THE ONE WORLD, MULTI-EVOLUTIONARY PARADIGM

RISK MANAGEMENT IN DYNAMIC MARKETS

Ferndon Consulting

December 25, 2025

team@ferndon.com
https://ferndon.com

Executive Summary

One World: We are increasingly **inter-connected**, both in opportunity and in threat. This creates influence across diverse sectors which are inclusive of but not exclusive to: global and organic supply chains, communication, talent pools, security, regulatory compliance, and inter-state conflict.

Two Significant Evolutions: The **geopolitical** situation is increasingly complex in a world of international conflict, natural disasters, and intricately complex supply chains. Meanwhile, **technological evolution** is rapidly growing past policy and, often, even human conceptualization.

Three Critical Trends:

1. **Technology use**. Within a rapidly evolving world, transnational criminal organizations are increasingly using ***technology*** for money laundering, collecting personal information on high profile persons, and used to process mass quantities of information in an expedited fashion.
2. **Rapidly changing international policies.** ***Policies*** that affect trade, payments, legal authorizations, immigration, and even, dare we say, academic curricula are changing rapidly while loopholes and practices are used against us by criminals who know our restrictions.
3. **International Conflict and a Hybrid Threat.** State actors are engaging in non-attributional conflict through means of ***hybrid threat***, best understood as the simultaneous and complimentary use of conventional military action, governed by international law, and unconventional means, which are unregulated and often insidious, to bring about military objectives. Both Russia and China are targeting US critical infrastructure already, and, given the state of geopolitics, this is likely to increase.

Four Steps Forward:

1. **Use actionable fusion intelligence to chart a path through the storm**
2. **Embrace risk intelligently**
3. **Turning understanding chaos into advantage**
4. **Restructure both organizational and team resilience with a more grounded context**

Introduction

Executive leaders face a changing world, forcing them to make life-altering decisions for themselves, their companies, and their business partners. CEOs are now planning amid a perfect storm which includes rapidly emerging technologies, dynamically evolving compliance policies, and the wild card of geopolitics. Future projections built across decades and developed with fastidious attention to detail are becoming violently disrupted with daily geopolitical imbalances. Meanwhile, predicting the ultimate environment often feels to be more logical with a magic 8 ball opposed to any seemingly real reason or logic through conventional analytics.

A company's passage in this environment is rife with risk, but successful navigation means great potential reward. To survive the turmoil, executives continually need to both plan for both the natural continuation of that which we have known for years and, simultaneously, a very different reality.

There are ways to gain necessary knowledge and effectively navigate these storms, inclusive of bringing in outside advisors. Calls for organizations to add "Chief Geopolitical Officers" to their C-suites or highlight increasing concerns of geopolitical dynamics compounded by interstate conflict are gaining traction. Some organizations seek to broaden their organic navigational insight through focusing on CEO development or selecting a leader with greater geopolitical experience. Large firms are beginning to build fusion cells of SMEs with expertise in niche sectors to fuse their advanced cross-functional capabilities.

Moored ships get sunk, but navigating waves on your native lake is different from charting a safe path through the straits where seas connect. Navigating dynamic change becomes even more challenging in a geopolitical storm.

One World

Power is shifting internationally. Whether emerging powers aspire to unseat established leaders or historical powers work to retain their standing, conflicts emerge. We are observing the direct targeting of civilians and civil infrastructure in the recent Russo-Ukraine war, and we know this is an embraced technique by many militaries to intentionally undermine their adversary's morale and disrupt their supply lines. This does not just affect the contending states in our interconnected world; we feel even the most indirect impacts from attacks on Polish railroads and Ukrainian ports, tariff pendulums, monopolization of certain rare earth minerals, extreme weather events, and even "traffic jams" or "water depths" of the Suez and Panama Canals.

Two Significant Evolutions

(1) To navigate these changes, *nuanced and actionable understanding* of **geopolitics** is an absolute necessity. Geopolitics, in this context, refers to more than just international relations and power plays among hegemonic actors. Geopolitics is a constantly evolving nexus of geography (inclusive of weather and climate), culture, international relations, and even power. Studying geopolitics is increasingly complex by hegemonic world views and cultural values differing, creating discrepancies of understanding and alignment.

