CYBERSECURITY: A PILLAR OF DEFENSE IN MODERN WARFARE

Christopher Gannatti – Global Head of Research
05/10/2022

We recently had a conversation with experts in cybersecurity at Team8. WisdomTree and Team8 collaborate on the WisdomTree Team8 Cybersecurity Index, and while we have frequent conversations, it was clear that we had to discuss cybersecurity in light of the Russia/Ukraine crisis.

We were able to speak to:

- **Admiral Michael S. Rogers:** Admiral Rogers served in the U.S. Navy for 37 years, rising to the rank of four-star admiral. He had a four-year tour as Commander of U.S. Cyber Command and Director, National Security Agency (NSA). He is currently supporting various companies in the private sector, speaking to business groups and working internationally in the cyber and national security areas.
- **Bob Blakley:** Bob is an Operating Partner at Team8, and he was previously Global Director of Information Security Innovation at Citi. He also recently served as a member of the National Academy of Science's Forum on Cyber Resilience.
- **Aaron Dubin:** Aaron is the Vice President of Strategy & Business Research at Team8. Earlier in his career, Aaron led early-stage strategic cyber investing in New York on Goldman Sachs' Principal Strategic Investments Team.

Below, we break the discussion into three clear segments:

1. Russia—what do we think they are doing and will do?
2. Cyber Offense and Cyber Defense—thinking at the national, corporate and individual levels.
3. Broader global considerations.

Russia

What do we think Russia is looking for?

We believe Russia was seeking to install a new pro-Russian regime in Ukraine, looking to ensure that Ukraine would never join the North Atlantic Treaty Organization (NATO) and looking for territorial annexation. These different objectives have been widely reported but are important to remember for the setting of context.

How is Russia doing in terms of results?

Thus far, if we accept the aforementioned objectives, Russia has not achieved them, and it remains in question how well it will be able to achieve them, if at all. It would appear that the more updated strategy is to focus more on eastern portions of Ukraine, like the Donbas. It would also appear that the focus is now on creating more damage to civilian infrastructure and civilian casualties.

How is Russia responding to the initial poor results?

It does not appear that Russia's response will be to seek a peaceful solution—it looks like they are repositioning and doubling down. One recent bit of news regarded a newer commander in the battle space, Alexander Dvornikov. General Dvornikov has a reputation from his actions in Syria, and he believes that civilian casualties are an essential

part of any war strategy. It also looks like the Western nations, led by the U.S. and Europe, will be doubling down on sanctions. Furthermore, China has not stepped away from Russia, at least not yet. Then, there is Ukraine, and they clearly believe that Russia's actions have been war crimes and that Russia needs to be held accountable. In short, it doesn't look like there is a high probability of any side immediately backing down and leading to a near-term peaceful resolution of this conflict.

Do we believe that Russia feels vulnerable to cyberattacks from the West?

We believe it is more likely that the U.S. and the West generally feel more vulnerable to Russian cyberattacks than Russia would worry about Western cyberattacks. Russia is actually in the process of decoupling its internet infrastructure from the global internet infrastructure. This amounts to building its own domain name system (DNS) infrastructure to avoid disruptions from Ukraine and other Western enemies. This would allow Russia's government to better control the country's internal information space.

Looking back at history, when the U.S. placed sanctions on Iran's financial system, Iran retaliated with cyberattacks on the U.S. financial system. Even if it hasn't happened yet with serious effect, the U.S. (and the West, more broadly) should be prepared for the possibility of cyberattacks on the financial system.

It also must be remembered that Russia is strongly dependent on energy revenues. It would not be outside the realm of possibility to see Russian cyberattacks on competing oil producers to lower global oil supplies and keep the price higher, as a high price, in general, leads to stronger Russian revenues.

If there is a primary risk that Russia might be considering, it could be the time to achieve its objectives. The country cannot support a wide-ranging conflict that goes on indefinitely, and eventually, there could be a political consequence there. When we had this discussion, it was roughly 45 days into the conflict, so it's clear that they can go longer than 45 days from what we see.

Cyber

Have we seen significant cyberattacks in Ukraine (yet)?

As of this writing, there has not yet been much cyber infrastructure damage in Ukraine. Instead of focusing just on this, we talked more about the possible reasons why Russia might have held back the "catastrophic cyber knockout punch."

1. Russia may have thought that the ground invasion would yield better, faster results and that a wide-scale cyberattack would not be needed.
2. Russia thought it would install a pro-Russia government that would then need all the infrastructure to run Ukraine effectively.
3. Ukraine has made massive improvements in its own cybersecurity infrastructure. There is a big difference between a surprise cyberattack and a cyberattack that the adversary knows is coming and is prepared for. The catastrophic surprise cyberattacks that have made history in the past, like "NotPetya," typically take months to prepare.

