S.F. CUSTOS GLOBAL REACH LTD.
SECURITY · INTELLIGENCE · PROTECTION

SPECIAL REPORT
2026-07-09

SPECIAL REPORT · STRATEGIC RISK / CYBER / COALITION SECURITY

# Petraeus's Strategic Risk Lens: Coalition Discipline, Cyber Exposure and China Deterrence

**Author:** Benjamin Traunecker

## Executive summary

The useful value in Gen. David H. Petraeus's public remarks is not a prediction about one crisis. It is a command lens: competition is decided by preparation, coalition discipline, cyber resilience and the ability to hold together large organisations under pressure. For companies, diplomatic actors, NGOs and high-net-worth travellers, that lens matters because the same pressures now appear in non-military operating environments: contested infrastructure, fragile alliances, cyber-enabled disruption, political caveats and reduced warning time before local conditions change.

Petraeus identifies the U.S.–China relationship as the central strategic relationship of the period. That judgment is consistent with the 2025 U.S. intelligence baseline, which treats China as the only competitor with the intent and capacity to challenge the United States across diplomatic, military, technological and economic domains. The practical risk for organisations is not a single Taiwan scenario. It is the broader exposure created when supply chains, technology dependency, port access, sanctions policy and executive travel all sit inside the same strategic competition.

His discussion of SolarWinds remains operationally relevant even though the incident itself is no longer new. CISA assessed that the campaign compromised U.S. government agencies, critical infrastructure entities and private-sector organisations beginning at least in March 2020, and that removing the actor from affected environments would be complex and challenging. The enduring lesson is that sophisticated adversaries do not need to defeat every perimeter control. They can enter through trusted software, identity systems, administrative credentials or supplier access, then exploit the delay between compromise and discovery.

The coalition lesson is equally important. Petraeus's account of multinational command stresses that allies bring strengths, political limits and operational caveats at the same time. NATO's 2025 Hague Summit commitment to invest 5% of GDP annually by 2035, including 3.5% for core defence and up to 1.5% for infrastructure, networks, civil preparedness and defence industrial resilience, reinforces the same point: resilience is now an alliance-wide capacity problem, not only a battlefield issue.

For SF Custos Global's client base, the main implication is straightforward. Strategic risk should be managed as a system of dependencies: people, routes, sites, networks, suppliers, insurers and public authorities. The organisations that perform best will not be those that merely monitor geopolitics. They will be those that translate warning indicators into movement rules, cyber controls, supplier decisions and leadership routines before a crisis forces the decision.

## What matters now

- **Strategic competition is an operating constraint.** U.S.–China tension affects technology supply chains, export controls, maritime routing, sanctions risk and executive exposure even when no military crisis is underway.

- **Cyber risk is now a strategic access problem.** The SolarWinds case shows that trusted vendors, identity infrastructure and administrative credentials can become the route into an organisation; defensive planning must treat suppliers and access rights as operational risk.
- **Coalitions create resilience and friction.** NATO's 2025 defence-investment baseline shows that allies are moving toward higher spending and stronger civil preparedness, but national caveats and uneven capabilities will still affect crisis response.
- **Leadership quality changes crisis outcomes.** Petraeus's emphasis on preparation, self-study, team contribution and adaptation is not motivational filler. It is a practical test of whether an organisation can act under pressure without waiting for perfect information.
- **Client impact is indirect but real.** Most organisations will not decide national strategy, but they will feel its effects through insurance costs, route availability, cyber exposure, border controls, staff movement and political-security spillover.

## Current operating picture

The senior-expert input reviewed for this report is best treated as strategic context, not as a current-event source. Its strongest material concerns enduring mechanisms: how leaders prepare for crisis, how coalitions work under political limits, why cyber operations create strategic vulnerability, and why the U.S.–China relationship sits at the centre of global security risk. Those mechanisms remain relevant in 2026 because the current open-source baseline points in the same direction.

NATO's Hague Summit declaration provides the clearest official European anchor. Allies reaffirmed Article 5, described Russia as a long-term threat to Euro-Atlantic security, and committed to invest 5% of GDP annually by 2035. The structure of that pledge matters: 3.5% is tied to core defence requirements and NATO capability targets, while up to 1.5% is tied to critical infrastructure, networks, civil preparedness, innovation and defence-industrial capacity. That is not only a military spending story. It is a resilience story that reaches ports, networks, industrial supply, mobility, emergency planning and host-nation support.

The cyber baseline is also clear. CISA's SolarWinds advisory assessed that an advanced persistent threat actor compromised public and private-sector organisations and that the actor showed patience, operational security and complex tradecraft. CISA also warned that SolarWinds Orion was not the only possible access vector, noting legitimate-account abuse and credential-related access paths. That aligns with Petraeus's warning that cyber threats are becoming more sophisticated and that the SolarWinds case exposed a detection gap between government systems and private-sector discovery.