(2) To apply these evolutions, *practical understanding* of **technological evolution** is imperative. Burgeoning threat vectors in generative and agentic Artificial Intelligence could potentially disrupt supply chains in ways we do not yet understand. As owners and operators adopt more technically dependent approaches to managing operations, attacks and vulnerabilities will increase. Given the interconnectivity of systems, access points for threats, vulnerabilities, and error have compounding and cascading effects.

Three Critical Trends

(1) Technology is rapidly advancing and affects planning in many ways. Supply chains are a complex interaction between enterprise information technology (EIT) and operational technology (OT),[i] each of which has its own unique security challenges. Artificial Intelligence (AI) is rapidly growing in use and popularity, and large language models (LLM) are rapidly integrating more information through any public facing use by individuals and organizations

whose material is now in the "big brain" data centers. While it is also possible that agencies could create or manage an in-house LLM for bulk processing, all LLMs are subject to hallucinations, data corruption, or even less qualified programming which then lead users to insufficient conclusions.[ii] Critical infrastructure and the energy grid, especially, have a particular concern with the trend of hallucinations or data corruption. The system is so vast with multiple generations of technology, they have a complex layering system with multiple access points, that penetration and damage is comparatively easy. Timed with a weather event (like an abnormally hot summer or a cold winter) there will be devastating effects on critical infrastructure supporting government and commercial entities.

(2) Policy change, both in a state(s) of operation and along a supply chain, will drastically affect risk, profit, and survivability. In the US, recent policy changes by executive order alone are especially extensive warranting entities to implement robust tracking mechanisms. The changes in regulatory compliance for finance, trade, communication, biometrics, immigration, air pollution, and DEI are producing unexpected secondary and tertiary effects.

These policy changes have secondary and tertiary effects that are challenging and becoming increasingly more difficult to predict. Some sanctioning policies are spawning advanced persistent threat groups to act in retaliation to those policies, as shown through the Russian cyber-attacks on US critical infrastructure in 2018.[iii] This was the first publicly acknowledged of many such attacks. Other times, policies of other countries indirectly affect us: China has passed financial policies whose requirements encourage circumventing and, so, encourage illicit movement. Other policies, such as China related financial policies, make money transactions more challenging for Chinese illicit finance organizations. These policies correlate with the rise of illicit money movement through criminal organizations, funding and bolstering international criminal activity.[iv] Still other policies, such as the increased use of and deregulation of cryptocurrencies, are purportedly affecting the increase in ransomware attacks.

(3) The **Hybrid Threat** is that gray space between hard and soft powers. The impact of inter-state conflict is something many executives understand conceptually, but effective integration of this understanding is internalized for effective forward planning usually after one has been burned. While this is more a sector for military and foreign policy experts, it is becoming increasingly important for non-governmental executives to understand implications and threats due to rising whole-of-society response to counter-hybridity. Conflicts are rapidly devolving from traditional force-on-force hard power applications of diplomacy and opting for softer, non-attributional instruments that complement critical infrastructure and supply chain degradation. The two primary threats discussed lately are China (PRC) and Russia. While both engage in indirect means of conflict, their approaches are different, and effective planning often ties back to hybrid geopolitical contexts within the competition continuum of soft to hard diplomacy.

Chinese doctrine emphasizes two key take-aways. First, China prefers avoiding direct confrontation – a hot war, if you will. Second, the PRC emphasizes a "whole of nation" approach to "all domain warfare" within which anything that is Chinese can be considered an asset. This, theoretically, can include but is not exclusive to organizations, companies, ports, formal state resources, human beings, and banks. Central to the Chinese emphasis on all-domain warfare is "systems confrontation" wherein the Chinese Military would seek to neutralize enemy systems with special emphasis on communication systems, logistics functions, intelligence systems (and their affiliated resources), and information systems.[v] Recent PRC-sponsored attacks on Agentic AI systems challenged many defenders: they were simply unable to predict what would happen next or what the ultimate impact of the attack would be because, unlike typical cyber-attacks, this involved the dynamic use of Agentic AI, and these agents were able to access information and rewrite source code without *any* human interaction or prompting.[vi] Further, Mexican drug cartels use Chinese criminal groups to launder money from the sale of fentanyl in the US. It is not uncommon for this fentanyl or its ingredients to originate in China or come through Chinese entities. These transactions benefit the end game by simultaneously providing increased pressure on the US medical and law enforcement sectors while also providing increased financial resources to China. It does not stop here: in "all domain" economic warfare, critical minerals, supply chains, and components are a few of China's many prospective weapons.

