Confluence INVESTMENT MANAGEMENT

Weekly
Geopolitical Report

By Patrick Fearon-Hernandez, CFA

November 2, 2020

Of Pirates and Computer Hackers

It's now been more than a quarter century since the first nefarious behavior was observed on the internet. There have been countless news reports about computer hacks, stolen data, ransom scams, misinformation aimed at manipulating elections, and the like. Many of us have had to change our passwords and sign up for free credit monitoring after a service provider suffered a digital breach. We've probably all seen how businesses have been forced to up their game and adopt stronger computer security, just like they lock their doors against common burglars.

But what if common burglars aren't necessarily the best model for thinking about hackers? Some of the hackers who threaten our personal data or the sensitive systems of our companies and public institutions certainly are "lone wolves," but in this report, we'll show that another model for understanding today's hackers can be found in the pirates who prowled the Spanish Main from the 1500s to the 1700s. We'll look at what some hackers have in common with those pirates and what it means for digital security. As always, we'll wrap up with a discussion of potential investment ramifications.

Pirates and Privateers

The word "pirates" in the paragraph above is a generalization. After all, there are rogues, and then there are rogues. Just so, those dastardly sailors who menaced shipping on the Spanish Main four centuries ago should be thought of in at least two distinct categories:

- ***Pirates.*** This generalized term applies to any individual who commits nautical misbehavior, whether it's robbery, kidnapping, coastal raiding, or seizing ships on the high seas. As noted in the *Encyclopedia Britannica*, "Robbery, kidnapping, and murder all qualify as piratical activities, provided there's some water and a boat involved. If there's no water and no boat, you're just a regular bandit. If there's a boat but no water, you need to go back to pirate school."

- ***Privateers.*** This term applies to a specific type of pirate, i.e., a private individual who is commissioned by a government to attack, harass, or steal from its enemies. For example, the government might grant private ship owners the right to rob a rival country's merchant vessels and raid their coastal settlements. Privateering therefore allows the government to project power and undermine its enemies without having to involve its own official naval forces.

Believe it or not, we can learn a lot about today's state-backed computer hackers by studying how Britain utilized privateers against Spain from the late 1500s to the 1700s. In some of those years, hundreds of British privateering voyages were launched against the Spanish coasts, the Azores, and Spanish colonial ports in the Caribbean. Many of those voyages were full-scale military operations. In 1585, for example, Sir Francis Drake sailed from Portsmouth for the Spanish Caribbean with 22 ships, with which he was able to sack the major ports of Santo Domingo, in today's Dominican Republic, and Cartagena de Indias, on the northern coast of today's Colombia.

Although we tend to envision piracy and privateering as one ship seizing another, British privateers actually focused their attacks on cattle ranches, sugar mills, and smaller, unprotected ports. According to British historian Hugh Thomas in his masterful three-volume history of the Spanish Empire, cattle hides were by far the most coveted loot for British privateers, followed by sugar, silver, gold, pearls, cochineal, logwood, and balsam.[1] When faced with an imminent privateer attack, Spanish settlers would often negotiate with the privateers to determine a payoff that would convince them to go on their way. On the open seas, the Spanish treasure ships that moved vast amounts of silver and gold back to Spain were rarely attacked because they traveled just once or twice a year in large convoys with naval escorts. The only successful seizure of a Spanish treasure fleet was in 1628 when the infamous Dutch pirate Piet Heyn was able to carry off the trick with a fleet of 31 ships. More often, the British (and, later, the French and Dutch privateers) focused on smaller, poorly defended merchant ships. In any case, the privateering attacks proved an effective method for the British crown to conduct economic warfare against Spain for more than a century.

The most fascinating thing of all was the relationship between the British nobility and the privateers. Privateering expeditions were typically chartered by the crown, and top government officials were intimately involved with them. In the late 1580s and 1590s, the Lord Admiral (Lord Howard of Effingham, Earl of Cumberland, who had commanded the British navy in its destruction of the Spanish Armada in 1588) even had a right to 10% of the value of any prizes captured. Captains who seized Spanish ships also agreed to give the admiral a fee of £3,000 per vessel.

