of the Christchurch Call Advisory Network.

A graduate of Emory University and Tel Aviv University, in 2019, Ben completed a research fellowship at the Harvard Kennedy School, where he examined the network propagation of extremist ideologies and their impact on global elections.

FGSGLOBAL.COM