Russian approach to warfare is more transparent from watching their fight with Ukraine (2014-?). Russians do not prioritize avoiding "collateral" damage, as seen by repeated strikes against sites most would consider protected (schools, hospitals). Russians actively target critical infrastructure during both cold and hot wars, and they intentionally maximize impact through aligning attacks with weather trends. Russia was attacking Ukrainian infrastructure even before invading; attacks just intensified in 2022. On December 12, 2025, Russia cut off power, water, and heat to one million Ukrainians:[vii] they continue targeting Odessa's infrastructure to cut Ukraine off from the Black sea, affecting the food supplies shipped out of Ukraine, port infrastructure, and civilian population.[viii] The Russians are already targeting US infrastructure. Since March 2016, the Department of Homeland Security and the FBI collectively advise us that: Russian government cyber actors were *targeting* US critical infrastructure sectors, including energy, nuclear and commercial facilities.[ix] Their activities are only increasing,[x] and in December 2025, reports are emerging stating that the Russians have been *exploiting* US critical infrastructure since 2021.[xi] To maximize impact, and consistent with Russian hybridized operations, Russian "information operations" cover a broader scope than previously understood by US intelligence organizations. Russian "Information Operations" focus on destabilizing, sowing chaos, and undermining adversary's social cohesion using a holistic, pervasive, and often covert approach (disinformation, cyberattacks, propaganda). The US national, state, municipal, and even commercial cyber defenses struggle with speed against Russia's intentional, integrated, persistent, and often brazen methods that exploit existing societal divisions.[xii]

Four Steps Forward

(1) Use actionable fusion intelligence to chart a path through the storm

Leaders make decisions, and leaders' understanding is accumulated and shaped by time and experience. Intelligence augments the changing landscape to support the decision-making process. The intelligence process is not an accumulation of information from as many sources as possible in as rapid a manner as practical. It is an intentional digestion and focusing of details to answer the key questions in a manner that elucidates actionable insight needed by leadership to make a specific decision at Decision Points. Decision Points are those places where a leader needs to choose between two (or more) potential paths. Actionable intelligence creates a maximized context of the known, likely (templated), and unknown situational nuances which then enable those decisions at each Decision Point.

Fusion intelligence contributes to a more accurate and complete understanding of the operating environment, including the organizations' internal strengths and weaknesses and its external opportunities and threats from political, economic, social, technological, environmental, and competitive factors. It is not just compilation of insight from various sources: it is a process within which one creates an intentionally multi-dimensional understanding of a complex context using insight from as many perspectives as possible. The most egregious failures of intelligence have often been aligned with insufficient intention in (1) processing the information into actionable intelligence, (2) focus on a single intelligence stream, or (3) comfort with the status quo of understanding wherein the analysts stop looking for the unseen and are dependent on that which is fed into their systems.

(2) Embrace risk intelligently

A robust and effective risk management framework can be a competitive advantage, and this is where actionable fusion intelligence shines. The dangers of relying on bulk-processing of more data and the growing dependency to optimize said tasks with AI poses different challenges and a potential paradigm shift. AI LLMs have come a long way from 2021 to 2025. Not just LLM creations, but the capabilities of Agentic AI to find more contextually significant information using Model Context Protocol. But LLMs still do suffer from hallucinations, and these hallucinations can have adverse effects on affecting policies based on AI queries.

Good risk governance ensures that strategy and culture support purpose and vision; that risk appetite is clearly articulated and upheld; and that decisions, resources, and actions remain aligned to strategy and are within risk appetite. Effective reporting ensures that decision-makers will remain well informed. Successful policies and procedures provide organizational guidance in the execution of strategy, within cultural expectations, and in the management of

risk. Effective processes, systems, and tools enable organizations to follow procedures within policy more consistently and more efficiently. Well-understood accountability and adequate capability and capacity enable success. A strong risk culture is the glue that holds the framework together, can cover gaps in the framework, and generally makes the management of risk more effective and more efficient.

