Teneo | TAG CYBER

Teneo Cyber Insights: A New Series for CEOs

# The Linkage Between Geopolitical and Cyber Risk Requires CEO Attention Now More Than Ever

Teneo Insights / April 2023

**Unfortunately, and out of necessity, organizations have accepted cyber risk as a cost of doing business. For years, business executives have repeated the mantra "it's a matter of when, not if" in reference to cyber-attacks. But the range of motivations for cyber disruption has evolved and geopolitics has become an increasingly more important part of the risk equation.**

Some of the most high-profile attacks over the last several years have been financially motivated, as evidenced by the surge in ransomware events. Others, however, have been the handiwork of sometimes teenaged hacktivists looking to prove their technical skills, as was seen in the 2022 Tesla, Samsung and Microsoft breaches. CISOs and cybersecurity executives have been keenly aware of and attuned to monitoring for these types of threats, which are largely random in nature. Bad actors are constantly scanning global networks in search of vulnerabilities, regardless of the company, sector or executives. Many threat actors also do their homework, honing in on companies that are perceived to be a "rich" target, meaning they appear to have the revenue and thus the motivation to make a ransom payment if the disruption or reputational hit is painful enough. More recently however, events like the Russia – Ukraine war have significantly amplified the need for CEOs and their executive teams to plan and prepare for the interconnected challenges presented by today's geopolitical and cyber risk.

The term "geopolitics" has been around since roughly the turn of the 20th century, and most experts claim that the topic of cyber risk dates back to the 1960s and 70s with the birth of the term "hacking" and the development of a project called The Advanced Research Projects Agency Network (ARPANET). Despite their relative proximity, both types of risk emerged over time in relative isolation to one another. That is no longer the case, and geopolitical motivations are just as important a consideration in the overall cyber risk assessment equation for global businesses. In the early days of cybersecurity, the primary motivation of hackers was simply mischief. Defaced websites and simple computer viruses were common exploits and such acts of cyber vandalism had no serious geopolitical implications. At that time hackers were mostly teenagers and one could argue that their work actually helped to expose troublesome software bugs.

The progression in cybersecurity from such innocent beginnings to the present day includes a significant rise in nation-state involvement in offensive threats. As a result, an irrefutable linkage has emerged between geopolitics and cybersecurity. This linkage demands convergence and interdisciplinary coordination between technology experts and geopolitical experts defining policy and negotiating with both allies and adversaries.

In this brief note, we outline the business challenges that emerge from this specific connection between geopolitical and cyber risk. Our focus is on how corporate executives and leaders should view and manage this new and interconnected risk and how it should influence global business decisions. This is particularly important in the context of work being done in a country that might be viewed as an adversary, as well as in business sectors that might face potential increased vulnerability.

## What is the Cyber Risk from Nation-States?

Nation-state cyber risk arises from the objective for certain countries to establish dominance over their adversaries. This includes the development of offensive capabilities that allow one country to target the assets and infrastructure of an adversary. Such offenses usually stem directly from the military, which implies that the capabilities are advanced and effective.

The challenge that arises for business executives is that while the offense is military-controlled, the defense must come largely from the private sector. As one might expect, the targets an adversary selects to attack will include the data, systems, services and infrastructure that societies depend on. Such assets are owned and operated by industry. Telecommunications, the banking industry and power are key examples of critical infrastructure sectors that are frequently targeted.

The resulting cyber risk is tough to manage, if only because of the asymmetry between powerful offensive teams targeting often inadequately trained and/or poorly funded IT security teams that were primarily created to manage compliance and deliver basic IT security. This helps to explain why companies continue to experience successful hacks such as ransomware, as well as why certain critical infrastructure sectors like oil and gas have proven to be relatively immature in the cybersecurity realm.

Corporate executives and boards commonly express frustration that security budgets continue to rise without the commensurate reduction in cyber risk one might have expected. The nation-state origin of most attacks, including financially driven attacks such as ransomware, helps to explain why cyber budgets remain on the rise and why cybersecurity continues to be such a challenge.

## How Do Cyber Threats Influence Geopolitics?

Since advanced cyber threats clearly involve the crossing of political boundaries, it should come as no surprise that many countries are beginning to develop cyber-related negotiating strategies as a component of their geopolitics. The idea is that cybersecurity is a new poker chip in the negotiating game, with diplomats now commonly bringing up the question of whether an adversary is hacking.

