

Geopolitical Threat Intelligence

AnnexVault LLC
Groundhog Research Group™

Original publication: April 2025
Revised: 26 October 2026

Geopolitical threat intelligence in cybersecurity explores the interplay between global politics and cyber threats, focusing on how nation-states and non-state actors leverage cyber tools for political, economic, and strategic gains. This paper examines motivations behind state-sponsored cyber activities, their impact on critical infrastructure and national security, and the influence of disinformation campaigns. Additionally, it highlights international responses to these threats and emerging risks from technological advancements. By analyzing specific cases and international norms, this study emphasizes the need for an integrated approach to cybersecurity that considers both technical and geopolitical dimensions.

Why this matters to AnnexVault

This report explains how global events can change the meaning of cyber and operational evidence. Context helps reviewers understand why a development matters.

Key Components of Geopolitical Threat Intelligence:

- **Data Collection:** Gathering information from various sources, including open-source intelligence (OSINT), human intelligence (HUMINT), and signals intelligence (SIGINT).
- **Analysis:** Evaluating the collected data to understand the intentions and capabilities of potential adversaries.
- **Dissemination:** Sharing actionable intelligence with relevant stakeholders to inform decision-making.

Importance in Government and Defense:

- **Strategic Planning:** Helps in formulating defense strategies by understanding global political dynamics.
- **Risk Mitigation:** Identifies potential threats, allowing for proactive measures to prevent or minimize impact.
- **Resource Allocation:** Guides the efficient distribution of resources to areas of highest risk.

Current Geopolitical Threat Landscape:

The geopolitical environment is increasingly complex, with state and non-state actors posing diverse threats. For instance, state-sponsored cyberattacks have targeted critical infrastructure, aiming to disrupt services and steal sensitive information. The U.S. Department of Defense's 2022 National Defense Strategy emphasizes the need to strengthen deterrence against nations like China and Russia, highlighting the importance of geopolitical threat intelligence in addressing these challenges. [11]

[Defense.gov](https://www.defense.gov)

Financial institutions are increasingly affected by geopolitical tensions that disrupt markets, regulatory landscapes, and operational stability. These geopolitical risks necessitate a proactive approach to risk management and threat intelligence.

Key Geopolitical Risks

- **Sanctions and Regulatory Changes:** International sanctions can restrict financial transactions and access to assets. FINMA's 2024 Risk Monitor identifies challenges for Swiss financial institutions in determining whether corporate payments fall under sanctions on Russia. [1]
- **Cybersecurity Threats:** Geopolitical tensions can increase cyber risk. Akamai's September 2024 report identified financial services as the most frequently targeted sector for Layer 3 and Layer 4 DDoS attacks in its observations and linked increased activity to geopolitical hacktivism. [2]
- **Market Volatility:** Political instability can affect trading activity and market volatility. CME Group reported second-quarter 2024 revenue growth of 13% year over year, alongside volume and open-interest growth across all asset classes. This result alone does not establish how much growth was caused by geopolitical events. [3]

Strategic Responses

- **Risk Assessment Frameworks:** Tailored risk assessment helps financial institutions evaluate their exposure to geopolitical risks. KPMG's 2024 financial-services guide addresses the management of these risks. [4]
- **Threat Intelligence Integration:** Financial institutions can incorporate geopolitical threat intelligence into risk assessment and strategic decision-making. [5]

Geopolitical threat intelligence is vital for the financial services sector to maintain resilience. Effective strategies such as risk frameworks and integrated threat intelligence enable institutions to navigate a complex global landscape. These approaches are essential in safeguarding financial stability against geopolitical uncertainties.

Geopolitical Threats to Healthcare and Pharmaceuticals

Supply Chain Disruptions:

- **Global Dependencies:** The pharmaceutical industry heavily relies on international supply chains for raw materials and active pharmaceutical ingredients (APIs). Geopolitical tensions, such as trade disputes or sanctions, can disrupt these supply lines, leading to drug shortages. Dependence on overseas suppliers can expose the supply chain to geopolitical disruptions. FDA's 2019 testimony cautioned that manufacturing-facility locations did not establish the volume of APIs supplied to the U.S. from particular countries. [6]

Regulatory Changes:

- **Policy Shifts:** Domestic policy and international relations can affect drug pricing, approvals, and market access. The U.S. Inflation Reduction Act established Medicare price negotiation for selected drugs, with the first negotiated prices taking effect in 2026. [7]

Cybersecurity Threats:

- **Geopolitically Motivated Attacks:** HHS reported that the pro-Russia hacktivist group KillNet targeted U.S. health and public-health organizations with DDoS attacks from December 2022 through March 2023. These attacks can disrupt service availability; this example does not by itself establish state sponsorship or theft of patient data. [8]

