Understanding the Impact of the Russia-Ukraine Conflict on Cybersecurity

Published March 15, 2022

Christopher Gannatti, CFA
Global Head of Research

We will always remember the waning days of February 2022, when Russia undertook an unprovoked attack on and invasion of Ukraine. As these words become available to read in March 2022, it is unlikely that we will have a clear roadmap toward a peaceful solution. In our thematic investing, we have been focused on the cybersecurity megatrend and find it interesting to consider this particular megatrend in light of Russia's well-established cyber warfare tactics. It is also important to consider how the very large stocks of raw materials in Russia and Ukraine can travel through related technology-oriented supply chains.

Companies Focused on Cybersecurity Are Taking Action

Microsoft is likely the world's largest cybersecurity company, if we accept the need to secure such things as Azure (its cloud platform) and Office 365 (its productivity suite, used across the world). The current size of Microsoft's cybersecurity business is $15 billion in revenue, representing year-over-year growth of 45%. This doesn't mean that Microsoft doesn't get compromised.1 Of late2:

- Microsoft was compromised in the December 2020 Solarwinds hack, an attack with possible links to the Russian government.
- Only months later, the Exchange email attack had possible links to China's government.
- Relatively recently, a flaw within the Azure cloud platform was discovered by cybersecurity company Wiz Inc.

Charlie Bell, a 23-year veteran of Amazon Web Services, is responsible for Microsoft's cybersecurity effort, and he has 10,000 reports and billions of dollars to deploy in this effort.

On February 23, 2022, CrowdStrike noted, on its blog, the existence of a new wiper malware being used to target Ukraine systems, known as DriveSlayer. According to CrowdStrike, this was the second destructive malware found recently targeting the region, the first being WhisperGate.3

Mandiant, another leading cybersecurity company, has reminded customers that Russia has twice turned off power to Kiev in winter. The company also implored customers to recall the effects of the NotPetya attack in 2017. Mandiant noted that cyber warfare is asymmetric, in that Russia, which cannot compete with the world's largest militaries straight up, needs to use such tactics to show the appearance of parity with other countries.4

Characterizing the KNOWN Risks

IT Outsourcing

Ukraine is a vibrant marketplace for information technology (IT) outsourcing services. Its Ministry of Foreign Affairs notes that more than 100 of Fortune 500 companies rely at least partially on services provided from Ukraine. In fact, Ukraine's IT export volume increased 36% to a figure of $6.8 billion in 2021, up from roughly $5 billion in 2020. Currently, there are 85,000 to 100,000 export service workers in Ukraine, focused primarily on software engineering and IT services.5

Certain companies have noted using and employing engineers in the region, including:

- SAP SE
- Revolut Ltd.
- Fiverr
- Wix.com

Semiconductor Supply Chains

Without question, the Ukraine conflict is not focused on a global center of semiconductor production—which would be in direct contrast to a location like Taiwan if it were to come up as a region of future potential conflict. However, Ukraine and Russia are important for the global supply of both neon and palladium.

This region supplies 40%–50% of semiconductor-grade neon, which is used in some of the lasers involved in chip production. About 75% of the global production of neon ends up used for this purpose. ASML, a major player in the production of chip-making equipment, has indicated that less than 20% of the neon it uses comes from this region, so there shouldn't be a massive impact in the shorter term.6 Of course, that could change as the conflict extends into the future.

Then, about 37% of the world's palladium supply comes from Russia. Even if it's not the main ingredient in chips, it does get used in certain sensor and memory chips.7 The global chip shortage from the pandemic has yet to be resolved, so further hurdles will not be helpful in putting this behind us in the global economic landscape.

Cyberattacks

Russia has an established history of using cyberattacks against Ukraine, most notably the NotPetya attack of June 2017. This knocked out federal agencies, transport systems, cash machines and even the radiation monitors at the Chernobyl site—in short, it was basically 'lights out' in Ukraine's infrastructure for a period. However, as is often the case with networked systems, NotPetya did not stay confined to Ukraine, a country that is globally integrated. Some of the world's largest companies were impacted8:

- Maersk-Shipping
- Saint-Gobain-French Construction

- Mondelez International (owns Cadbury)
- Merck-Pharmaceuticals

The overall estimate of the global damage was in the range of $10 billion, and it is widely believed to be the most expensive example of a cyber attack ever recorded.

It is also worth noting that even before the specific Ukraine conflict in February 2022, there had been a 100% rise in significant nation state incidents between 2017 and 2020. In fact, there was an average of more than 10 publicly attributed cyberattacks a month in 2020.9

Specific cyberattacks are often tricky to attribute precisely. Expeditors International, a logistics supply chain company based near the Port of Seattle, was attacked in late February 2022. Their operations were severely impacted,10 but, as of this writing, the attack is not known to have links to Russian state actors. Nvidia also had a cybersecurity issue in late February 2022, but early disclosures also do not indicate a direct Russia connection. They also indicate that Nvidia was able to largely continue its operations.11

Ways to Invest in the Cybersecurity Response

We would pause to emphasize that any war is a tragedy, and the best possible outcome is always found on a path back toward peace. Barring that for the moment, it is our responsibility as investors, consumers and businesspeople to be reminded of the importance of cybersecurity precautions and having a security mindset. It was interesting to see a quote attributed to Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency in the Biden Administration, to the effect that using two-factor authentication could protect the general user in 99% of cases.12