Queen Elizabeth knighting Sir Francis Drake aboard the Golden Hinde, *1581.*
(Source: History.com)

British privateering ships were often owned by wealthy and powerful individuals. They might even be owned by partnerships consisting of up to eight investors seeking to profit from anti-Spanish piracy while sharing the risks. One owner, John Watts, had interests in five privateering ships.

[1] The description of privateering herein comes from the final volume of this history. Thomas, Hugh. (2014). *World Without End: Spain, Philip II, and the First Global Empire*. New York, NY: Random House.

Another, John Chidley, owned interests in three, including one in which a cousin of Queen Elizabeth had also invested. Indeed, Queen Elizabeth herself invested in privateers as did Sir Walter Raleigh. Many of the investors grew rich from their privateering activities, which in turn gave them an incentive to build bigger, more heavily armed vessels. Some privateering ships were nearly as powerful as the Royal Navy's best battleships.

Just as there are few major enterprises where all work is done by the owners, privateer ships relied on large crews. In fact, because of the promise of booty, privateers were usually overmanned, even though their crews were typically not paid. Crews were compensated by their share of any loot captured. The captured cargo was divided among the crew by established rules, heavily influenced by seniority. For example, the master gunner might get the Spanish gunner's personal items and the second-best gun. The happiest ships were those where the crew had the right to sell their share of the loot to the captain or quartermaster. [Captured food and wine were typically consumed immediately; the pirates' reputation for being ravenous eaters and hard drinkers was evidently well deserved.] The arrangement had much in common with today's technology start-ups, where workers often don't get paid much but do get stock options. In sum, the economics of British privateering against the Spanish ensured that the interests of the capital owners and workers were aligned with each other and with the sponsoring government.

State-Sponsored Computer Hackers

So, how do the pirates and privateers of five centuries ago relate to today's computer hackers? Perhaps the first thing to get straight is exactly what we mean by "hacking." What we're concerned with here are actions like electronically breaking into an individual's or an organization's computer systems to gather confidential information, steal money or intellectual property, hold the system for ransom, plant malware, or otherwise disrupt or disable the system. Since modern societies are uniquely dependent on the integrity of their information technology infrastructure, it's easy to see that while some of these hacking activities might be little more than an annoyance, others could have enormous, dramatic impacts on an organization or on the wider society.

Unfortunately, hacking attacks have become common and ubiquitous. The Center for Strategic and International Studies publishes a list of significant hacking attacks around the world since 2003 that now runs 53 pages! The problem is that people often only have a vague understanding of what these attacks entail and who is perpetrating them. Indeed, the "attribution problem" of identifying who was behind a hack can be challenging, though probably not as challenging as widely assumed.[2] We think it's best to think of today's hackers in three separate categories:

Private Criminals and Criminal Gangs. Just as some of the pirates prowling the Spanish Main from the 1500s to the 1700s were independent brigands pursuing their own individual interests, many of today's computer hackers are simply bored, young computer nerds looking for a thrill, or perhaps small-scale criminals looking to steal money from other individuals. Some may work for larger criminal networks using more sophisticated technology tools and tricks to steal significant sums in mass

[2] Carlin, John P. (2018). *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. New York, NY: Public Affairs/Hachette Book Group.

attacks. But the key characteristic with these criminals is that they are limited to the capabilities you might see in regular crime, be it individual or organized.

National Governments. At the other extreme, many national governments have now developed the capability to hack into the computers of rival states, criminal organizations, or individuals for purposes of national defense, foreign policy, or law enforcement. One prominent example is the Stuxnet malware used to sabotage Iranian nuclear research operations beginning in 2010. Stuxnet is widely believed to have been developed by the U.S. and Israeli militaries. Another example is the wide-ranging offensive hacking activities carried out by Russia's military intelligence service, the GRU.