The bottom-line consideration regards how both sides see the concept of escalation. As of this writing, based on a discussion that occurred roughly 45 days in, both sides seem to desire to limit escalation. Big cyberattacks are notoriously difficult to control once they are out of the box, and they could spread into other countries. However, as time drags on, the calculus of the desired escalation may change.

Has Russia already attacked Western systems and left back door access for future attacks?

While this narrative is possible, the West has now gone through a multi-month period of heightened cybersecurity awareness. If these access points exist, their effectiveness will be diminished as updates or new configurations are applied and cybersecurity protocols are changed. As the world continues to focus on cybersecurity and make certain preparations, it will become more difficult to use old tactics to the same effect, even if nothing is ever 100% protected.

What should people do?

Everyone should be backing up their systems frequently and using two-factor authentication. It also is more important to run updates in a timely manner and have an antivirus system.

Broader Geopolitical Backdrop

What about China?

There are lots of discussions that look to China next, and it must be remembered that China is also formidable on the cyber front. China has historically used cyber for intellectual property and espionage. They do increase their activities when they believe that the West or the U.S. is focused on something else—and this situation would qualify. However, it is not clear that it is in their interest to perform massive, disruptive attacks.

Conclusion

Cybersecurity is constantly evolving, with new headlines occurring all the time. While we hope that a peaceful resolution to the Russia/Ukraine conflict comes as quickly as possible, we also believe that people have to pay attention to their unique cybersecurity risks in light of this conflict, whether they do that through their own actions, corporate actions or investments.

For standardized performance and the most recent month-end performance click here NOTE, this material is intended for electronic use only. Individuals who intend to print and physically deliver to an investor must print the monthly performance report to accompany this blog.

Related Blogs

+ Understanding the Impact of the Russia-Ukraine Conflict on Cybersecurity

Related Funds

+ WisdomTree Cybersecurity Fund
+ WisdomTree Cloud Computing Fund
+ WisdomTree Battery Value Chain and Innovation Fund

View the online version of this article here.

IMPORTANT INFORMATION

U.S. investors only: Click here to obtain a WisdomTree ETF prospectus which contains investment objectives, risks, charges, expenses, and other information; read and consider carefully before investing.

There are risks involved with investing, including possible loss of principal. Foreign investing involves currency, political and economic risk. Funds focusing on a single country, sector and/or funds that emphasize investments in smaller companies may experience greater price volatility. Investments in emerging markets, currency, fixed income and alternative investments include additional risks. Please see prospectus for discussion of risks.

Past performance is not indicative of future results. This material contains the opinions of the author, which are subject to change, and should not to be considered or interpreted as a recommendation to participate in any particular trading strategy, or deemed to be an offer or sale of any investment product and it should not be relied on as such. There is no guarantee that any strategies discussed will work under all market conditions. This material represents an assessment of the market environment at a specific time and is not intended to be a forecast of future events or a guarantee of future results. This material should not be relied upon as research or investment advice regarding any security in particular. The user of this information assumes the entire risk of any use made of the information provided herein. Neither WisdomTree nor its affiliates, nor Foreside Fund Services, LLC, or its affiliates provide tax or legal advice. Investors seeking tax or legal advice should consult their tax or legal advisor. Unless expressly stated otherwise the opinions, interpretations or findings expressed herein do not necessarily represent the views of WisdomTree or any of its affiliates.

The MSCI information may only be used for your internal use, may not be reproduced or re-disseminated in any form and may not be used as a basis for or component of any financial instruments or products or indexes. None of the MSCI information is intended to constitute investment advice or a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such. Historical data and analysis should not be taken as an indication or guarantee of any future performance analysis, forecast or prediction. The MSCI information is provided on an "as is" basis and the user of this information assumes the entire risk of any use made of this information. MSCI, each of its affiliates and each entity involved in compiling, computing or creating any MSCI information (collectively, the "MSCI Parties") expressly disclaims all warranties. With respect to this information, in no event shall any MSCI Party have any liability for any direct, indirect, special, incidental, punitive, consequential (including loss profits) or any other damages (www.msci.com)

Jonathan Steinberg, Jeremy Schwartz, Rick Harper, Christopher Gannatti, Bradley Krom, Tripp Zimmerman, Michael Barrer, Anita Rausch, Kevin Flanagan, Brendan Loftus, Joseph Tenaglia, Jeff Weniger, Matt Wagner, Alejandro Saltiel, Ryan Krystopowicz, Jianing Wu, and Brian Manby are registered representatives of Foreside Fund Services, LLC.

WisdomTree Funds are distributed by Foreside Fund Services, LLC, in the U.S. only.

You cannot invest directly in an index.