Nasdaq

Geopolitical Tensions and Cyber Threats: Potential Consequences of U.S. Tariffs

June 2025

Ilaria Sangalli, *Index Research Lead*

Navigating uncertainty: the impact of U.S. tariffs on global trade and cybersecurity

On April 2, the U.S. announced levying tariffs on its largest trading partners. Following the announcement, the average effective U.S. tariff rate increased from 2.5% to 27%, representing the most significant increase in nearly a century.[1]

The tariffs signaled a potential escalation in trade wars, particularly with countries like China, Canada, and Mexico. This development prompted concerns among investors regarding possible retaliatory actions, which could further impede global trade and economic growth. Furthermore, trade tensions may incite retaliatory measures from nation-state actors, encompassing cyber espionage and cyber-attacks. These threats have the potential to compromise both governmental and private sector entities.

In addition to increased cyber risk, companies now face the prospects of increased costs and logistical challenges as supply chains may have to adapt to the newly imposed trade barriers.

The 90-days suspensions announced on April 9, the trade deal with the UK on May 8, and the provisional agreement with China on May 12 prompted a market rebound. However, despite the recent trade agreements and temporary tariff pauses, companies continue to face significant uncertainty. The provisional nature of these measures makes it premature to fully understand their impact. Businesses remain cautious about making substantial changes to their supply chains, opting instead to await more stable and predictable conditions. This caution is further intensified by the complexity of supply chain adjustments and the potential for new cybersecurity vulnerabilities to arise.

Rise in politically motivated cyber-attacks exploiting geopolitical tensions and tariff disputes

In an era marked by escalating geopolitical tensions and sophisticated cyber threats, nations across the globe face unprecedented challenges to their security. Europol's[2] latest report unveils a concerning rise in state-sponsored hybrid threat actors targeting the European Union, via "shadow alliances" with criminal gangs. These actors employ a range of destabilizing tactics like cyberattacks, data theft, disinformation, and sabotage of critical infrastructure. According to Europol, the current geopolitical climate provides opportunities for these actors to exploit vulnerabilities and spread disinformation.

[1] https://www.politico.com/news/magazine/2025/04/10/tariff-reality-check-trump-retreat-00285270
[2] European Union Agency for Law Enforcement Cooperation, is the EU's law enforcement agency. Europol's mission is to support EU member states in preventing and combating serious international and organized crime, cybercrime, and terrorism.

While the report does not explicitly label Russia as a hybrid threat actor, it implies that activities from this region align with hybrid threat tactics: "There is an increase in politically motivated cyber-attacks against critical infrastructure and public institutions, originating from Russia and countries in its sphere of influence".[3,4]

In response to this, the European Commission plans to strengthen security protocols to counter sophisticated cyberattacks and intends to double Europol's staffing and funding. This strategic move is expected to boost cybersecurity spending across both public and private sectors, driving the demand for cybersecurity products, services and advanced threat detection solutions.

The rise of cyber operations closely linked with geopolitical tensions have also been identified as a key trend in recent years by Microsoft in its Digital Defense Report 2024. According to the report, cybercrime gangs are collaborating with nation-state groups, exchanging tools and techniques to advance their goals. This partnership has resulted in major cyber incidents worldwide, involving not only actors from Russia, but also from China, Iran, and North Korea.

Microsoft has also detected a rise in election-related homoglyph domains, in the lead-up to the last U.S. presidential election. These are fraudulent links that closely resemble legitimate ones, crafted with the intent to deceive users. These domains are used to deliver phishing attacks and malware, which can steal information or damage systems. According to Microsoft, the activity behind these domains is driven by both cybercriminals seeking profit and nation-state actors pursuing political objectives.[5]

In light of recent tariff tensions, especially between the U.S. and China, the risk of cyberattacks is expected to increase. Economic frictions, like trade wars, sanctions or tariffs, can escalate cyber conflicts, exposing organizations to higher security risks. This is what was observed in 2018, during the previous U.S.-China trade war, when cyber espionage activities significantly increased due to Chinese state-sponsored actors.[6] Additionally, trade wars may provoke cyber activism, with nationalist hackers launching independent attacks against perceived adversaries.