The China baseline is broader. U.S. intelligence assessments have consistently framed China as the principal strategic competitor with the capacity to challenge U.S. influence across multiple domains. Petraeus's emphasis on avoiding miscalculation is therefore not theoretical. A crisis involving Taiwan, the South China Sea, cyber activity, export controls or sanctions would not remain confined to military planners. It would affect shipping, aviation, technology procurement, insurance, compliance and executive travel decisions.

The Iran, North Korea and extremist-threat elements in the expert discussion should be handled with more caution. Petraeus mentions them as part of the broader threat set, but the reviewed material does not provide enough current detail to support a dedicated Iran or counterterrorism assessment. For this report, they are treated as background examples of revisionist or persistent threat actors, not as the core analytical focus.

## Key risk mechanisms

### 1. Strategic competition compresses business warning time

The main danger in U.S.–China competition is not only a deliberate military decision. It is miscalculation, signalling failure or a coercive move that produces rapid secondary effects. A maritime or airspace incident can change executive travel approvals, insurance assumptions and supply-chain routing faster than corporate governance cycles can adapt. Organisations exposed to China-linked supply chains, Taiwan-linked technology, U.S. export controls or dual-use equipment should treat strategic competition as a standing operating variable, not as a distant geopolitical theme.

### 2. Coalition strength depends on caveats as much as capability

Petraeus's coalition-management point is directly transferable to corporate and diplomatic crisis planning. Partners rarely bring equal authority, equal capability or equal political tolerance for risk. In Afghanistan, he described allies that provided valuable forces but operated under national caveats. The corporate equivalent is a response network in which the insurer, local guard force, logistics provider, embassy, medical provider and headquarters all have different limits. Plans fail when those limits are discovered during the incident rather than mapped before it.

### 3. Cyber exposure follows trust relationships

SolarWinds remains a useful case because it attacked a trusted management pathway. CISA's advisory described the campaign as patient and well-resourced, with supply-chain compromise, legitimate-account abuse and possible additional access vectors. For organisations, the lesson is that cyber security is not only a technical perimeter issue. It is a supplier-governance, identity-management and crisis-communications issue. A trusted update channel, privileged administrator account or outsourced service can become the operational route into the organisation.

### 4. Leadership routines shape crisis performance

Petraeus returns repeatedly to preparation, self-study, team contribution and adaptation. Those points are not abstract leadership lessons. In security terms, they translate into rehearsed decision authorities, after-action learning, clear escalation thresholds, a common operating picture and the ability to support another unit or partner when the main effort changes. Organisations that only write plans usually discover the gaps late. Organisations that exercise plans discover the gaps early.

### 5. Resilience is becoming a policy requirement

NATO's 1.5% defence-and-security-related spending category explicitly includes critical infrastructure, networks, civil preparedness, innovation and defence-industrial capacity. That language points toward a wider policy trend: governments will expect parts of the private sector to carry more resilience burden. Companies operating in critical infrastructure, logistics, cyber services, defence-adjacent manufacturing, energy, maritime support or emergency supply should expect stronger scrutiny of continuity planning and supplier assurance.

## Scenarios and outlook

### Scenario 1 — Managed strategic competition remains the base case

The most likely near-term path is continued competition without a direct major-power clash. Engagement continues where both sides need it, while technology controls, military signalling, cyber operations and regional pressure persist. For organisations, this means persistent compliance complexity, periodic travel uncertainty and a need to review suppliers that sit inside sensitive technology or defence-adjacent chains.

**Early indicators:** new export-control rounds, expanded sanctions designations, additional military exercises around Taiwan or the South China Sea, and more restrictive corporate security guidance for senior executive travel.

### Scenario 2 — A regional incident produces rapid commercial disruption

A collision, blockade scare, cyber operation or coercive inspection regime could produce short-notice effects on shipping, aviation, insurance or diplomatic movement. The incident may remain below the threshold of war but still force companies to reroute staff, delay site visits or activate continuity procedures.

**Early indicators:** new air or maritime exclusion notices, embassy movement restrictions, insurance-market repricing, emergency shipping advisories and official warnings to citizens or companies.

### Scenario 3 — Cyber exploitation triggers operational response without physical violence

A campaign against government, logistics, telecoms, energy or supplier networks could create operational disruption without a kinetic event. The SolarWinds case shows why this scenario can be difficult to detect early: the entry point may look legitimate, the adversary may move patiently, and the first public signal may come from a private-sector victim rather than a state warning system.

