Confluence INVESTMENT MANAGEMENT

Weekly Geopolitical Report

By Bill O'Grady

May 21, 2018

Reflections on Cyberwar

(Due to the Memorial Day holiday, our next report will be published on June 4.)

On Saturday, May 11, the *New York Times* ran an article on the threat of Iranian cyberattacks.[1] Although the report didn't necessarily break any new ground, cyberwar does pose some interesting issues for American hegemony. In this report, we will begin with American military superiority and the increase in unconventional threats. From there, we will discuss the impact of near abroad risks on hegemony. The problem of security and efficiency will be addressed and, as always, we will conclude with market ramifications.

The American Military

On January 16, 1991, the air campaign of the Gulf War began. By February 28, 1991, the conflict was over. Going into the war, there was concern about the American military's ability to successfully fight a war half a world away against a hardened Iraqi army, given that the U.S. hadn't conducted a major military operation since Vietnam.

Although it would be unfair to discount the contributions from the allies in the conflict, the reality was that the Gulf War was an American-conducted event. Of the 750k soldiers who participated in the ground campaign, over 70% were American.

The results, at least for the allied side, were phenomenal. The air campaign lasted 42 days, with the allies conducting over 100k sorties. The ground phase of the war officially began on February 24, 1991, and was halted three days later, with a ceasefire called on February 28, 1991. In the conflict, 150 American soldiers lost their lives.

It was clear the American military had improved since Vietnam. The air campaign undermined Iraqi command and control, isolating Iraqi troops in the field. Once the combined air forces achieved air supremacy, Iraqi troops were in a precarious position. By the time allied ground forces entered the field, Iraqi troops were poised to be routed. The American way of war, which combined multiple aircraft platforms, signals intelligence, rapid armored movement and highly trained troops, was a form of "shock and awe."

The U.S. military showed the world that entering into a conventional conflict with the U.S. was probably foolhardy. Although the flat desert terrain was almost ideal for U.S. war planners, the fact remained that the military had learned to fully integrate the armed services into a single functional unit that could deliver precise, overwhelming firepower.

So, how does a nation deal with the U.S. military? Numerous trends have developed. First, a reliance on asymmetric warfare methods has increased. By asymmetric warfare methods, we mean insurgency tactics, which include small unit attacks, improvised explosive devices and widespread attacks that force the conventional military to expend lots of resources when responding to threats. A good example of this is the 2003 Iraq War.

[1] https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html

The U.S. military and coalition partners invaded Iraq and rapidly moved toward Baghdad. The invasion began on March 20, 2003. Baghdad fell on April 9, 2003. On May 1, 2003, President Bush delivered his "Mission Accomplished" speech on the deck of the U.S.S. *Abraham Lincoln*. However, soon after, the coalition found itself fighting an insurgency. Initially, the insurgency was dominated by former Iraqi military personnel, mostly Sunni, but then elements of al Qaeda became involved and Iranian Republican Guard Corps supported a Shiite insurgency. Although the official U.S. engagement ended when U.S. troops left Iraq on December 18, 2011, there is still a sizeable American military presence in Iraq, mostly due to the war against Islamic State.

Asymmetric tactics are designed to draw a superior force into a war of attrition. Although it is difficult to win such a conflict outright, the key for the opposing power is to simply outlast the U.S. To some extent, that was the lesson of Vietnam, Iraq and probably Afghanistan.

Second, some militaries are trying to put critical American military infrastructure at risk. For example, nothing exemplifies American naval power better than the aircraft carrier. These vessels have been essential to U.S. power projection since WWII. China has been working on a medium-range ballistic missile[2] that could be used against aircraft carriers. It is thought to have a range of 780 nautical miles which would make the "first island chain" a no-go zone for aircraft carriers. Although the Chinese have never used the weapon in actual combat, the risks to a carrier are probably enough to weaken the power projection of the carrier fleet—at least that is what China is aiming for.

China and Russia appear to be working on "satellite killers"[3] that could be used to destroy or impair U.S. assets in space. One familiar resource is the American Global Positioning Satellite system. Although that system has become a familiar tool for smartphone users, the system was originally created for the military. The satellite killers could also adversely affect a whole series of assets, including weather and communications satellites. These weapons are designed to undermine American command and control capabilities and impede the U.S. military's ability to respond.

