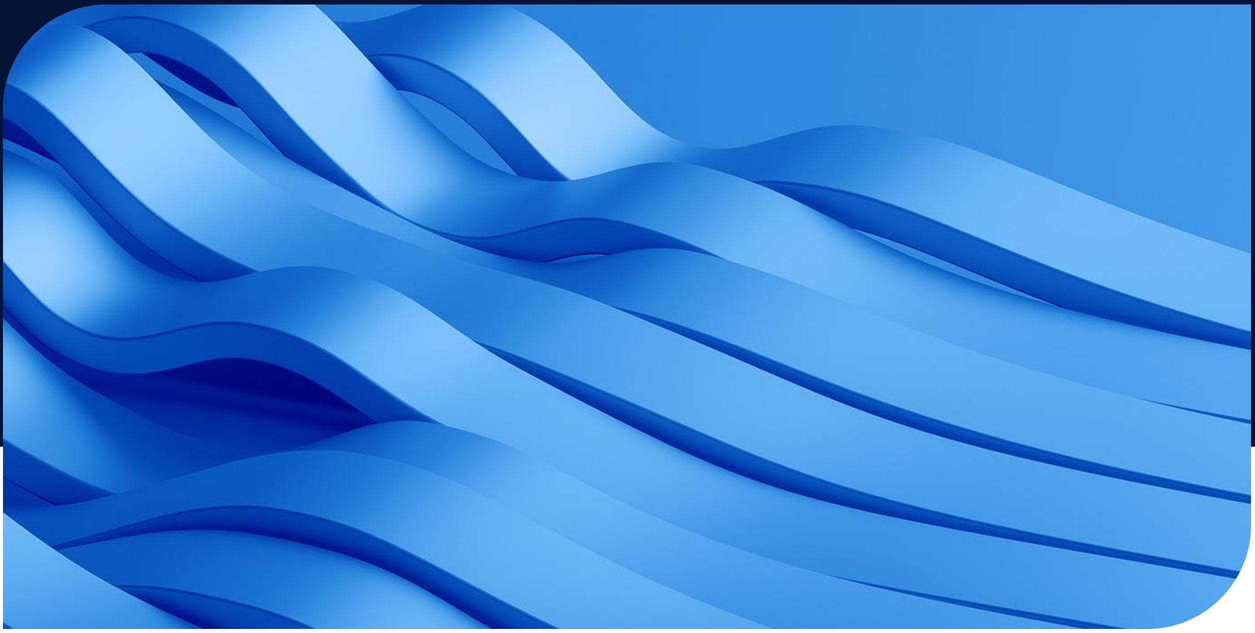
Teneo

From NotPetya to Today's Global Conflict Landscape:

Cyberpolitical Risk Emerges as a Critical Challenge to Business & Society

Teneo Insights | September 2024



In the 19th century, Prussian general Carl von Clausewitz famously stated that war is politics by other means. Nearly two hundred years later, another arena has opened for states to accomplish their political objectives: the cyber realm.

Already, states have begun to demonstrate the real-world implications of conflict in cyberspace, with rising geopolitical tensions across the globe threatening to unleash a new era of cyber disruption. No longer is the threat of a cyberattack confined to the world of financially motivated criminals or teenage hacktivists. Today, the cyberattack that crashes a company's servers or steals its valuable customer information is just as likely to stem from competition and conflict between nation-states within a new playing field of politics.

Understanding the challenges stemming from "cyberpolitical risk," the complex interplay between international politics and cybersecurity, has become crucial for CEOs and their executive teams as they navigate a world marked by constantly evolving international politics. Perhaps no other incident exemplifies the impact of cyberpolitical risk better than the 2017 NotPetya attack, the most destructive cyberattack to date. This article highlights the direct impact of global events such as the NotPetya cyberattack and the Russia-Ukraine war on international business and trade – and outlines several key considerations for organizations adapting to novel threats emanating from the intersection of geopolitics and cyberspace.

Blueprint for Chaos

As of June 27, 2017, the Russia-Ukraine War had been simmering for more than three years, with Russian, Ukrainian and separatist forces locked in a bloody standstill marked by mostly static trench warfare over the contested territories of eastern and southern Ukraine. On that day, however, the geopolitical contest over sovereignty and territory would take a dramatic, unprecedented turn into the cyber realm. On the morning of June 27, the first signs that a major cyberattack was underway began in Ukraine, with government agencies, banks, hospitals, the state power utility, Kiev's airport and metro systems and Chernobyl's radiation monitoring system all going offline.

