Cybersecurity Is Still at the Frontline of Geopolitics

Published July 7, 2022

Christopher Gannatti, CFA
Global Head of Research

We recently hosted an *Office Hours* webinar on Disruptive Growth Megatrends. During the audience polling, 'geopolitics' was a big topic in focus. In looking at the global investment flows to different megatrend investment vehicles, cybersecurity was also a huge topic.1

However, for all the focus that people are putting on cybersecurity, the share price performance of the companies hasn't been great.

As we look at the picture and landscape, we note:

1. A lot of attention turned to cybersecurity as a result of the Russia/Ukraine crisis. Microsoft published a report recently summarizing some of the very real attack efforts being made by Russia against both Ukraine and other NATO members.2
2. The way in which cybersecurity is done has been evolving, particularly with the COVID-19 pandemic and the need for many people to access all sorts of data from anywhere. Many of the companies providing these innovative solutions are newer, possibly only having entered public markets quite recently. As they seek to achieve scale, they may have revenues, but they may not yet have positive free cash flows or earnings.
3. The macroeconomic backdrop functions independently of any specific cybersecurity concerns—to put it simply, inflation is high and central banks are undertaking policies to combat it. A side effect is that newer companies that don't yet have positive earnings have been punished with negative share price performance and lower valuations. The first half of 2022 has seen this approach using a very broad brush, so it is our view that at a certain point it will again be appreciated that a company providing cybersecurity solutions should be treated differently than one providing a more discretionary service.

Here, we can take a look at some of these different factors in turn.

Microsoft's Cybersecurity Report on the Ukraine Conflict So Far

One notable factor, that would not have been the case in any prior conflict, is that Ukraine was able to get much of its most critical systems and data into the cloud. Microsoft noted the provision of services valued at $107 million (provided to Ukraine's government at no charge) to help with this cloud transition. The result is there isn't a physical 'on-prem' data infrastructure that Russia can target and destroy.3

Russia is waging cyberattacks across multiple fronts and operational units4:

- GRU (the Main Directorate of the General Staff of the Armed Forces of the Russian Federation): The GRU is involved in trying to steal data with phishing attacks through its STRONTIUM operation. Its IRIDIUM operation showcases some of the types of malware that are aiming for data destruction. DEV-0586 also is involved in data destruction and influence operations.
- SVR (the Foreign Intelligence Service of the Russian Federation): The NOBELIUM operation has been spread across both Ukrainian and NATO member diplomatic targets.
- FSB (the Federal Security Service in Russia): The FSB's ACTINIUM, BROMINE and KRYPTON operations are primarily involved in phishing attempts and further data theft.

The report also notes that Russia has been very adaptive in its cyberattacks, combining them with physical attacks against specific targets, for example. Good words to describe the efforts so far could be "strategic" and "deliberate." To date, there haven't been any attacks using 'wormable' malware like the 2017 NotPetya attack, in which the malware could jump from one computer network to another. The attacks appear to be designed to stay inside Ukraine.

The report also details 128 Russian network penetration and cyber espionage operations outside Ukraine. Roughly half of these targeted government agencies, but notably, the success rate was only 29%. One must remember that cybersecurity attacks can be a numbers game, but it is interesting that while the world is now fully focused on this, they are able to mount at least a somewhat effective defense—at least so far.

Let's Look at CrowdStrike

CrowdStrike is a company well positioned for the current cybersecurity environment, helping with cloud security and endpoint protection. In its most recent quarterly results, CrowdStrike actually raised its full-year guidance. Like many other security providers, CrowdStrike indicated that they have not seen any overt evidence that customers are going to be cutting back on their security spending. When articles are written and analyst coverage is relayed, it is generally very positive and focused on a strong long-term story for CrowdStrike.5

So where is the disconnect coming from—specifically with such difficult 2022 share price performance? While we probably cannot know with certainty why a stock trades the way it does, we can see that CrowdStrike has tended to have a very high valuation relative to earnings or revenues. Maybe the long-term growth story can support this, but in the current macro environment, having exposure to such a high multiple company may lead to near-term volatility regardless of the product or service being provided.

Conclusion: SaaS Companies Should Trade based on the Problem They Solve

It's amazing how competitive the Software-as-a-Service (SaaS) space can be. Think of Shopify—a great business. Their reward, at least one of them, for being a great e-commerce platform is getting to compete with Amazon Prime. Think of Zoom—a household name. Now, they get to compete against Microsoft Teams, quite a tall order. It's great that these upstarts can keep some of the largest companies in the world on their toes, consistently improving their product offerings.

However, cybersecurity, in our view, is a bit different from other SaaS businesses. While the specific companies that people can work with differ, every business and really every person needs to have some sort of cybersecurity strategy to protect their data and their other digital efforts. Additionally, the space is constantly evolving, whether due to the COVID-19 pandemic, the Russia/Ukraine crisis or other factors. We believe that in a way, you need to be focused on newer companies providing more cutting-edge solutions. Even if the coming months may be volatile, we do love the longer-term case for this megatrend.

For those interested in the cybersecurity space, consider the WisdomTree Cybersecurity Fund (WCBR).

As of 7/7/22, WCBR held 5.35%, 0%, 0%, 0%, 0% of its weight in CrowdStrike, Shopify, Amazon, Zoom Video Communications, and Microsoft, respectively..

1 Sources: WisdomTree, Morningstar & Bloomberg. All data as of 3/31/22 from WisdomTree's quarterly thematic classification study and subsequent quarter updates.
2 Source: "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, 6/22/22.
3 Source: Microsoft, 6/22/22.
4 Source: Microsoft, 6/22/22.
5 Source: Eric J. Savitz, "CrowdStrike Posts Strong Earnings and Boosts Guidance, but the Stock Slips," Barron's. 6/2/22.

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.

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 that 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.