Asset Management COO Community

Perspectives on geopolitical risk assessment

ARMSTRONG WOLFE™

In March 2022 the Asset Management iCOOC membership undertook a post event review of the considerations and lessons learnt from February's invasion of the Ukraine by Russia.

In March 2022 the Asset Management iCOOC membership undertook a post event review of the considerations and lessons learnt from February's invasion of the Ukraine by Russia. Five months' later the summary framework of considerations born from this initial TTX was used to structure debate at a second TTX. This discussion was prompted by a heightened awareness of the emerging possibility of geopolitical contagion of the European conflict into APAC. Purposedly the hypothesis was not defined beyond an open-ended title, inviting the 'what if' from participating COOs and prompting debate as to theoretical consequences.

Geopolitical risk has been an agenda item for the CEO and C-Suite for many years, common practice being the C-Suite to be updated on the geopolitical landscape on a six-to-twelve-month cycle. These informative meetings were largely kept to the executive and in some cases, C-Suite minus one. In the room would be a global crisis management consultancy, whose business was the observation and evaluation of geopolitics, offering insights and prioritising the likelihood of events happening, and possible, consequent knock-on events.

In conversations with the COO community, it was clear little was done to take this information and share it downstream with the managing directorate, let alone the levels below. Therefore, even less was done to translate this data, geopolitical red flags, into a non-financial risk context. Business continuity (BCM) plans were the fall-back, the catch-all and foundation of operational resilience. Although, notedly, no BCM play book lasted the test of the first 24 hours of the pandemic and non either the Russian - Ukraine crisis.

Foresight In the spring of March 2021 iCOOC ran a buy-sell side forum, its agenda:

» What would the macro, micro and operational consequences be if Russia invaded the Ukraine?

Nine months later this theoretical debate and hypothesis moved from the what if to being real life.

At this debate the response was mainly that the COO is focused on today and the probabilities of tomorrow, with limited time or resources to contemplate the possibility of future events. Some referenced the industry was adept and had experience in the likely consequence, being sanctions, and as such preparedness of this possibility moving to probability to actuality, was arguably sufficient. This proved to be a significant underestimation, as eight months into the conflict the ramifications, the complexity, the variation of response and policy and their economic impact are yet to be definitively understood.

Operational Resilience the FCA appeared to have been gifted foresight, with its pre-war focus on developing organisational and operational resilience, as clearly little effective or meaningful work was done to prepare organisations and the industry to be able to meet the cacophony of events that unfolded, which moved non-financial risk into the domain of material financial risk almost seamlessly.

There has been, however, an increasing understanding and appreciation of non-financial risks. In a series of iCOOC forums undertaken from the summers of 2020 to 2022, the COO community has been engaged in an ongoing debate centred on the evolution and consequent need to manage and translate non-financial risk.

Within the taxonomy of this evolving risk category, the COOs concurred that very few had been actively engaged in the forward-looking assessment of the potential consequences of geo-political risk.

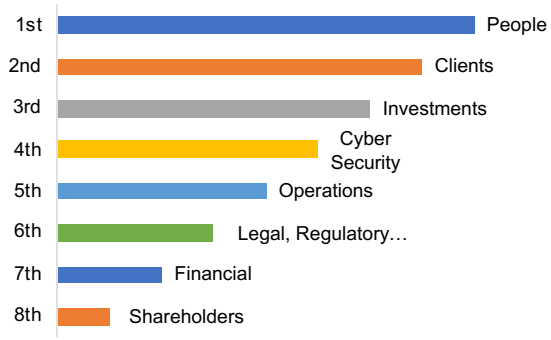
The focus was very much today, with operational and/or enterprise risk tasked accordingly in this context, but such allocation was not best equipped or directed to spend time and resources on real time risk assessment, less so emerging risks, perhaps the exception being regulatory matters, let alone undertaking horizon scanning.

What is understood now is the inter-relationship and entanglement of the non-financial family of risks. They feed of each other symbiotically.