**It should come as no surprise that countries are beginning to develop cyber-related negotiating strategies as part of geopolitical risk mitigation.**

Consider, for example, the role that cybersecurity plays in the geopolitics related to the Russian invasion of Ukraine. It is well-known that the Russian military has targeted Ukrainian infrastructure, including serious cyber-attacks on the telecommunications network and power grid. Disinformation has also been used to obscure the source and motivation of such attacks.

The Ukrainian military has coordinated its defensive response with assistance from many allied countries, vendors and experts around the world. Many observers have noted that Ukraine has been largely successful in avoiding major consequences, but it would seem too early for anyone to declare that Ukraine has ultimately been successful.

The implication is that cybersecurity has become intertwined with conventional geopolitics in a way that causes cyber offensive and defensive tactics to become part of most negotiations. The United States and China are perhaps the most powerful global cyber players and one must expect that ongoing negotiations between the countries can and must include cyber.

## Should Executives Have a Geopolitical and Cyber Risk Action Plan?

The implications of this geopolitical cyber risk on businesses are greatest when an organization has business interests in a region where an active cyber conflict is ongoing. The war in Ukraine, for example, has prompted many business leaders to review their supply chain, with emphasis on ensuring that proper cyber defense is in place where dependencies might exist.

Organizations may also find themselves in the crosshairs of a foreign adversary because of geopolitics stemming from alliances even if there is no direct business operation in that adversary's country. The most obvious example of this would be again the Russian invasion of Ukraine and the concerns of NATO ally countries becoming secondary critical infrastructure targets. Increasing tensions between China and Taiwan, which serves as a significantly geostrategic country to the rest of the world, and U.S. domestic trade strategies and incentive programs like the CHIPS Act further exacerbate and highlight the interconnectedness of geopolitics and the potential for significant cyber disruption as a tool for foreign adversaries.

The interconnectedness between geopolitical and cyber risk becomes increasingly more important in the context of work being done in a country that might be viewed as an adversary, as well as in certain industry sectors. Critical infrastructure has proven to be a target where cyber-attacks are one strategy in a geopolitical standoff. That said, it would be imprudent to assume that the cyber risk diminishes if the business is not in a critical sector such as energy, telecommunications or defense. The complexity of supply chains highlights the domino effect when one link in the wider chain is impacted.

The longer-term issue for business leaders is that geopolitics will become increasingly complex as more countries develop advanced offensive capabilities. In addition, cybersecurity does not have the physical boundaries one finds with conventional warfare. As a result, the possibility is high that geopolitical unrest in one region could cause serious cybersecurity implications in a completely different area.

Corporate action plans should be in place that include contingency plans, supply chain diversification and accurate monitoring of geopolitical risks. Technical strategies should include measures designed to distribute assets and tighten security controls. Seasoned crisis management partners will help companies develop crisis response plans and support testing readiness to manage geopolitically oriented cyber issues.

These are not, however, activities and responsibilities that should be allowed to operate as separate taskings within organizations. CEOs and boards should be prioritizing strategic risk assessments which examine business exposure to current and emerging geopolitical risk and in the context of potential cybersecurity vulnerability.

**Corporate action plans should be in place that include contingency plans, supply chain diversification and accurate monitoring of geopolitical and cyber risks.**

Scenario planning exercises and simulation drills at the executive level are no longer a "nice-to-have." We know that foreign adversaries are capitalizing on sophisticated cyber technologies to inflict harm – the last several years brought the world events like Solar Winds, Colonial Pipeline and Kaseya – yet only recently are we seeing CEOs and boards putting actual structures in place and making concerted efforts to mobilize executive teams around this type of interconnected geopolitical and cyber risk identification, management and mitigation. Each executive brings the point of view and domain knowledge from her/his area of the business. The collective power of their analysis will help highlight potential vulnerabilities and geopolitical risk exposure so that the CEO can build and maintain a more resilient organization.

# Authors

**Ed Amoroso**
**Senior Advisor, Teneo**
CEO TAG Infosphere, Inc., Research Professor, NYU and Senior Advisor to Teneo Risk

**Courtney Adante**
**President, Teneo Risk Advisory**
Teneo Cybersecurity Client Lead and Cyber Crisis Management Advisor

Teneo®
The Global CEO Advisory Firm

## Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions, and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

**teneo.com**

---

## About TAG Cyber

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 500 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth guidance, market analysis, consulting, and personalized content based on thousands of engagements with clients and non-clients alike—all from a practitioner perspective.

**www.tag-cyber.com.**