Third, the use of cyberwar tactics will likely increase. Cyberwar can include a myriad of tools, including the corruption of social media, manufacturing news, undermining the financial system, stealing secrets, disrupting manufacturing processes, etc. And, cyberwar has an added benefit—it is relatively easy to conceal the origin of the attack. Without the ability to attribute the attack, an enemy can act with impunity. In the next section, we will discuss cyberwar in the context of hegemonic security.

Hegemony and the Near Abroad

A tenant of hegemony is that the superpower needs to be in a position where the near defense of the nation is inexpensive. That's because the hegemon must project power across the globe. If the hegemon spends significant resources on defending the homeland, there will be less available for securing the world.

Spain's geography was less than ideal for the superpower role. Although its northern

[2] http://nationalinterest.org/blog/the-buzz/chinas-new-carrier-killer-missile-could-mean-big-trouble-the-24284

[3] https://www.thedailybeast.com/russias-killer-satellites-re-awaken

border was separated from Europe by the Pyrenees mountain range, only a small waterway protected the peninsula from Africa. For example, the Moors from Northern Africa dominated the peninsula from 711 to approximately 1492, although its influence was reduced by 1236 when Cordoba fell to the Christians. Spain had to defend itself against a return of the Moors on its southern border and from France on its northern border.

The next superpower, the Netherlands, used its navy to project power. However, the constant threat from France prevented the Dutch from maintaining hegemony.

The British were favored by being an island. The last successful land invasion of the British Isles was in 1066. The British dominated the world from Napoleon into WWII. However, the development of air power meant the islands were vulnerable to attack.

Geographically, the United States has proven to be the most protected hegemon. The last time a foreign power invaded the U.S was in 1812. As the country expanded it pushed the Canadians into regions far enough north to only support a small population. In the south, a series of conflicts pushed the Mexicans into the desert. As Otto Von Bismarck noted, "America is surrounded by weak powers and fish." This condition made America ideal for hegemony.

Through two world wars, the lower 48 states were mostly unscathed when much of the rest of the world, especially the industrialized world, was devastated by bombing and the conduct of the war. Americans have become accustomed to the geographical protections offered by its position in the Western Hemisphere.

Since a conventional attack against the lower 48 is highly unfeasible, what can a foreign power do to actually attack the U.S.? Nuclear powers with the capacity to deliver such weapons could attack the U.S. However, the U.S. possesses a potent nuclear triad of bombers, missiles and sea-launched submarine missiles. Any nation to engage in a first strike against the United States could be reasonably certain that the forthcoming response would likely be devastating. For most of the Cold War years, Mutually Assured Destruction (MAD) prevented a nuclear exchange and allowed the lower 48 states to avoid a nuclear attack.

The second way to attack the U.S. is through terrorism. The 9/11 attacks are the most notorious but there have been numerous smaller scale attacks. In general, government counterterrorism efforts appear to have been sufficient to prevent a large-scale terrorist operation similar to 9/11. Terrorism as a tactic is frightening (hence the name), but it's rare that a terrorist group can overthrow a government. Sometimes insurgencies will use terrorism to inflict damage on a government but eventually insurgencies have to turn into mass movements to oust a government. If the military remains loyal to a government, insurgencies can usually be managed. When an insurgency gains enough sympathy among the military to lead the latter to oppose the government in power, terrorism can lead to a revolution. In the case of the U.S., terrorism as a tactic has not threatened the government. A foreign power can use terrorism to attack the U.S. but we doubt that it could actually lead to an overthrow of the U.S. government or end American hegemony.

The third way to attack the U.S. is through cyberwarfare. This method is still new, thus we can't say definitively that it wouldn't

work to end American hegemony. Cyberwarfare takes on many forms. It includes using social media to disseminate internal dissention to disrupting communications, financial transactions and industrial processes. Foreign powers find cyberwarfare tempting because it is difficult to specifically attribute the source of attacks.

The U.S. is vulnerable to cyberwarfare because the economy is technologically advanced. The internet is connecting more devices in businesses, households and government. Smartphones have become widespread; although they are clearly useful, they can also be used by a hostile power to track behavior and selectively send information. Foreign powers and criminal groups have penetrated critical infrastructure, including dams and the electrical grid.