Within the megatrend investment landscape, we offer two primary avenues:

1. **Cloud computing:** Cloud computing refers to a specific infrastructure setup that allows for the consumption of software through subscriptions and internet connections as opposed to needing physical, local copies. Updates and bug fixes are often pushed seamlessly across all users, and packages can be highly customized. Diversified portfolios of cloud computing companies, such as the WisdomTree Cloud Computing Fund (WCLD) generally include companies focused on delivering cybersecurity solutions.
2. **Cybersecurity:** Cybersecurity is an important enough topic that concentration could be warranted. Diversified portfolios of specific cybersecurity companies would necessarily be more concentrated than broad-based cloud portfolios, but could provide interesting ways for investors to align with those looking to beef up their cyber defenses. The WisdomTree Cybersecurity Fund (WCBR) is one such example.

WisdomTree, in collaboration with Nasdaq, leverages the expertise of Bessemer Venture Partners in the case of cloud computing and Team8 in the case of cybersecurity. While Bessemer is a leading venture capitalist in cloud computing firms, Team8 boast in its leadership ranks former heads of the National Security Agency (NSA) and the Israeli Defense Force's Unit 8200. In both strategies, this expertise is leveraged twice per year to refresh portfolio constituents.

1 Source: Tilley, Aaron & Robert McMillan, "Microsoft's New Security Chief Says it Is Time to Take Shelter in the Cloud," Wall Street Journal, 2/23/22.
2 Source: Tilley, 2022.
3 Source: Thomas et al, "CrowdStrike Falcon Protects from New Wiper Malware Used in Ukraine Cyber-attacks," CrowdStrike Blog, 2/25/22.
4 Source: Joyce, Sandra. "The Ukraine Cyber Crisis: We Should Prepare, but Not Panic," Mandiant Blog, 2/15/22
5 Source: Bousquette, Isabelle & Suman Bhattacharyya, "Ukraine's Booming Tech Outsourcing Sector at Risk after Russian Invasion," Wall Street Journal, 2/24/22.
6 Source: Bhattacharyya, Suman, "Russian Attack on Ukraine Could Dent Chip-Maker Supply Lines," Wall Street Journal, 2/25/22.
7 Source: Bhattacharyya, 2022.
8 Source: "Companies Have a Lot to Fear from Russia's Digital Warmongering," The Economist, 2/19/22.
9 Source: McGuire, Michael, "Nation States, Cyber Conflict and the Web of Profit." HP Wolf Security, 2021.
10 Source: Liu, Nicolle, "Expeditors International Shuts Down Computer Systems after Cyberattack," Wall Street Journal, 2/22/22.
11 Source: King, Ian & William Turton, "Nvidia Breach Seen as Ransomware Attack Unconnected to Ukraine," Yahoo Finance, 2/25/22.
12 Source: Jen Easterly @CISAJen, Twitter, 11/9/21.

Important Risks Related to this Article

Christopher Gannatti is an employee of WisdomTree UK Limited, a European subsidiary of WisdomTree Asset Management Inc.'s parent company, WisdomTree Investments, Inc.

For holdings of Funds mentioned in the blog post, please click the respective ticker: WCLD, WCBR.

WCLD: There are risks associated with investing, including the possible loss of principal. The Fund invests in cloud computing companies, which are heavily dependent on the internet and utilizing a distributed network of servers over the internet. Cloud computing companies may have limited product lines, markets, financial resources or personnel and are subject to the risks of changes in business cycles, world economic growth, technological progress, and government regulation. These companies typically face intense competition and potentially rapid product obsolescence. Additionally, many cloud computing companies store sensitive consumer information and could be the target of cybersecurity attacks and other types of theft, which could have a negative impact on these companies and the Fund. Securities of cloud computing companies tend to be more volatile than securities of companies that rely less heavily on technology and, specifically, on the internet. Cloud computing companies can typically engage in significant amounts of spending on research and development, and rapid changes to the field could have a material adverse effect on a company's operating results. The composition of the Index is heavily dependent on quantitative and qualitative information and data from one or more third parties and the Index may not perform as intended. Please read the Fund's prospectus for specific details regarding the Fund's risk profile.

WCBR: There are risks associated with investing, including the possible loss of principal. The Fund invests in cybersecurity companies, which generate a meaningful part of their revenue from security protocols that prevent intrusion and attacks to systems, networks, applications, computers and mobile devices. Cybersecurity companies are particularly vulnerable to rapid changes in technology, rapid obsolescence of products and services, the loss of patent, copyright and trademark protections, government regulation and competition, both domestically and internationally. Cybersecurity company stocks, especially those which are internet-related, have experienced extreme price and volume fluctuations in the past that have often been unrelated to their operating performance. These companies may also be smaller and less experienced companies, with limited product or service lines, markets or financial resources and fewer experienced management or marketing personnel. The Fund invests in the securities included in, or representative of, its Index regardless of their investment merit and the Fund does not attempt to outperform its Index or take defensive positions in declining markets. The composition of the Index is heavily dependent on quantitative and qualitative information and data from one or more third parties, and the Index may not perform as intended. Please read the Fund's prospectus for specific details regarding the Fund's risk profile.