The War of Misinformation makes Cyberspace the new Battlefield

As the events in Ukraine continue to unfold (#StandWithUkraine), one must keep in mind how this invasion started. Well before Russian troops started pouring over the borders into Ukraine the cyberwar was laying the groundwork.

Beginning on February 15th, a series of distributed denial of service (DDoS) attacks commenced. These attacks impacted Ukrainian government organizations including the Ministry of Defense, Ministry of Foreign Affairs, Armed Forces of Ukraine and the publicly funded broadcaster Ukrainian Radio. Additionally, the attacks targeted two banking institutions, PrivatBank and Oschadbank. On Feb. 18, both the United States and the United Kingdom attributed these DDoS attacks to Russia's Main Intelligence Directorate (GRU).

These attacks have continued, and on February 23rd, a new variant of malware named HermeticWiper was discovered in Ukraine. Shortly after, a new round of website defacement attacks were also observed impacting Ukrainian government organizations. Putin and his team of henchmen were trying to shake the resolve of the Ukrainian people with misinformation, while attempting to disrupt, disable or destroy critical infrastructure. But don't think that the threat ends there. Future attacks may target U.S. and Western European organizations in retaliation for increased sanctions or other political measures against the Russian government.

I don't know if it is related or not but today Toyota Motor Corp. (NYSE: TM) will suspend work at all of its Japan factories after a supplier shut down its computer systems over concern about a possible cyberattack. The world's top auto

producer said it will suspend operations at all 14 plants in its home country. The stoppage is linked to Kojima Press Industry Co., which detected an abnormality in its internal server network. The manufacturer of metal, plastic, and electronic components found evidence its network was accessed from outside the company, raising concern about a possible cyberattack and leading Kojima Press to shut down the system.

The supplier is trying to restore the system for March 2nd but I wouldn't be surprised if it takes a lot longer than that. Regardless, a possible hack at a supplier will shut down the world's largest car manufacturer for at least 2 days where a one-day stoppage for Toyota's factories in Japan translates to roughly 13,000 vehicles. This is going to have a material impact on cash flow for a lot more companies in the overall supply and distribution chain than just Toyota and Kojima.

These are just the latest examples of the importance of protecting our digital way of life across clouds, networks, and mobile devices. There is virtually no commerce done on this planet anymore that doesn't have some sort of digital impact that can be tampered with, hacked or stolen, unless of course you produce local goods or crafts, only accept cash for payment, leave that cash in a safe and don't report it to the tax authorities. Otherwise, everyone in the developed and even most developing nations has some sort of digital footprint. That's why cyber security should be paramount for virtually every corporation and potentially every individual out there and why I believe it is a very compelling investment thesis.

Somewhat surprisingly, at least to me, is that a lot of the ETFs and individual cyber security stocks are trading at lower prices than they were when I first visited this subject on October 28, 2021. However, at the time they were trading at fairly rich levels and with most growth stocks being put in the penalty box due to the specter of rising interest rates, a lot of these stocks sold off through to the end of January. Then the whole sector seemed to get caught up in the panic

selling last week as Putin began the ground war in Ukraine, despite all the cyber attacks that preceded physical troops crossing the border. This was probably the dip to buy as everything related to cyber security has caught a serious bid the last 3 days.

Granted, one stock has outperformed its peer group and is trading 19% higher than its October 28 close. Palo Alto Networks Inc. (NYSE: PANW) appears to be in a slightly different league than its competitors based on the performance of its share price over the last 4 months. Albeit the stock is up 25% in the last 4 days, which might make someone wonder if now is the time to buy. Technically, it just broke out to a new all-time high yesterday which is considered a bullish move by most technicians and sets the stock apart from its peers. Combine that with the fact that they are in a sector that could be one of the most important businesses going forward and you might want to put Palo Alto Networks on your radar. If nothing else, the Company has a good blog to help keep you up to speed on global cyber threats, which is where I sourced a bunch of the information in this article.