There are two sides to cyberwarfare, offense and defense. The U.S. has formidable capacity on offense—the Stuxnet virus, the first known government deployment of cyberwarfare, was developed, in part, by the U.S. So far, the U.S. seems to have decided to follow a MAD model of deterrence; essentially, officials warn that the U.S. could strike a foreign power, making it imprudent to use cyberwarfare to attack the U.S. However, given the ability to mask the source of attack, this model may not work like it did for nuclear weapons.

In addition, the spectrum of weapons is broad. It appears the Russians used social media in the last U.S. presidential election to attempt to affect the outcome. Russian behavior is nothing new—Russia has tried to influence the U.S. political system since the Soviet era. But, social media has proven to be a much more effective tool than what was previously available. Democracies have been susceptible to social media being used to sway opinion. It would be difficult for the U.S. to find a degree of proportionality against low-grade cyberattacks.

Although economists struggle to find solid evidence of productivity gains from technology, there is little doubt that technology has changed how Americans work and behave. Our businesses no longer have steno pools. Word processing and spreadsheets allow us to make constant changes to documents and reports; perhaps in the "old days" we simply lived with items not being "perfect," but there is little doubt that we can make changes more easily. Overhead projectors have given way to PowerPoints, although it is arguable whether the information offered has improved. Ordering at restaurants is changing; increasingly we can bypass the middleman and send our selections directly to the kitchen.

At the same time, this interconnectedness means that our economy may be becoming increasingly fragile. I put myself through college by working in retail. Our cash registers could be hand cranked during power outages, but there is no way current scanning registers could operate without power. I wonder if new drivers could actually read a paper map to find their way around. The electronic processing of documents means that it is nearly impossible to secure a report from a hacker; to ensure security, we would have to revert to typewriters, probably manuals.

Technology changes the skills required to operate in society. If an attacker took the GPS system offline, Americans may struggle to get around. Persistent power outages and surges could fry delicate circuits. It's possible that items like programmable thermostats could be

damaged, whereas the old manual ones would be fine.

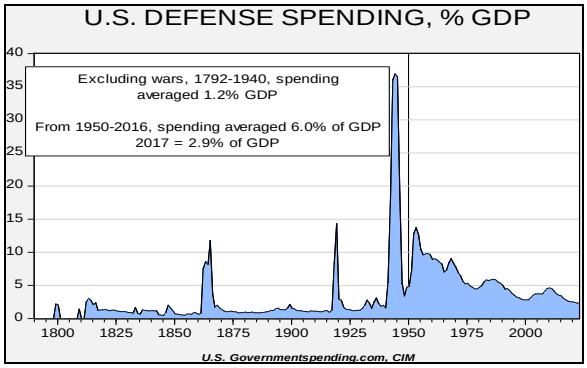
Defending against cyberwarfare is expensive and may slow the progression of technology. U.S. regulations have generally not held tech companies responsible for software that is vulnerable to hacking. Doing so would have put high burdens on innovation. But, the costs don't go away; merely shifting the costs to the consumer puts the burden on the party with the least resources to protect themselves.

And so…

Given America's overwhelming position in conventional warfare, we believe that cyberwarfare will become the tactic of choice for powers opposing U.S. hegemony. Protecting the U.S. from these attacks will not only be expensive, but it may also change how the economy deals with technology. In other words, taking security into account when introducing new technology may become more important in the future.

Ramifications

Since the U.S. accepted the superpower role, defense spending has become an important factor in the economy.



This chart shows U.S. defense spending as a percentage of GDP. Note that pre-hegemony, U.S. defense spending was rather low; only during conflict periods did spending rise but, soon after the conflict ended, demobilization occurred and defense spending fell sharply. After 1950, defense spending remained elevated compared to earlier periods.

As we noted above, other nations have likely concluded that engaging in a conventional war with the U.S. is foolhardy. Thus, they have tried to develop technologies that weaken critical components of the American military. Overall, it appears that cyberwarfare is probably the most promising avenue to attack the U.S.

From a market perspective, this may mean that defense spending will shift away from a conventional focus to dealing with the threat of cyberwarfare. As a result, firms engaged in internet security should find favor. At the same time, we would also expect regulators to place a higher burden on tech firms to "harden" their products, including software and "the internet of things." This change will tend to raise costs for these firms, impacting their valuations.

Bill O'Grady
May 21, 2018

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, fundamental 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.