Soon, it became clear that the attack was not limited to Ukraine, as firms around the globe, including Mondelēz International, Merck, and shipping giant AP Moller-Maersk, reported that their systems had been paralyzed by malware. Later that day, Kaspersky Lab, a Russian cybersecurity and antivirus provider recently banned by the Biden administration, traced the attacks to approximately 2,000 victims across Ukraine, Poland, Italy, the United Kingdom, Germany, France and the United States. NotPetya, as the attacks were named, had been unleashed onto the world stage.

Within hours, NotPetya had paralyzed Ukraine's government, transportation, energy and financial sectors, then spread to shutter the operations of some of the world's largest international firms. The attacks earned their name due to their initial resemblance to the ransomware Petya, an encryption code that emerged in 2016 that targeted Microsoft's Windows-based systems and extorted digital currency payments from victims in exchange for a key to unlock their systems and files. However, as the attack spread globally, cybersecurity experts quickly determined that NotPetya was an entirely different beast.

NotPetya differed markedly from its predecessor in its ability to spread rapidly and inflict damage on infected systems. The malware introduced two key exploits targeting computers running outdated Windows software versions called EternalBlue, which grants remote access to outsiders to run their own code, and Mimikatz, which extracts user passwords from a computer's RAM, enabling access to other machines on a shared network. Although Microsoft had patched the EternalBlue vulnerability prior to the attack, the combination of EternalBlue and Mimikatz enabled NotPetya to infect computers running outdated software, steal their passwords and then use those credentials to infect updated computers running on the same network.

Furthermore, it became clear that NotPetya's objective was not to extort for financial gain, but to cause mayhem, not only within Ukraine but also against international organizations doing business there. Unlike the original code, which encrypts the master boot records (MBRs) that allow computers to boot and load Windows until a ransom is paid, NotPetya was designed to encrypt MBRs and a computer's files. Crucially, it did so without generating a decryption key. Although companies across the globe received messages demanding a ransom to unlock their systems, they were merely a ploy. Without a decryption key, NotPetya left its victims with no means to recover their encrypted data. As the malware spread from Ukraine to the wider world, it left a trail of unprecedented damage in its wake.

The New World of Cyberpolitical Risk

The initial days of chaos inflicted by NotPetya were followed by months of scrambling by impacted international organizations to restore normal software functionality. Companies across the globe reported staggering losses resulting from the disruption; among the $10 billion in total damages attributed to the attack were losses of $870 million by U.S.-based Merck, $384 million by France-based Saint-Gobain and $129 million by UK-based Reckitt Benckiser. Danish-based AP Moller-Maersk, responsible for one-fifth of the world's shipping, reported losses between $250 to $300 million due to multiple days of complete technological paralysis across its global offices and ports. No industry or geographic region of the world, it seemed, had been untouched by NotPetya's rapid and destructive spread.

Later, after much of the dust had settled, NotPetya was traced to a software business in Kiev that was responsible for distributing updates to M.E.Doc accounting software, a tax-filing program used by most people living or doing business in Ukraine. At some point in the months before the NotPetya attack, the business's servers had been infiltrated by hackers. On June 27, 2017, they launched their strike. On June 27, the hackers utilized the infiltrated servers to deploy NotPetya to any computer within Ukraine and across the wider globe that had M.E.Doc installed. The culprits, when their origin was finally identified, would come as little surprise to those in Ukraine who had been engaged in over three years of warfare on their eastern flank. In 2018, the White House formally attributed "the most destructive and costly cyberattack in history" to the Russian military.

While not the first cyberattack by Russia against Ukraine, the NotPetya attack most forcefully punished Ukraine and demonstrated to its global economic partners that they were not exempt from retribution. In an instant, the technological infrastructure underpinning some of the world's largest corporations, operating on the other side of the world and seemingly disconnected from the conflict, came crashing down. NotPetya demonstrated that the threat of a major cyberattack to business interests was no longer limited to criminal hackers out for profit or mischievous teenage hacktivists. Additionally, it showed that they do not need to be directly attacked. Today, the cyberattack that paralyzes an organization's operations may be the spillover resulting from geopolitical competition between nation-state adversaries an ocean away.

