Facilitating a better future
lmalloyds.com

Lloyd's Market Association
Suite 426 Gallery 4
One Lime Street
London EC3M 7DQ
T. 020 7327 3333

LMA & Control Risks: Geopolitical Risk Briefing – Key Themes

Purpose

This note summarises the key themes discussed at the recent Control Risks briefing, with a specific focus on implications for Lloyd's Managing Agents risk functions.

1. Global Context: "No Rules, New Rules"

The global geopolitical environment continues to move away from rules-based multilateralism towards interest-driven, transactional, power state behaviour.

Established international institutions are increasingly challenged, while new groupings and parallel structures are emerging, particularly across the Global South.

Key dynamics highlighted by Control Risks include:

- **Erosion of geopolitical norms**, with states more willing to break or selectively apply rules.
- **Fragmented global order**, with different rules for different partners and increased politicisation of trade and business.
- **Strategic competition over sovereignty**, with the EU prioritising protection of critical and strategic sectors (notably technology) while pursuing new trade arrangements globally.
- **China positioning itself as a leader of alternative multilateralism**, deepening engagement with emerging markets and easing trade barriers for selected partners, including African states.
- **Declining trust in institutions**, reflected in growing public support for disruptive or activist movements across multiple regions.

For insurers, this implies **greater volatility and lower predictability** at the international level.

2. Activated Societies and Political Risk

Societal pressures are intensifying, driven by economic stress, legitimacy gaps and demographic trends.

Control Risks highlighted:

- **Rising youth unemployment**, particularly in Sub-Saharan Africa, MENA and parts of South Asia, increasing susceptibility to unrest and radicalisation.
- **Elections as flashpoints**, with upcoming or recent cycles linked to protest movements and instability (including Morocco, Brazil and the US in 2026; France and Argentina in 2027).
- **Major public events and reform agendas** (e.g. pensions, healthcare, education) acting as potential catalysts for unrest where trust in governance is low.

For Managing Agents, this reinforces the need to **track political timelines and socio-economic stress indicators**, not just formal country risk ratings, as leading indicators of loss activity and disruption.

3. Organised Crime as a Geopolitical Risk Channel

A central message from the session was that **geopolitical instability is increasingly driving organised crime risk**, rather than these risks developing independently.

Key observations included:

- A **material increase in violent organised crime incidents affecting businesses**, with hybrid tactics spanning criminal, political and state-linked activity.
- Organised criminal groups exploiting geopolitical distraction and governance weaknesses to scale operations.
- Use of **sabotage, espionage and infrastructure disruption** as part of criminal activity.
- Sectors particularly exposed include **electronic equipment, technology supply chains and pharmaceuticals**.
- Corruption levels remain a critical early warning indicator of where organised crime risks are likely to intensify.

Control Risks cautioned against "**normalisation**" – the assumption that elevated crime and disruption represent temporary blips rather than a structurally higher risk environment. CROs were encouraged to treat organised crime as a **strategic, not purely operational, risk.**

4. Scenario Thinking: Avoiding the "Normalisation Trap"

Control Risks experts emphasised the importance of **scenario planning beyond base-case assumptions**.

Key points included:

- Wildcard scenarios are becoming **more frequent and more plausible**, even if low probability.
- Overlapping crises (geopolitical, climate, technological) could interact in ways not captured by traditional stress testing.
- There is a need to think **beyond immediate impacts**, considering second- and third-order effects across sectors (e.g. knock-on impacts from chemical or technology supply chain disruption).
- Shifting corporate and societal **risk tolerance** may change behavioural responses following shocks.

For risk functions, this supports deeper use of **cross-scenario mapping, event triggers and escalation thresholds** within enterprise risk and underwriting frameworks.

5. Middle East: Conflict Outlook and Infrastructure Risk

The Middle East was identified as a key area of elevated but fluid risk.

Control Risks assessed that:

- Current hostilities represent the **most intense period of regional conflict since October 2023**, with direct targeting between Israel and Iran and subsequent US involvement in 2025.
- **Critical infrastructure has been directly targeted**, including:
  - Energy facilities (notably in Saudi Arabia and Qatar),
  - Power and desalination assets (Kuwait and Bahrain),
  - Transport hubs, including Dubai and Doha airports,
  - Residential infrastructure.
- Maritime disruption remains a key concern. While reports of mining in the Strait of Hormuz remain unconfirmed, uncertainty alone has material risk implications for shipping and energy.

Short-term outlook:

- Most likely: a **partial, fragile ceasefire** with ongoing tensions.
- Credible alternative: **sudden re-escalation**.
- Outlier: a **shallow US–Iran agreement**.

Managing Agents should assume **continued volatility rather than resolution**, with implications across property, energy, marine, aviation and political violence classes.

6. Emerging Cyber Risks: Converging Digital and Physical Threats

The cyber risks session highlighted an accelerating convergence between digital and physical attack vectors.

Key themes included:

- Digital intelligence (open-source data, social media, corporate disclosures) is increasingly used to enable **physical targeting**.
- Conversely, **physical attacks are now being used to generate digital impact**, particularly through disruption of data centres, power supply and connectivity.
- Computing capability itself is emerging as a **strategic asset**, shaping targeting decisions.
- Growing maturity of AI tools is expanding attackers' capability to:
  - Identify software vulnerabilities,
  - Reverse-engineer and weaponise software updates,
  - Deploy deep-fake and synthetic content for social engineering and disinformation.
- Despite geopolitical tensions, **financially motivated cybercrime remains the dominant threat** to most organisations.

Control Risks noted a sharp rise in cyber incidents over 2024–25, with early signs of business failures following severe events, though Middle East conflict has not yet driven cyber impacts on the same scale seen after Russia–Ukraine.

For Managing Agents, this underscores the importance of **systemic cyber exposure, aggregation risk and contingent business interruption**, particularly where physical and digital dependencies intersect.

7. Implications for CROs and Risk Functions

Across themes, several practical implications emerged:

- Strengthen **geopolitical monitoring frameworks**, with defined triggers for escalation following major events.
- Integrate **political, organised crime and cyber risk** more explicitly within scenario analysis.
- Avoid anchoring on recent experience; **current volatility is not a temporary anomaly**.
- Engage underwriting, exposure management and claims teams in forward-looking risk conversations, particularly around infrastructure, supply chains and systemic cyber events.

The **LMA's CRO committee** will continue to facilitate discussion and peer exchange on these themes and communicate output regularly.