The discovery of increased state-sponsored hybrid threats and the prevailing geopolitical tensions highlights the undeniable critical importance of robust cybersecurity measures. The potential rise in cyber risks due to recent tariff disputes further emphasizes the necessity for heightened vigilance and proactive cybersecurity measures.

The hidden cybersecurity risks in global supply chains

The recent US tariffs have significantly increased uncertainty for companies worldwide. These tariffs may pose substantial challenges for the future of business operations, necessitating critical adjustments to supply chain strategies. Any adjustment could have important long-term implications for the cyber resilience of companies and their global supply chains. It is important to specify that, as of today, it is

[3] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
[4] According to the Polish undersecretary of state for internal affairs, a state actor caused a recent hospital cyberattack, disrupting medical care for hours. Lithuanian prosecutors accused the Russian military intelligence agency (GRU) of orchestrating an arson attack on an Ikea store in Vilnius last summer.
https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol#:~:text=The%20Europol%20report%20also%20warns,out%20hacking%20and%20cyber%2Dattacks
[5] https://blogs.microsoft.com/on-the-issues/2024/10/15/escalating-cyber-threats-demand-stronger-global-defense-and-cooperation/
[6] https://www.secureworld.io/industry-news/trade-wars-us-tariffs-cyber-risk

premature to predict the full extent of these effects, as there is much to learn about the future evolution and implications of these tariffs.

As businesses navigate the complex, long-term process of modifying supply chain structures, they must carefully assess new suppliers, renegotiate contracts, and reconfigure logistics networks. During such transitions, vulnerabilities may emerge, particularly if security standards are uneven across new partners or if systems are integrated without thorough testing. This may introduce new vulnerabilities that could be exploited by threat actors, further increasing the risk of cyber-attacks.

The importance of addressing these vulnerabilities is underscored by recent findings. In the WEF Global Cybersecurity Outlook 2025 survey, 54% of large organizations identified supply chain challenges as the most substantial barrier to achieving cyber resilience. In today's world, where supply chains have become more complex and reliant on global connections and technology, the vulnerabilities within these systems have become increasingly evident.[7]

Today's supply chains involve numerous stakeholders, including suppliers, manufacturers, distributors, and retailers, all working together across various countries and regions. A single vulnerability, such as a compromised link, can have multiple effects on the entire ecosystem. Cybercriminals can infiltrate multiple companies by targeting third-party vendors or service providers like software vendors, open-source software, cloud services, and hardware suppliers. This is what happened in November 2024, when Blue Yonder, a supply chain management software provider, was targeted by a ransomware attack, which affected many of its clients, including Starbucks UK and supermarket chains Morrisons and Sainsbury's. The attack led to system outages, forcing these businesses to implement manual processes and contingency plans. In the quarter ending January 2025, Morrison's sale growth decelerated to 2.1% down from 4.9% in the previous quarter. The company attributed this decline partly to the outage, which impacted on its ability to maintain optimal stock levels during the Christmas period.

One of the most significant incidents remains the SolarWinds attack.[8] In December 2020, hackers compromised SolarWinds' software updates, distributing malware to their customers through this channel. This allowed them to access the systems of numerous organizations, including U.S. government departments and major companies. This breach was a significant shock, highlighting the vulnerabilities in supply chain security and the potential widespread impact of such attacks. Since the SolarWinds breach, cybercriminals have continued to target supply chain organizations more aggressively. By compromising a single supplier, attackers can potentially access multiple organizations, making supply chain attacks highly profitable and impactful.

As cybercriminals increasingly target supply chain links, it is critical for companies to not only bolster their internal cybersecurity measures, but also rigorously assess and enhance the security practices of their suppliers, especially in light of recent tariff announcements and the potential long-term effect on supply chain disruptions. Achieving cyber resilience in today's globalized world requires a comprehensive approach that addresses vulnerabilities across the entire supply chain ecosystem.

Sources: Nasdaq Index Research, Bloomberg, FactSet.

[7] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
[8] A company that provides IT management software

Disclaimer:

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.