CYBER GEOPOLITICAL INTELLIGENCE

Leveraging World-class Threat Intelligence to Gain Political Threat Insights and Mitigate Risks

Geopolitics shapes state and non-state threats in the cyber domain and requires organizations to continuously monitor events that affect their business operations and supply chain. Intel 471's Cyber Geopolitical Intelligence provides organizational leaders with a unique lens into significant regional events and changes in policy, leadership, and technology that are likely to impact cyber risks.

Cyber Geopolitical Intelligence arms customers with key insights and contextualized analysis of political activity focused on nations such as China, Iran and Russia, and their respective impact on the complex cyber threat environment. It also examines the role of cyberspace in geopolitical power dynamics. It analyzes how state leaders use cyber capabilities to achieve strategic objectives, including espionage, offensive cyber operations, and information warfare. It also considers the potential for cyberattacks to escalate into real-world conflicts or to undermine international trust and cooperation.

ANALYSIS DESIGNED TO STRENGTHEN RISK PROFILE

Clear, concise and contextualized analysis of cyber threats stemming from geopolitical events enable government and organizational leaders to incorporate geopolitical events into their cyber risk management, and improve their decisions about cybersecurity investments, policies and strategies.

Cyber Geopolitical Intelligence from Intel 471 helps organizational leaders:

- Lower the noise floor
- Improve situational awareness
- Understand exposure to regional threats
- Manage risk from suppliers, subsidiaries and M&A activities

Intel 471's Geopolitical Intelligence provides accurate, locally sourced information that is shared in five discrete report types. Customers receive daily, weekly, bi-weekly and quarterly updates which ensures they have the most up-to-date and accurate information, as well as a full analysis of trending geopolitical events. Our regional intelligence experts and linguistic analysts assess first-hand sources to contextualize adversary activity and tactics. Organizational leaders can use these reports to improve situational awareness and proactively manage risks to their regional operations, supply chains, and merger and acquisition interests.

Report	Coverage
Spot Reports	Emerging activity about significant geopolitical events with contextual analysis
Profile Reports	Overview of threat actor or group, including summary of activity, target trends, and TTPs
Intelligence Bulletins	Thematic reports covering country-specific threats, key geopolitical issues and emerging trends
Intelligence Summaries	Insights into significant, trending geopolitical events during a reporting period in China, Iran, Russia, and the "rest of world".
Threat Briefs	Comprehensive reports on a country or regional topic, including in-depth country primer report.

Intel 471's Cyber Geopolitical Intelligence provides five report types

ABOUT INTEL 471

Intel 471 empowers enterprises, government agencies, and other organizations to win the cybersecurity war using the real-time insights about adversaries, their relationships, threat patterns, and imminent attacks relevant to their businesses. The company's platform collects, interprets, structures, and validates human-led, automation-enhanced intelligence, which fuels our external attack surface and advanced behavioral threat hunting solutions. Customers utilize this operationalized intelligence to drive a proactive response to neutralize threats and mitigate risk. Organizations across the globe leverage Intel 471's world-class intelligence, our trusted practitioner engagement and enablement and globally-dispersed ground expertise as their frontline guardian against the ever-evolving landscape of cyber threats to fight the adversary — and win. Learn more at **www.intel471.com**.