State-Sponsored Hackers. As mentioned above, national intelligence agencies and law enforcement bodies can now identify who perpetrated a computer hack much more easily than is widely imagined, which makes government-run hacking risky. Therefore, many U.S. adversaries now rely heavily on private criminals and co-opted tech experts to carry out hacking for them. The goal is to attack, harass, or steal from the nation's adversary while obscuring who was really behind the attack in hopes of avoiding blowback. Perhaps the most infamous example of this approach is Russia's use of the Internet Research Agency (IRA) to interfere in the 2016 U.S. presidential election. The IRA, based in St. Petersburg, Russia, is an ostensibly independent troll farm, but it is funded by wealthy restauranteur Yevgeny Prigozhin, a close associate of President Putin with extensive ties to the Russian government. Even if the IRA isn't directly controlled by or funded by the Russian government, it has worked extensively and secretly to advance Kremlin interests in the U.S., Ukraine, and in Russia itself.

It's important not to overstate the parallels between state-sponsored hackers and the privateers of yore. To date, we've seen little evidence of computer hackers walking around on peg legs with parrots on their shoulders. All the same, the use of hackers who are sponsored by the state, but not actual state employees, blurs the line between government action and criminal activity, just as privateering against the Spanish Empire did centuries ago.

As with the privateers, the use of state-sponsored hackers is a way to bring the resources of a nation state to bear against its enemies in a way that minimizes costs and preserves some modicum of deniability. Allowing private individuals and organizations to profit from harassment and theft against a nation's enemies is a way to incentivize the hackers to develop ever more powerful tools, processes, and organizations. The IRA, for instance, is a highly sophisticated organization that employs hundreds of trolls with specific schedules, quotas for how many untrue blog posts are posted each shift, and even bonuses and benefit plans. This is comparable to the way British privateering profits would have been channeled back into ever larger and more powerful ships in order to improve their ability to seize Spanish vessels or attack Spanish towns. Since the state sanction is only provided so long as the hackers work to advance the state's interests, the system ensures that the hackers generally operate in line with the state's goals, even if they are simultaneously pursing their own interests.

Ramifications

Looking forward, the costs imposed by today's state-sponsored hackers are similar to those imposed on Spanish settlers and seafarers by the British privateers. Backed by the resources of a nation state, the hackers potentially have the power to disrupt U.S. commercial ventures and impose a wide range of costs with relative impunity. Sometimes, state-sponsored attacks may be little more than annoyances. Other times, they may involve relatively inexpensive ransom attacks. More importantly, however, the state-sponsored hackers constitute a new vector of attack that could be hard to defend against in times of tension with rivals like China, Russia, Iran, and North Korea. At the very least, the possibility of attack will impose ongoing digital security costs on U.S. businesses, since they could be at risk of a major hacking attack at any moment.

Lone-wolf hacking, state-sponsored attacks, and government cyberwarfare can best be seen as a major background risk that investors need to keep in mind going forward. Given the difficulty in defending against such attacks, investors considering individual companies probably need to pay close attention to their cyber defenses. That's especially true for firms operating in the infrastructure sectors that are widely seen as key potential hacking targets, like utilities. In contrast, this analysis suggests that companies in the cyberdefense industry may enjoy continuing strong demand for their services going forward.

Finally, the risk of state-sponsored computer hacking is an added reason for investors to carefully maintain good diversification across domestic and international asset classes, including safe-haven assets like gold and other precious metals. When considering where to deploy their foreign exposure, investors may want to favor countries whose governments demonstrate they have good digital defenses and are highly vigilant about hacking risks. A similar consideration may apply to gold. Some investors are becoming enthralled with cryptocurrencies for purposes of both high potential returns and safety, and indeed, gold and cryptocurrency values do tend to move together. However, cryptocurrencies are hackable, and there have been reports of cryptovaults being targeted by hackers, while gold is unhackable.

Patrick Fearon-Hernandez, CFA
November 2, 2020

This report was prepared by Patrick Fearon-Hernandez of Confluence Investment Management LLC and reflects the current opinion of the author. It is based upon sources and data believed to be accurate and reliable. Opinions and forward-looking statements expressed are subject to change without notice. This information does not constitute a solicitation or an offer to buy or sell any security.

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.