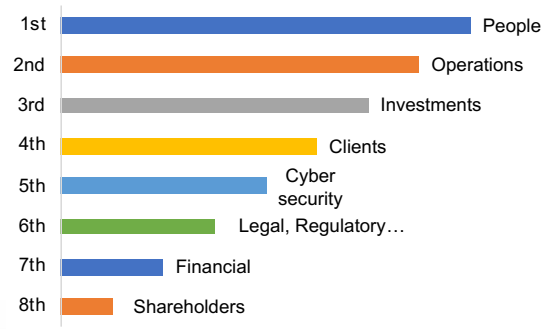
In this context, having a grasp on geopolitical risks, knowing their consequences can reach across regions, boundaries and dissect economies and the financial services that serve the global economy and society, will ensure each participant in the sector is better prepared and in doing so the sector will develop operational reliance to deal with the unforeseen.

TTX Comparisons

2021 geo-political event assessment priorities (in reference to the Russia-Ukraine conflict)



2022 geo-political event assessment priorities (in reference to APAC geo-political contagion and exposure)



At TTX 1 in March an on-line and live survey was undertaken by the attending COOs, asking them to prioritise resources and response to different factors. This same survey was undertaken in August at TTX 2, with time passing and an ability to look forward as to what your priorities would be with lessons learnt.

People remained the number one priority, whilst Clients and Cyber moved down the list of priorities, to be usurped by Operations. The Cyber threat did not materialise, or rather the work undertaken to defend the industry against this inevitability appeared to be money well spent (note: whilst the volume of cyber activity increased, many experts state its complexity did not).

Framework of considerations drawn from the TTXs undertaken March and August 2022

Considerations: Overlaying Russian Sanctions onto China.

Clients

- Significant relationships in the region and globally (impacts or liquidity needs)
- Interconnections of clients and relationships (global fragmentation, blocs of nations or clients)
- Communications (by client, client type, and region)
- Disclosures (data quality, timeliness, compliance, and selective disclosure risks)
- Coordination across client service teams, investment teams, and other business functions

Cyber Security

- Infrastructure
- Surge in attacks (e.g., malware, ransomware, DDoS, network attacks, zero-day vulnerabilities, and code flaw vulnerabilities)
- Vendors and fourth-parties (as above)
- Critical infrastructure (as above)
- Communication, awareness, and education

Financial

- Support for our people (travel, temp housing, relocation)
- Client service costs (added data, reporting, services)
- Loss of AUM and revenues
- Contractors and services (backfilled support)
- Third-party costs (added services)

Investments

- Exposures in the region and globally (direct, related, and contagion – consider supply chain)
- Trading (closures, circuit breakers)
- Counter-party risk (exposures, sanction impacts)
- Valuation (data and fair value determinations)
- Liquidity (market assessment, product status and client concentration data)
- Volatility
- Impact of sanctions
- Factor risks (energy, inflation, interest rates, fed responses and other geo-political (fragmentation and blocs))

Legal, Regulatory and Compliance

- Sanction monitoring, assessment, and compliance (initiatives across many jurisdictions – some coordinated, some not; breadth of targets – financial institutions, individuals and entities, and sovereign debt; and our global footprint – investing relationships, clients and eco-system)
- Client communications (see considerations in the clients section above)
- Disclosure and shareholder reporting (amendments to current and future disclosures)
- Regulatory reporting (as required by current rules and newly issued mandates)

Operations

- In the region (inventory; potential impact; concentrations; and alternatives)
- Nearby areas and global impact (as above)
- Service providers (as above)
- Extended enterprise (Fourth- and fifth-party providers - as above)
- Potential for other disruptions
- Impact of trading, counter-party, valuation, liquidity, volatility, sanctions, and factor risks on all activities
- Impact of regional outages globally (power, telecommunications, travel, connectivity)
- Interconnected or Cascading theaters of concern (regional concentrations or dependencies)