Market Access and Operations:

- **International Operations:** Pharmaceutical companies operating across borders must monitor local regulatory and enforcement risks as well as geopolitical tensions. On 30 October 2024, AstraZeneca stated that its China president was cooperating with an investigation by Chinese authorities and that its China operations continued under the general manager. The statement did not establish a geopolitical cause. [9]

Mitigation Strategies:

- **Diversification:** Reducing reliance on single-source suppliers and markets can help mitigate risks associated with geopolitical tensions.
- **Regulatory Intelligence:** Staying informed about global regulatory changes enables companies to adapt swiftly to new policies.
- **Cybersecurity Measures:** Implementing robust cybersecurity controls helps reduce exposure to state-sponsored and other cyber threats.
- **Scenario Planning:** Developing contingency plans for geopolitical scenarios supports preparedness for potential disruptions.

Understanding and proactively managing geopolitical threats are essential for maintaining the resilience and integrity of healthcare and pharmaceutical operations in an increasingly interconnected and volatile global landscape.

Geopolitical threat intelligence within critical infrastructure is a field focused on analyzing and understanding how political tensions, regional conflicts, and international relations impact the security and stability of essential systems, such as energy grids, transportation networks, and communication systems. As nations and regions increasingly depend on interconnected infrastructure, understanding these threats has become crucial for both government agencies and private sector entities tasked with protecting vital services.

1. What is Geopolitical Threat Intelligence?

Geopolitical threat intelligence involves monitoring, analyzing, and predicting the impact of political events and tensions on critical infrastructure. This includes identifying potential risks, such as:

- **Cyber-attacks** from nation-state actors targeting essential services.
- **Physical attacks** or sabotage on infrastructure facilities.

- **Economic sanctions** impacting supply chains and operations.
- **Trade wars or embargoes** disrupting resource availability.

This intelligence helps organizations prepare for disruptions that could affect everything from energy supplies to internet connectivity.

2. Vulnerabilities in Critical Infrastructure

Critical infrastructure sectors like energy, water, transportation, and telecommunications are particularly vulnerable to geopolitical threats due to their interconnected nature and reliance on digital systems. Threat actors may exploit these vulnerabilities to destabilize regions or influence foreign policies.

The 2015 cyberattack on Ukraine's power grid illustrates the potential operational impact of cyber activity during geopolitical conflict. In 2020, the U.S. Department of Justice charged Russian military-intelligence officers in connection with destructive attacks on Ukrainian infrastructure in 2015 and 2016. [10]

3. Types of Geopolitical Threats to Critical Infrastructure

Cybersecurity Threats:

- **Nation-state hacking groups** may target infrastructure for espionage, disruption, or other strategic objectives. [10]
- **Ransomware attacks** on municipal systems disrupt local services and create cascading impacts on a broader scale.

Supply Chain Disruptions:

- Geopolitical conflicts often lead to **trade restrictions**, affecting the flow of essential resources and materials necessary for infrastructure maintenance and expansion.

Physical Threats:

- **Terrorist attacks or sabotage** at key facilities can disrupt energy, water, and communication systems, impacting millions.

Regional Distribution of Geopolitical Threats

Regional assessments should consider political conditions, infrastructure dependencies, and security posture. The following are qualitative considerations, not comparative measurements of attack frequency:

- **Europe:** Assess energy infrastructure exposure to conflict, disruption, and dependence on imported resources.
- **North America:** Assess cyber exposure across interconnected digital and critical-infrastructure systems.

- **Asia:** Assess cyber and physical risks in the context of local conflicts, cross-border dependencies, and major infrastructure projects.

These insights underscore the need for tailored, region-specific threat intelligence strategies to safeguard critical infrastructure from varied geopolitical threats.

References

- [1] FINMA: Risk Monitor 2024, sanctions
- [2] Akamai: Financial-services DDoS findings (September 2024)
- [3] CME Group: Second-quarter 2024 earnings commentary
- [4] KPMG: Managing geopolitical risks, financial-services guide (2024)
- [5] Dragonfly: Current product description (not evidence of efficacy)
- [6] FDA: Safeguarding Pharmaceutical Supply Chains in a Global Economy (2019)
- [7] CMS: Medicare Drug Price Negotiation Program - selected drugs for initial price applicability year 2026
- [8] HHS HC3: KillNet targeting of the health sector (April 2023)
- [9] AstraZeneca: China president investigation statement (30 October 2024)
- [10] U.S. DOJ: Charges relating to attacks on Ukrainian infrastructure (2020)
- [11] U.S. Department of Defense: National Defense Strategy (2022)