(3) Turn understanding chaos into an advantage

The executive who can successfully navigate their course through a storm has a greater chance at profit than those who stay in a port or those who launch into the ocean armed with good intention and robust passion. Effective navigation includes assessing one's strategy, culture, and risk management frameworks in relation to the currently evolving geopolitical environment. As an example, we are all affected, either individually or tangentially, by the global supply chain. Successful management of global supply chains are increasingly relying on interdisciplinary understanding of geopolitics, policy evolution, and even the technical fusion of mathematics, data analytics, AI, OT, and EIT security. Sometimes one knows the route: at other times, maps, navigators, or a guide can be found. When one effectively navigates these niche fields, they gain a clear advantage over the competition.

(4) Restructure both organizational and team resilience to be more grounded

Grounded leaders build and execute a strategy to fulfill their purpose and realize their vision within their dynamic context. They plan for and drive the most impactful actions to meet strategic objectives, including understanding and managing risk. Effective leaders are grounded in purpose and values. They lead people with passion to fulfill that purpose and to live those values. People and organizations are most effective and efficient (including managing risk) when they are 'purpose-full' with aligned values. Furthermore, grounded leaders communicate a compelling vision of what it looks like when they and their organization are fulfilling their purpose. They build strategy, make decisions, and take actions that will realize their vision.

With this grounding, both leaders and organizations become increasingly resilient. The next generation of leaders also becomes a developing beneficiary through empowerment and mentorship. As we face a dynamic environment, different generations, and those from different world views, can capture different opportunities. Cross-organizational collaboration within a company, integrating various perspectives into wargaming, and even enabling the "shadowing" of rising leaders with current leadership will have compounding positive effects. Not only will the younger leaders feel valued, involved, and seen, but also their different perspectives can create a better contextual understanding for executives.

Contributions

Ferndon Consulting LLC
team@ferndon.com
https://ferndon.com

Contributing Authors

- Dr. Dawn Hersey, Chief Executive
- Dr. Thomas Winston, Director of Cyber/Technical Analytics
- John Hart, MBA, Director of Executive Risk Management
- Prof. Suzanne Lynch, Director of Counter-Threat Finance
- Thomas Brown, MPA, Director of Research and Policy Analysis

Information

Information cut-off date: December 20, 2025

Material contained in this paper has no distribution restrictions.

Works Cited

[i] Hattar, I. Z., & Felföldi, J. (2024) *Impact of Information Systems in the Supply Chain: A Systematic Literature Review*. Applied Studies in Agribusiness and Commerce, 18(1). https://doi.org/10.19041/apstract/2024/1/3

[ii] Kane, A. T., & Baily, M. N. (2025) Harnessing AI for economic growth. Brookings. https://www.brookings.edu/articles/harnessing-ai-for-economic-growth/

[iii] CCISA. (2023) *Russia Cyber Threat Overview and Advisories | CISA*. Www.cisa.gov. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia

[iv] U.S. Treasury (2024) *2024 National Strategy for Combating Terrorist and Other Illicit Financing*. https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf

[v] Sullivan, Ian (2025) *How China Fights in Large-Scale Combat Operations*. https://www.army.mil/article/285395/how_china_fights_in_large_scale_combat_operations

[vi] Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for Cyber Attacks. Journal of Information Security and Applications, 57(57), 102722. https://doi.org/10.1016/j.jisa.2020.102722

[vii] Maxim Volovich. (2025) *No power, no heat, no water: How a city of 1 million survives when everything stops - Euromaidan Press*. Euromaidan Press. https://euromaidanpress.com/2025/12/15/odesa-blackout-russia-attack-december-2025/

[viii] Gozzi, L. (2025) *Russia escalates attacks on key Ukrainian region of Odesa*. https://www.bbc.com/news/articles/cdxe8yqlvgzo

[ix] *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations | Senate Select Committee on Intelligence*. (2016). Senate.gov. https://www.intelligence.senate.gov/2018/05/29/publications-russian-targeting-election-infrastructure-during-2016-election-summary-initial-findings/

[x] CISA. (2024) *Russian Military Cyber Actors Target US and Global Critical Infrastructure | CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

[xi] Sead Fadilpašić. (2025) *Amazon says Russian hackers behind major cyber campaign to target Western energy sector.* TechRadar. https://www.techradar.com/pro/security/amazon-says-russian-hackers-behind-major-cyber-campaign-to-target-western-energy-sector

[xii] *U.S. vs Russian "Hybrid Warfare" Doctrine: A Comparative Glance*. (2024) Grey Dynamics. https://greydynamics.com/u-s-vs-russian-hybrid-warfare-doctrine-a-comparative-glance/