People

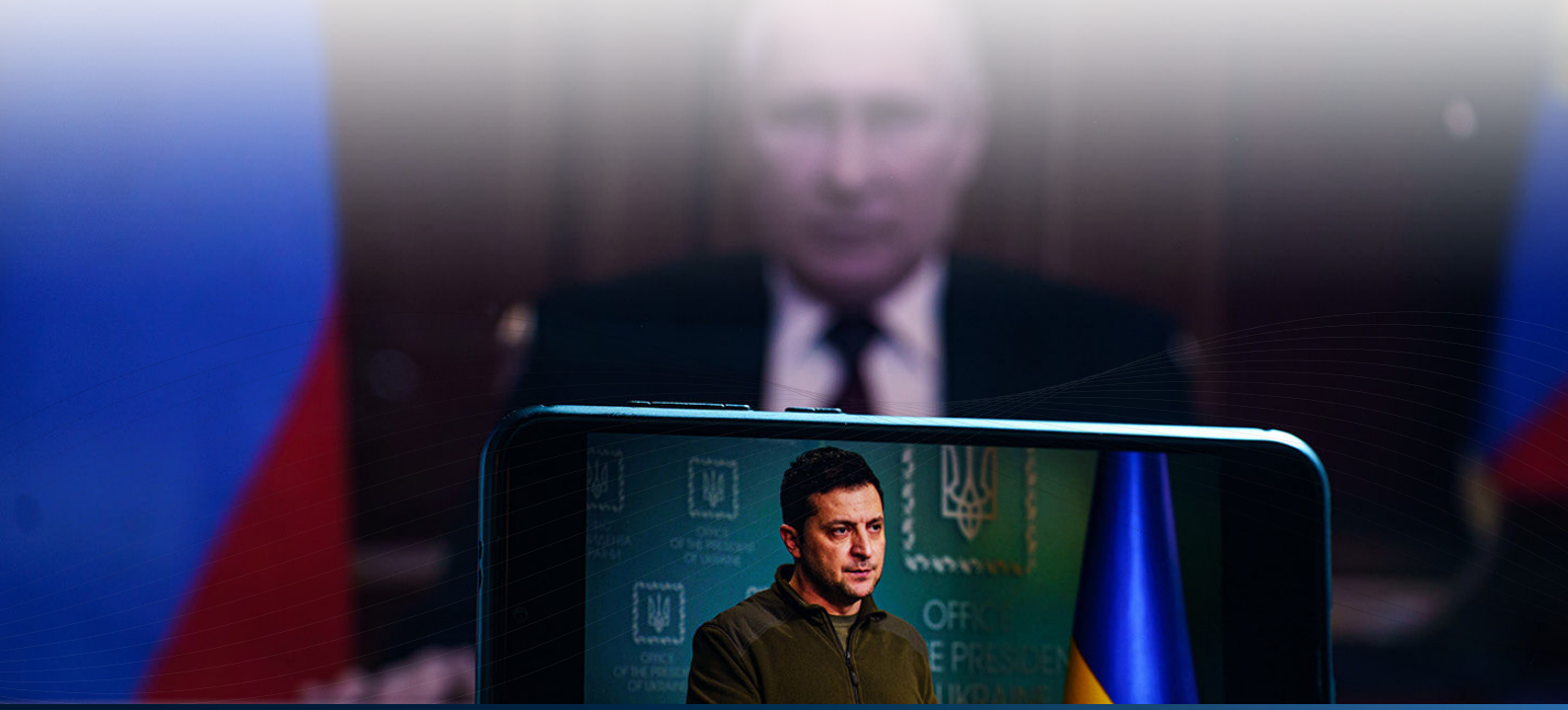
- Status of employees in all locations
- Direct impacts (well-being, availability)
- Indirect (e.g., family, refugees)
- Whereabouts and status of any travelers
- Interconnected or Cascading theaters of concern (regional concentrations or dependencies)
- Employee communications (tone, regional interpretations and sensitivities)
- Mental Health (cumulative impact of stress)

Shareholders

- Communications (messages, channels, velocity)
- Public policy (immediate expectations)
- Board communications (Corporate & Products)
- How might we be different than anyone else?

Considerations: Overlaying Russian Sanctions onto China

- 1. Legal entities in China and employees
- 2. First order effects
    a. China direct and indirect exposures (public assets and private assets (securities or physical assets)
    b. Fund suspension risks
    c. Capital controls
    d. Valuation and liquidity risks
    e. Stockconnect and trading channels
    f. Index delisting
- 3. Second order effects
    a. Market dynamics
    b. US treasuries
    c. Resource procurement
    d. Unintended consequences
    e. Unknown unknowns



Contact

Maurice Evlyn-Bufton
CEO, Armstrong Wolfe
maurice.evlyn-bufton@armstrongwolfe.com

Find us on LinkedIn: Armstrong Wolfe

Find us on LinkedIn: Women in the COO Community

ARMSTRONG WOLFE™