KCS Group Europe

The New Cold War

March 2024

In the evolving network of global relations, a New Cold War landscape has emerged, marked by intensifying geopolitical tensions among the world's major powers. The United States, the European Union and their allies, find themselves in an increasingly complex standoff with nations like Russia, China, North Korea and Iran. This modern Cold War, unlike its mid-20th-century predecessor, unfolds in the shadows of cyberspace and the boardrooms of global commerce, where espionage, cyber warfare and social engineering blur the lines between statecraft and the corporate world.

Within this theatre, internationally traded businesses are inadvertently becoming frontline actors in this full-scale clandestine war. Espionage activities not witnessed since 1947 (the first Cold War), that would not be out of place in a spy novel, now attack all manner of corporate entities and governments. The goal is to retrieve trade secrets commonly referred to as Intellectual Property (IP) and sensitive information. The world’s superpowers are now all hungrily vying for global dominance.

Cyberwarfare cases have grown exponentially, with reports of state-sponsored hackers stealing, sabotaging and causing reputational damage, becoming daily events in the media. Social Engineering, the very human face to face engaging tools of secret service intelligence gathering units globally, has also seen a resurgence.

In this new Cold War environment, businesses are navigating a minefield of risk, from competing businesses to unfair market conditions, to secret government operations looking to service their own specific requirements and interests. There has never been a time like this where there is such a necessity for vigilance and counter measures to protect corporate interests and reputation.

The Invisible Frontlines: Espionage and counter-espionage

The frontlines of this modern-day Cold War are not declared by boundaries or armed fortifications, they are, in fact, integrated into international business operations. Secret Service shadow warfare and intelligence, and espionage operations, regularly enter the corporate sector. The effects of these activities for businesses can be profound, causing havoc for decision-making and international partnership ventures. A company could find itself engaged in espionage activities, with their resources and networks being exploited by state-sponsored intelligence operations, without even knowing.

KCS Group Europe (KCSGE) is aware of many espionage operations masquerading as regular business operations. In this hypothetical entity example, a business offering consulting, technology development and guidance, or even trade facilitation lines, could be a front to help operatives gather intelligence under the veil of legitimate commercial activities. The current uncertain geopolitical atmosphere serves as an optimum breeding ground for covert intelligence operations to continue without arousing suspicion.

Money Trails: Laundering, fronts and the global economy

The lines between legitimate business and illicit activities are often conveniently blurred, especially when laundering money is concerned. Small enterprise or multinational corporations can be established purely as fronts for processing money for governments and organised crime groups (OCG's). The sectors KCSGE has identified as most vulnerable to this practice include real estate, luxury goods and financial services, as large transactions are commonplace here and can be disguised. The vast amounts exchanged within these business sectors, and the sophisticated methods used by the perpetrators, can often see money flowing between several jurisdictions, making investigations complex. Research has revealed that legal and accounting sectors often storing client IP are also susceptible to attack, due to insufficient safeguards.

Undercover intelligence gathering operations

Case studies

USA - NSA Hacking for UAE Monarchy – Project Raven - 2016

Project Raven saw several US NSA analysts being deployed in the Middle East to hack and monitor for an Arab monarchy. They were tasked with engaging in the surveillance of neighbouring governments, militants and rights activists against the royal family. The NSA team were stationed in Abu Dhabi, in a building referred to as "the villa", where they hacked into phones and computers of specified targets. Project Raven did manage to help the UAE's National Electronic Security Authority (NESA) break up an ISIS network responsible for stabbing a teacher to death in Abu Dhabi in 2014. One operative complained and felt uncomfortable when Project Raven merged with a private UAE Intelligence firm called Dark Matter. The agents found themselves targeting US citizens state side and this did not sit well with the team.

China - Global covert police stations – 2023

China came under scrutiny from international law enforcement following the FBI's arrest of two Chinese Americans operating an illegal police station in China. This single operation led to the revelation of over 102 stations in 53 countries, as identified by a Pan-Asian Human Rights NGO called Safeguard defenders. These stations have been implicated in activities viewed as transnational repression, like surveillance and harassment of dissidents living abroad, looking to pressurise them to return to China. These clandestine operations have proven very difficult to link to the Chinese government.

Russian operations in Poland/Hungry/Slovakia/Lithuania – 2023

In 2023, sanctioned Russia managed to acquire sensitive technology from EU companies to supply critical technology to a Russian military-industrial complex. The networks' purpose was to purchase equipment from microchips to ammunition on behalf of the Kremlin. This sanction evading vehicle was able to acquire machine tools from Germany and Finland with little resistance. The "Serniya Network" was accused by the US Department of Justice of being involved in sensitive and classified procurement activity for Russia's FSB intelligence agency, to include the Directorate for Scientific and Technological Intelligence, also referred to as "Directorate T".

This cell's ability to operate hidden among civilian commercial businesses in Europe acting on behalf of sanctioned Russian intelligence, illustrates the risks and complexities of trading in this era of Cold Warfare.

Iran

The Islamic Revolutionary Guard Corps (IRGC), a dominant force in Iran's politics, has become a business empire since the Iran-Iraq war when it was suggested by then President Rafsanjani's government that the IRGC be used for economic undertakings to fund its activities. It now controls businesses in oil and gas, construction and telecommunications. The IRGC has a huge commercial facing front which has brought with it concerns of Western firms conducting business linked to sanctioned terrorist organisations.

A case worth noting occurred when the Trump Organization got involved in a construction project in Azerbaijan. In 2012, contracts were signed to build a skyscraper in Baku with the Mammadov family group. Called The Trump Tower Baku, the project came under fire with accusations made in 2017 suggesting that the deal was a money laundering operation for the IRGC. The Mammadov family had previously awarded contracts to Iranian construction firm Azarpassillo, who are allegedly controlled by the IRGC. No hard evidence surfaced, and all officials were cleared of acting illegally. However, questions were raised about the possibility of future Western partnered construction project revenues falling into the hands of the IRGC.

Data Mining: The role of social media in modern espionage

For some time, social media platforms like X, Facebook, WhatsApp, TikTok and Google have been resourceful tools in gathering intelligence for profiling and delivering malware payloads for surveillance monitoring. Businesses have good reason to be significantly concerned about data security, privacy, and distribution of sensitive information.

Navigating the Minefield: Strategies for business survival

As businesses begin to accept the existence of the new Cold War environment, they must navigate the landscape with caution and be aware of the warning signs.

There has never been a greater need to employ independent intelligence gathering specialists capable of providing insightful analysis on existing threats and opportunities. By being notified of cyber-attack trends and counter-espionage operations, as well as employing vigorous vetting processes to defend against espionage, businesses can establish necessary levels of operational continuity. In establishing these defences, businesses can be better prepared for unforeseen obstacles.

Conclusion: The path forward in a divided world

The new Cold War era depicted by cyber skirmishes and tactical espionage means governments and businesses face complex challenges. The new modern day conflict landscape of cyberwarfare and intellectual property theft, coupled with the social engineering tactics of old, requires a greater breadth of intelligence resources and heightened vigilance. The lines are evidently blurred between legitimate commercial enterprise and clandestine operations, in particular, those sectors prone to money laundering.

From a macro perspective, the symbiotic nature of these superpowers is evident, when one economy suffers, they all suffer. The elite nations know that they actually need each other. This juxtaposition of evading sanctions and breaking international laws, conducting Cold War clandestine monitoring and disinformation operations, as well as cyber theft and attacks, yet still demanding free trade conditions and wanting to experience growth, appears a farcical dichotomy. The superpowers must ask themselves, are you at war or aren't you? You cannot have both, and more to the point, why would you want to?