In Present-Day Wars the First Shots are Likely in Cyberspace & Supply Chains

Published 31 March 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 into Ukraine. As these words become available to read in March 2022, it is unlikely that we will have a clear roadmap towards a peaceful solution.

However, we have been focused on the cybersecurity megatrend within our thematic investing platform for about 13 months, and it is notable to consider this particular megatrend in light of the obvious connectivity back to Russia's likely, and well-established tactics. It is also important to consider how the very large stocks of raw materials in Russia and the Ukraine can feed through related technology-oriented supply chains.

Companies Focused on Cybersecurity are Taking Actions

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 growth of 45% year-over-year. This doesn't mean that Microsoft doesn't get compromised1. Of late2:

- Microsoft was compromised in the December 2020 Solarwinds hack, an attack with possible links to the Russian government
- Only months after the Solarwinds hack, there was the Exchange email attack, with possible links to China's government
- There was also a relatively recent flaw within its Azure cloud platform, which was discovered by the 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 23 February 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 recently found destructive malware targeting the region, the first being 'WhisperGate3'.

Mandiant, another leading cybersecurity company, has reminded customers that Russia has twice turned off power to Kiev in winter and also imploring them to recall the effects of the NotPetya attack in 2017.

They note 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 countries4.

Characterizing the KNOWN Risks

IT Outsourcing

Ukraine is a vibrant marketplace for information technology (IT) outsourcing services, with the Ministry of Foreign Affairs noting that more than 100 out of the Fortune 500 companies relying, at least partially, in 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. 85,000 to 100,000 export service workers are currently in Ukraine, focused primarily on software engineering and IT services5.

Companies like SAP SE, Revolut Ltd., Fiverr and Wix.com have noted using and employing engineers in the region.

Semiconductor Supply Chains

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

40-50% of semiconductor-grade neon comes from this region, 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 in their case less than 20% of the neon they use comes from this region, so in the shorter-term there shouldn't be a massive impact6. Of course, that can 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 chips7. The global chip shortage from the pandemic has yet to be solved, so further hurdles here will not be helpful to putting this behind us in the global economic landscape.

Cyberattacks

Russia has an established set of historical precedents using cyberattacks on Ukraine, most notably through the 'NotPetya' attack of June 2017. This attack 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 of time. 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 including Maersk-Shipping, Saint-Gobain-French Construction, Mondelez International (owns Cadbury) and Merk-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 war began in February 2022, there had been a 100% rise in ‘significant’ Nation State incidents between 2017 to 2020. In fact, there was an average of more than 10 publicly attributed cyberattacks a month in 20209.

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 impacted10, but it was not disclosed to have known links back to Russian state actors as of the time of this writing. Nvidia also had a cybersecurity issue in late February 2022, but the early disclosures also did not indicate a direct Russia connection and also indicated that Nvidia was able to largely continue its operations11.

Investing in the Cybersecurity Response

We would pause to re-emphasize that any war is a tragedy, and the best possible outcome would always be found on a path back towards peace. Barring that for the moment, it is our responsibility as investors, consumers and business people 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, stating that using two-factor authentication could protect the general user in 99% of cases12.

Within the megatrend investment landscape, we see 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 customised
2. **Cybersecurity**: Cybersecurity is an important enough topic where 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 defences.

WisdomTree’s thematic platform benefits from working with subject-matter experts, 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 Defence Force’s Unit 8200. In both strategies, this expertise is leveraged twice per year to refresh portfolio constituents.

1 Tilley, Aaron & Robert McMillan. “Microsoft’s New Security Chief Says It is Time to Take Shelter in the Cloud.” Wall Street Journal. 23 February 2022.

2 Tilley, 2022.

3 Thomas et al. “Crowdstrike Falcon Protects from New Wiper Malware Used in Ukraine Cyberattacks.” Crowdstrike Blog. 25 February 2022.

4 Joyce, Sandra. “The Ukraine Cyber Crisis: We Should Prepare, but Not Panic.” Mandiant Blog. 15 February 2022.

5 Bousquette, Isabelle & Suman Bhattacharyya. “Ukraine’s Booming Tech Outsourcing Sector at Risk After Russian Invasion.” Wall Street Journal. 24 February 2022.

6 Bhattacharyya, Suman. “Russian Attack on Ukraine Could Dent Chip-Maker Supply Lines.” Wall Street Journal. 25 February 2022.

7 Bhattacharyya, 2022.

8 Companies have a lot to fear from Russia’s digital warmongering.” Economist. 19 February 2022.

9 McGuire, Michael. “Nation States, Cyber Conflict and the Web of Profit.” HP Wolf Security. 2021.

10 Liu, Nicolle. “Expeditors International Shuts Down Computer Systems After Cyberattack.” Wall Street Journal. 22 February 2022.

11 King, Ian & William Turton. “Nvidia Breach Seen as Ransomware Attack Unconnected to Ukraine.” Yahoo Finance. 25 February 2022.

12 Jen Easterly @CISAJen 9 November 2021 on Twitter.

Related products

+ WisdomTree Cloud Computing UCITS ETF - USD Acc (WCLD/KLWD)

+ WisdomTree Cybersecurity UCITS ETF – USD Acc (WCBR/CYSE)

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an oer for sale nor a solicitation of an oer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can oen lead to a number of dierent interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public oering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any ailiate, nor any of their respective oicers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.