VERSPRITE

Political Risk

Typically a (negative) change in a firm's business or security environment within a country, that leads to negative effects on operations

Geopolitical Risk

Typically a (negative) change in a firm's business or security environment across borders, that leads to negative effects on cross border operations and supply chains

Examples of Political Risk

- New regulations/compliance requirements raising costs of doing business in a firm's home country
- Changes to corporate tax rates, etc Shrinking pool of skilled labor
- Anti-terror or anti-insurgency campaigns
- Natural disaster in a country where the government struggles to speedily restore vital services- water, power, Internet access, transit routes, etc.
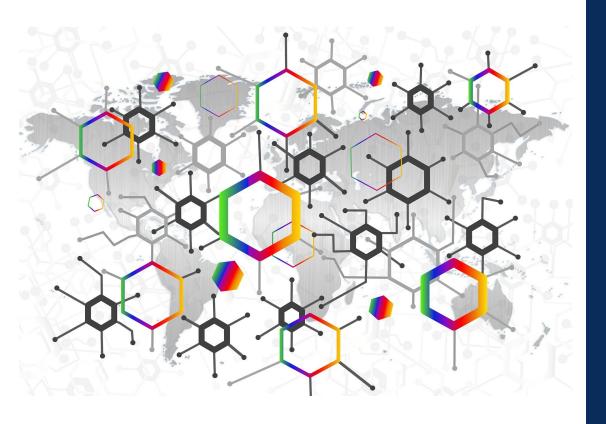
Examples of Geopolitical Risk

- Weaponized interdependence
- Cross-border violence or war
- Mass migration and refugee flows
- Competition from state-owned firms
- Changes to foreign investment codes, taxes, and rules
- New regulations affecting foreign businesses, or preferential treatment for local firms
- Foreign/adversarial intelligence service targeting of businesses

Geopolitical Risk and Business Continuity:
Top 5 Concerns for Executives

- Surveys of executives continue to indicate geopolitical risk and related issues - like regulatory and legislative changes - are consistently among the top 5 concerns for businesses.

- Over the last two years, major cyber attacks, as well as major natural disasters and infrastructure problems, catapulted concerns about business continuity to the top of executives' to do lists.

- Most business continuity plans are untested- never been practiced

Geopolitical Flux

- Political and geopolitical risk usually refer to negative consequences and externalities, but this insufficient

- To make (geo)political insight actionable and useful, we need to consider both negative and positive consequences, but especially positive changes that could lead to negative second and third order effects

- I use the term "geopolitical flux" where the focus is on the element of change, value neutral

The Nexus of Geopolitics and Cybersecurity

- Reputational effects of having poor security or being based in a country with cyber laws that ban encryption, require back doors

- IP theft and forced technology transfer

- Geopolitically motivated attacks/data thefts/intrusions

- Tariffs, embargoes, and sanctions that affect source code or ability to sell abroad

- Workforces protesting contracts with military or law enforcement agencies

- Technology empowering oppressive governments –tech used for censorship/targeting

- Issues of automation and job losses that exacerbate inequality and other social problems

- AI, deep fakes, and other technological advancements adapted for nefarious purposes-swaying elections, exacerbating ethnic or religious tensions, etc.

- Internet-connected infrastructure exploited by governments or attackers

VER SPRITE

Every Role Through a Geopolitical Lens

- Everyone should see their role through a geopolitical lens and understand the part they play in mitigating or exacerbating exposure

- Previously only the extractive industries worried about (geo)political flux – personnel safety and sunk costs in unstable countries with natural resources were the main concerns

- Now every company needs to understand that the data is collects and holds is valuable to a number of entities

  - Exercise/step trackers that revealed military bases

  - Ridesharing services which can reveal places people frequent, that could be used as blackmail in areas with repressive social policies

  - Online shopping histories that are used to calculate loyalty scores in countries like China

We Need Automation AND Action

ACTION in the form of interactive simulations will help us understand what to AUTOMATE:

- Evolution of how automation will change geopolitical balances

- Increasing complexity of supply chains

- Illusory solutions like misapplied or poorly implemented blockchains

- Inadequate security automation

- Geopolitical connections to, and effects of, automation

Interactive Simulations Help…

- Answer the question: What is the point of proposed automation?

- Identify which functions can be automated

- Explore the pros and cons of automating various functions

- Demonstrate the security vulnerabilities introduced by automating certain functions by considering a range of scenarios

- Ensure automated functions are regularly reviewed and modified to reflect changing circumstances

- Allow employees engaging with automated functions to experience possible problems and show them how they play a part in exacerbating/mitigating exposure to vulnerabilities

- Prevent the "I hadn't considered that" moment – they change minds

To Automate or Not to Automate...

Do automate:

- Identity and Access Management/Password Management
    - Onboarding, terminating

- Patching/Updating Software

- Primitive Threat Detection
    - Basic spam, malware, etc

- Data Protection

VERSPRITE

Definitely Do Not Automate...

Do not automate:

- Pen-testing/Social engineering attacks

- Continuous Testing and Verification - vendor and third party access and code

- Continuous Simulations and Training Programs - for employees of all levels

Overreliance on Automation

Dangers of overreliance on automation

- Misplaced trust - ceding our responsibility to be skeptical and trusting passes/uniforms

- Attackers finding low tech workarounds - social engineering with a crying baby to gain empathy and trust, causing someone to circumvent protocols

In Conclusion

- Bottom line - every company needs to have a Corporate Geo-Cyber Policy - like a foreign policy for your business, and this is best accomplished via simulations and other experiential learning tools to diagnose existing issues, analyze complex questions, and practice major decisions

- Once a firm has experienced the effects of geopolitical flux on operations, and how the firm's actions can mitigate or exacerbate exposure to geopolitical flux, creating the policy becomes an easier, better informed process