Confluence INVESTMENT MANAGEMENT

Weekly Geopolitical Report

By Bill O'Grady

June 21, 2021

The Geopolitics of the Colonial Pipeline Ransomware Attack: Part II

In Part I, we provided an overview of the Colonial Pipeline ransomware attack, followed by reflections on organized crime and why ransomware has become so attractive to criminals. We also described Darkside, the firm involved in the attack. This week, we will conclude with a discussion of why this attack was a mistake and who will suffer from it. As always, we will conclude with market ramifications.

The Error of the Colonial Pipeline Attack

Using the background from last week's report, we can assert that the attack on the Colonial Pipeline was a terrible mistake. It is likely that the attackers, by focusing on Colonial's business systems software, assumed the pipeline would be able to remain in operation. In the hackers' intelligence gathering, it appears they failed to recognize that the business software was incorporated in the command and control software, thus compromising the business software, which led to a shutdown of the pipeline. This action led to high levels of publicity, the kind that catches the attention of governments. One of the reasons for President Carter's unpopularity was gasoline shortages. There is little chance that any administration would tolerate a pipeline shutdown that would threaten its popularity. Simply put, this was not the level of attention the hackers were seeking.

Soon after realizing the attack was becoming a problem, Darkside tried to explain its position. It made a public statement that it was "apolitical" and wasn't seeking to create problems for society. It also indicated that it was not acting on behalf of any government. Soon after, it accepted 75 bitcoins (approximately $5 million) in payment. Some analysts have argued that this payment was six to seven times less than normal.[1] If true, this would suggest that Darkside and its affiliated gangs realized they had made a mistake and were willing to take a significant discount to simply end the crisis. Even that decision probably was a mistake. Outside parties were able to track Colonial Pipeline's payments. The U.S. government may have encouraged Colonial to pay the ransom in order to track the payment. There are reports that indicate Darkside closed down its operations, and the DOJ has confirmed it was able to track the ransomware payment and retrieve the bitcoins.

The Losers

What is remarkable about this incident is the losers in this hack. We detail four parties who were especially harmed by this event:

Ransomware hackers: In our analysis of criminal behavior, we noted that ransomware falls into the tolerated category. The behavior doesn't fulfill an unrequited demand but is parasitic on the economy. Successful parasitic activity is rewarding enough to benefit the parasite but not overly damaging to the host. As we noted above, Darkside had clearly professionalized the model. It had a customer service department and made it clear that if your entity did not have sufficient protections against such hacking, it intended to make you pay…but

[1] Listen at the 6:40 mark of the linked podcast.

not pay so much that you resisted. Darkside analyzed its targets and tried to establish a price that would not lead a victim to seek help from the government. The goal was to encrypt the data, get payment, and release the data as smoothly as possible. Most victims simply paid the ransom and tried to protect themselves from suffering another attack.

This model undoubtedly did not want to attack a critical target that would get the attention of government and society, but that is exactly what Darkside and/or its affiliate did. And although this action was clearly unanticipated, the attack has changed the view of ransomware. The Department of Homeland Security has issued cybersecurity regulations for pipelines. There is a chance that regulators will extend these rules to other areas of the economy, including electric utilities (beyond what is currently required), finance, transportation, etc. At a minimum, mandatory reporting will likely be required. This increased regulation would mean that it will become less lucrative to conduct ransomware. This is especially true if insurers decide to stop underwriting such policies.

If the U.S. did put Darkside out of business, it suggests that being in a safe harbor nation only protects against arrest. But if the U.S. can disrupt a hacker's servers and take their cryptocurrency, it means that hackers would need to keep the costs of paying ransomware so low that it becomes less attractive to criminals.

To some extent, the ransomware "business" existed because governments didn't care enough to intervene. Governments probably didn't care because they weren't convinced it was a large enough problem to warrant intervention. The Colonial Pipeline attack made it clear it was material and needed attention.

America's enemies: The United States enjoys a geographic benefit that assists its hegemony. It is surrounded by weak powers and oceans. Earlier superpowers often had regional powers near them that forced the hegemon to divert resources to domestic security. Spain, for example, had to protect itself from France, although the Pyrenees did offer some natural defense. The Netherlands was especially vulnerable to France and other powers. Britain enjoyed the protection of the English Channel, but that turned out to be less adequate in the age of airpower.

The U.S. is difficult to invade. Navies must traverse long distances and can be attacked in route. Even aircraft can be detected. Missiles can strike the U.S., but without nuclear weapons they are only a modest threat. In the last two world wars, America's enemies were unable to mount effective attacks on the lower 48 states. This natural defense allowed America's industrial might to arm itself and its allies, eventually leading to victory in both conflicts.

After WWII, the U.S. did face the threat of a nuclear attack from the Soviet Union. However, as both sides built their nuclear arsenals, it became apparent that neither side would survive a full-scale attack. The doctrine of Mutually Assured Destruction (MAD) meant that nuclear war was unlikely unless either side was faced with certain defeat. Having and being able to deliver nuclear weapons means that such nations don't ever have to accept unconditional surrender.

The terrorist attacks of 9/11 by al Qaeda raised the possibility that foreign non-state

actors, perhaps aided by rogue nations, could attack the U.S. But that attack turned out to be a "one-off" and has not been repeated.

America's conventional military prowess, exhibited in the First Gulf War, showed that the U.S. is probably impossible to defeat in a conflict with clearly defined objectives. Consequently, America's enemies have mostly opted for unconventional strategies. In Iraq and Afghanistan, the strategy was to simply outlast the U.S. In preparation for other conflicts, the plan includes psychological tactics and cyberattacks.