**Early indicators:** emergency directives from cyber authorities, vendor advisories for widely deployed platforms, unusual identity-provider activity, forced credential resets and confirmed compromise of managed-service or network-management providers.

### Scenario 4 — Alliance adaptation improves deterrence but exposes uneven readiness

NATO's higher investment baseline should strengthen deterrence over time, but implementation will be uneven. Some allies will move faster on defence-industrial capacity, networks and civil preparedness; others will remain constrained by budgets, politics or procurement delays. That unevenness matters for crisis planning because local host-nation support and infrastructure resilience will not improve uniformly.

**Early indicators:** annual national implementation plans, procurement bottlenecks, public disputes over spending categorisation, and new rules for critical-infrastructure resilience.

## Implications for organisations

**Personnel and executive movement:** Senior travel into politically sensitive environments should be tied to triggers, not general mood. Triggers include embassy movement notices, airspace restrictions, protest locations near hotels, sanctions announcements, cyber incidents affecting local infrastructure and credible reports of border or airport disruption.

**Site and supply-chain exposure:** Facilities linked to ports, logistics corridors, energy infrastructure, defence-adjacent production or politically exposed suppliers need clearer continuity assumptions. A supplier may be technically reliable but strategically exposed through ownership, location, sanctions vulnerability or dependency on contested shipping routes.

**Cyber and identity controls:** The SolarWinds lesson is that privileged access and trusted software pathways require governance at board level, not only technical administration. Organisations should know which vendors can reach core systems, which accounts can bypass normal controls, and who has authority to disconnect, suspend or isolate a supplier during a suspected compromise.

**Crisis leadership:** The leadership lesson is to define the main effort before the incident. In a crisis, not every department can receive priority at the same time. Security, legal, communications, operations and executive leadership need a shared escalation model that decides when movement stops, when suppliers are isolated, when clients are notified and when external advice is required.

**Insurance and contractual exposure:** Strategic-risk events often surface through exclusions, notification deadlines, force-majeure disputes and cyber-coverage conditions. Organisations should confirm what is actually covered before a crisis, not when an insurer or provider is already applying a restrictive interpretation.

## Recommended actions

### Within 72 hours

- **Map critical dependencies:** Identify the five suppliers, platforms or access relationships that would create the largest operational loss if compromised or suspended.
- **Check executive travel triggers:** Confirm which conditions would delay or cancel senior travel to higher-risk destinations, including cyber disruption, airspace changes, embassy restrictions and local unrest.
- **Review privileged access:** Ask security and IT teams for a current list of vendors and administrators with privileged or remote access to core systems.

### Within seven days

- **Exercise one coalition problem:** Run a short tabletop in which a local provider, insurer, embassy contact or logistics partner cannot support the plan as assumed. The purpose is to expose caveats before a real incident.
- **Validate supplier-removal authority:** Confirm who can suspend a vendor connection, block a managed-service account or pause a software update if a compromise is suspected.
- **Update watch indicators:** Add NATO implementation, China-related export controls, major cyber directives and regional movement advisories to the executive risk watchlist.

### Within thirty days

- **Align strategy and operations:** Convert geopolitical themes into operating rules for travel, procurement, cyber access and crisis communication.
- **Review insurance and contracts:** Check whether cyber, political violence, travel and business-interruption policies match the organisation’s actual exposure.
- **Rehearse leadership handover:** Ensure the crisis team can operate if the CEO, regional director, security lead or IT lead is unavailable.

## Early warning indicators

- New official guidance on China-related export controls, sanctions or dual-use technology restrictions.
- Airspace, maritime or embassy movement advisories affecting Taiwan, the South China Sea, the Red Sea, the Gulf region or NATO’s eastern flank.
- Cyber emergency directives involving identity providers, managed-service providers, network-management tools or widely deployed enterprise software.
- NATO national implementation plans that materially change host-nation support, infrastructure protection or defence-industrial procurement.
- Insurance-market changes affecting war risk, cyber coverage, political violence, kidnap and ransom, or business interruption.

## Selected sources


- Public colloquy with Gen. David H. Petraeus, U.S. Army (Ret.), reviewed by SF Custos Global on 9 July 2026.
- NATO, The Hague Summit Declaration, 2025.
- Cybersecurity and Infrastructure Security Agency, Alert AA20-352A on advanced persistent threat activity and SolarWinds Orion compromise.
- Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, 2025.
- NATO public background material on alliance membership and participation flexibility.


## Method note

This report is based on open-source material reviewed up to 9 July 2026 and analytical assessment by SF Custos Global. It does not replace legal, insurance, sanctions, medical or country-specific professional advice.