Cyberpolitical risk, the intersection between geopolitics and cybersecurity, poses new and powerful threats to the technologies and data upon which all global businesses and organizations depend, regardless of their industry or geographic location. In the years since NotPetya, politically motivated cyberattacks have become a normal feature of the Russia-Ukraine War and, increasingly, they have become a worldwide phenomenon. Following Russia's invasion of Ukraine, cybersecurity authorities in the U.S., UK, Australia, Canada and New Zealand released a joint Cybersecurity Advisory (CSA) "to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity." The advisory followed a joint advisory issued by CISA, the FBI and the NSA warning of Russian-state sponsored cyber threats to U.S. critical infrastructure. More recently, the Olympic Games became a rich target of opportunity for cyber threat actors. Hosting the Olympics, France had to contend with a heightened threat of cyberattacks during the competition, including denial-of-service attacks and ransomware attacks. According to Microsoft, Russia also intensified disinformation campaigns against France in the lead up to the Olympics, which came against the backdrop of the IOC's 2022 ban on Russian athletes from competing for their country and France's support for Ukraine.

Politically motivated cyberattacks have often directly impacted private business and investment interests. In December 2023, a group linked to Israel claimed responsibility for disrupting approximately 70% of gas stations operating in Iran "in response to the aggression of the Islamic Republic and its proxies in the region." In October 2023, North Korean hackers targeted key South Korean shipbuilding firms, attempting to gather naval intelligence that would enable Pyongyang to build larger ships. In June 2022, the FBI, NSA and CISA disclosed that since at least 2020, Chinese state-sponsored hackers had been exploiting the systems of major American telecommunications firms, developing a foothold from which to launch additional, more sophisticated attacks.

Today, with geopolitical tensions rising between nations across North America, Europe, Asia and the Middle East, the threat of politically motivated cyberattacks and the challenges presented by cyberpolitical risk are multiplying. CEOs and their executive teams must acknowledge and address the real cybersecurity challenges stemming from a new playing field for international politics: cyberspace. While future geopolitical developments may seem uncertain, the resiliency of their organizations in the face of cybersecurity threats cannot be.

Considerations for Executives

Historically, Fortune Global 500 companies have been high-value targets of cyberattacks due to their resources, data and intellectual property, and prestige. Today, the threat of a cyberattack impacting major international corporations is compounded by potential spillovers from geopolitically minded cyberattacks designed to punish or disrupt adversaries and rivals of nation-states. In response to these evolving threats, we provide several key considerations and actions organizations may consider while navigating today's geopolitical landscape:

- **Cybersecurity preparedness:** NotPetya spread by exploiting vulnerabilities in computers running outdated versions of Microsoft Windows. In the case of AP Moller-Maersk, the company's global technology infrastructure was infiltrated through a single computer that had installed the M.E.Doc application. The attack highlighted the crucial need for organizations to establish robust cybersecurity measures to protect their systems and data, including regular data backups, software updates, password resets, network segmentation, threat detection programs, strong access controls and employee security awareness and training.

- **Geopolitical awareness:** CEOs and executive teams must be mindful of the geopolitical contexts within which their organizations and their partners operate. Understanding the geopolitical risks emanating from country and regional contexts is critical for protecting a company's operations, investments and people against political, security, economic and, increasingly, cyber shocks. Maintaining heightened geopolitical awareness enables leaders to anticipate potential threats to their operations and cyber infrastructure, as well as the supply chains they depend on, thereby improving business continuity in the event of a crisis.

- **Supply chain security:** NotPetya exploited the third-party software, M.E.Doc, to infiltrate and crash network systems discretely. Organizations must consistently vet their third-party software and service providers to ensure they are adhering to the same cybersecurity standards and anticipating similar cybersecurity risks. Understanding how third-party providers update their products and protect client data, while limiting their access to the company's network, can help mitigate the risk of a cyberattack.

- **Incident response planning:** Scenario planning exercises and simulation drills at the executive level are critical components of developing a comprehensive incident response plan. Understanding the impact of a potential cybersecurity incident on a company's operations streamlines potential response plans in the event of a real-world scenario. Incident response planning exercises should incorporate elements of an organization's IT team, thereby ensuring that technical considerations regarding the impact of network downtime, data loss and recovery efforts are integrated in any crisis response plan.

For more information, email: Resilience&Intelligence@teneo.com

Author

Eric Ryan
Associate, Security Risk Advisory
eric.ryan@teneo.com

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

This material was produced by Teneo for use solely by the recipient. This communication is intended as general background research and is not intended to constitute advice on any particular commercial investment or trade matter or issue and should not be relied upon for such purposes. The views expressed here represent opinions as of this date and are subject to change without notice. The information has been obtained from sources believed to be reliable but no guarantees can be given as to its accuracy, completeness or reliability. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or otherwise, without the prior consent of Teneo. Teneo refers to Teneo Holdings LLC and its affiliates.