It is not overly difficult to imagine a situation where an American opponent who desires to engage in an act that would trigger an American military response would couple that action with an asymmetric attack on American soil. For example, if Russia wanted to invade Ukraine, or China wanted to attack Taiwan, launching a cyberattack on American infrastructure as a distraction would make sense. Forcing an American president to juggle a military response while dealing with large parts of the electric grid "going dark" would give the invader an edge. In prior wars, American civilians were mostly isolated from direct attacks; cyberattacks open a new front.

Military planners prefer an element of surprise. Although a surprise isn't always necessary for victory, it usually is a benefit. So, if China, Russia, Iran, or other nations were planning some sort of cyberattack on the U.S. infrastructure as part of other military operations, one would have to think that these actors were displeased about Darkside's attack on the Colonial Pipeline. The attack revealed a clear vulnerability that an enemy would have probably preferred to have available to use against the U.S. if it engaged in a military action in another theater.

The Darkside hack is a bit like a small unit of Japan's Imperial Navy launching a small-scale strike on Pearl Harbor to show "proof of concept" for a bigger operation. Although the initial attack would have likely worked, it would also signal a vulnerability that the U.S. would almost certainly have addressed. Although militaries sometimes deploy a new technology before it's ready, giving the adversary a chance to adapt, one would expect militaries to prefer to maintain the element of surprise.

This hack may fade from the memories of U.S. policymakers over time, but it is more likely to create a reaction from the U.S. government to increase protection from cyberwarfare activities. If it does, it could have taken away a tool from America's adversaries or at least weakened the ability to plan surprise attacks.

Ramifications

This event has several market ramifications. Some of the potential effects are as follows:

Bullish for cybersecurity: Although this an area of growing interest, this event will make it abundantly clear to firms that they are vulnerable, to some degree, to ransomware. The industry that provides cybersecurity resources, from security consultants to anti-malware providers, should see increased interest, especially with government subsidies.

Bearish for cryptocurrencies/bullish for gold: In a recent *Asset Allocation Weekly*, we noted that the correlation between gold and bitcoin has flipped from positive to negative. Increasingly, investors are choosing between gold or bitcoin when purchasing currency debasement hedges.

Bitcoin and other cryptocurrencies have seen remarkable price appreciation recently, but prices have shown weakness over the past month. Some of this weakness is a function of the fact that cryptocurrencies have become the payment of choice for organized crime.[2] The fact that cryptocurrencies can be sent around the globe without physical movement and are mostly anonymous makes them attractive to criminals. In a sense, cryptocurrencies are replacing the infamous "suitcases of small, untraceable bills" for paying ransom. And the popularity of cryptocurrencies with criminals is catching the attention of law enforcement and regulators. It's not just U.S. officials; China is increasingly hostile to cryptocurrencies. This attention could bring measures to make cryptocurrencies more easily traceable, not just to catch criminals but for taxing authorities as well. As our aforementioned analysis showed, anything that weakens the demand for cryptocurrencies should be bullish for gold. Again, something to note for investors looking to protect portfolios from currency debasement.

Bearish for software: The software industry has tended to view security as an afterthought, something to be patched later. Anyone with a smartphone can notice that operating software updates usually involve improving security. That, in and of itself, suggests that security isn't the primary focus of software providers. The goal is to be first to provide the software; first movers often enjoy an advantage and fix vulnerabilities later. After all, the motto of the tech industry is to "move fast and break things." However, that stance creates serious problems. Even providing security patches can be an issue. Users are not always good about downloading the new software, leaving themselves at risk. There are other vulnerabilities as well. There is a lot of business that runs on legacy software that interfaces with newer software, which may open areas for attack. There is evidence to suggest that some software firms are beginning to realize this stance is not sustainable. How investors treat this stance remains to be seen, but we suspect it won't be welcomed.

Ultimately, security in software experiences what economists call "negative externalities." These are costs that are not attributed to the supplier but to others. The classic example of a negative externality is pollution. The price of the good does not capture the cost in addressing the cleanup of the pollution. Because the price is too low, consumers buy more than they would otherwise, and producers supply more than they would if the price reflected the full cost. We may be reaching the point where society can no longer bear the cost of these externalities. In the case of Colonial Pipeline, the decision to not fully air gap the command and control software from the business systems caused a shutdown of critical infrastructure. The costs of this loss probably won't be borne by the software designer or the pipeline but by those who sat in gasoline lines. If we are at the point where such events won't be tolerated, software costs will rise.

Bearish for critical infrastructure: Related to the software issue is that critical infrastructure will likely be forced by regulators to improve their security. Although there may be some debate as to how secure an individual software user needs to be, for utilities, pipelines, commercial transportation, etc., security from cyber risk will almost certainly need to improve. Although some of these costs will be passed on to consumers, regulators may

[2] Not to mention its energy footprint.

also force capital owners to share in the burden.

Overall, the Colonial Pipeline event will potentially affect several areas of geopolitics and markets. Although we don't know with certainty how all this will roll out, we believe that it will reach far beyond a simple act of ransomware.

Bill O'Grady
June 21, 2021

Confluence Investment Management LLC

Confluence Investment Management LLC is an independent Registered Investment Advisor located in St. Louis, Missouri. The firm provides professional portfolio management and advisory services to institutional and individual clients. Confluence's investment philosophy is based upon independent, fundamental research that integrates the firm's evaluation of market cycles, macroeconomics, and geopolitical analysis with a value-driven, company-specific approach. The firm's portfolio management philosophy begins by assessing risk and follows through by positioning client portfolios to achieve stated income and growth objectives. The Confluence team is comprised of experienced investment professionals who are dedicated to an exceptional level of client service and communication.