Confluence
INVESTMENT MANAGEMENT

Weekly Geopolitical Report

By Bill O'Grady

January 23, 2017

War Gaming: Part II

Two weeks ago, we began this two-part report by examining America's geographic situation and how it is conducive to superpower status. This condition is problematic for foreign powers because it can be almost impossible to significantly damage America's industrial base in a conventional war with the U.S. In addition, it would be very difficult to launch a conventional attack against the U.S. (a) with any element of surprise, and (b) without significant logistical challenges. The premise of this report is a "thought experiment" of sorts that examines the unconventional options foreign nations have to attack the U.S. Although these may not lead to regime change in America, such attacks may distract U.S. policymakers enough that foreign powers could engage in regional hegemonic actions that would otherwise be opposed by the U.S.

In Part I of this report, we discussed two potential tactics to attack the U.S., a nuclear strike and a terrorist attack. This week, we will examine cyberwarfare and disinformation. We will conclude with market effects.

#3: Cyberwarfare

Cyberwarfare is a broad tactical category, ranging from the use of computer technology in conventional warfare to hacking enemies' industrial, financial, media, utility and social networks to gain information, monitor behavior, spread disinformation and disrupt operations of these networks. Both state and non-state actors are active in cyber activities. There is a significant criminal element as well.

The best known cyberattack was allegedly jointly created by Israel and the U.S. Dubbed "Stuxnet,"[1] it was a computer virus which took control of systems that monitored Iran's nuclear centrifuges. The virus returned information to its handlers and eventually was able to adversely affect the operation of the machinery itself, causing some of the centrifuges to spin out of control. Although Iran's nuclear facilities were not directly connected to the internet, the bug was apparently introduced through a flash drive. This means that either a spy plugged a drive into Iran's system or an innocent Iranian did it by mistake.

Initially, as reports from Iran began emerging about problems in its nuclear facilities, it was generally assumed that the Persians simply didn't know what they were doing or had purchased faulty equipment. Eventually, Stuxnet ruined about 20% of Iran's nuclear centrifuges. The virus turned out to be rather pervasive, spreading to Indonesia, India, Azerbaijan and Pakistan, and, interestingly enough, also infecting about 1.6% of American computers.

There are numerous other examples of cyberwarfare. The U.S. hacked insurgents' cell phones in Iraq, allowing the American military to track their movements and even send them texts with false orders that may have led to their capture or demise. China has become notorious in its hacking of U.S. government and defense sites. Criminals routinely use "phishing" emails to gain

[1] See WGR, The Stuxnet Virus, 10/4/2010.

control of individual and business computers, sometimes to "kidnap" their data (ransomware) or to simply gain their information.

Cyberwarfare carries numerous risks. As seen with Stuxnet, once released, a virus can become uncontrollable, harming friends and foes alike. It is relatively easy to conceal as it can be difficult to determine where an attack originated. In other words, a state actor could make it appear that a criminal group was responsible for the hack. Or, the criminal group could act as a mercenary for a state, giving the government plausible deniability. Governments have an incentive to co-opt and coerce technology firms to build in "back doors" that allow them to monitor information from citizens.[2] This deliberate defect makes the product less attractive to consumers. On the other hand, an impregnable information system would be a very attractive tool for terrorists and criminals. Essentially, personal privacy is always at risk in a world where cyberattacks are possible.

Technology, for the most part, improves efficiency. Recently, my family traveled to the Caribbean which required a tour through U.S. Customs upon our return. We were checked into the country using an automated kiosk that scanned our passports, took a picture and sent us to a border agent. The following day the system crashed and what took us about 45 minutes to navigate took others up to six hours to clear. Payment systems have become increasingly electronic. This allows households to carry less cash and lets banks and other financial institutions move funds more easily through the economy. However, it also makes the system vulnerable to hackers. Banks are constantly facing threats from criminals trying to gain access to accounts. Fraudulent purchases on credit cards are common. These acts are more easily facilitated due to technology.

In financial services, technology has changed how orders are handled. Trade execution is nearly instantaneous. The futures pits used to be populated with wildly waving traders in colorful jackets; now, these trades are executed via terminals and, in many cases, ordered by algorithm. Although this has lowered execution costs, it also makes financial markets susceptible to "flash crashes" that occasionally roil the markets.

Essentially, technology has been eliminating the number of people directly involved in processing transactions, everything from financial markets to retailing and government services. Although this makes the economy more efficient, it also makes it more fragile. If a system crashes, it can cause widespread disruptions and close firms, government agencies and markets. The U.S. economy, due to its technological advances, may be more vulnerable to cyberattacks than other nations.

Although cyberattacks won't likely cause regime change in the U.S., it could seriously disrupt the American economy, giving a foreign power time to use conventional military means to establish regional hegemony. Thus, if China wanted to capture Taiwan or if Russia wanted to invade the Baltics, a major cyberattack, such as bringing down the electrical grid,[3]

[2] See WGR, The Apple Problem, 3/14/2016.

[3] Russia allegedly hacked a Vermont utility but did not actually access the grid. See: https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.7f4d92b403ca

causing dams to malfunction or disrupting air traffic control, may be enough to shift security and other officials' attention in order to improve the odds of a successful attack.

Cyberwarfare is a significant threat to U.S. security and has very attractive characteristics. It is stealthy; the origin of the attack can be disguised and it can cause significant damage to an economy. Although the U.S. may be vulnerable to such an attack, it should be noted that American intelligence agencies and the military have significant firepower in this area as well. The difference is that disrupting the Russian economy might not matter all that much because it's already in poor shape. But, in the U.S., shutting down the electrical grid for several days would be considered catastrophic; in fact, simply bringing down the internet might be just as bad. The U.S. faces a constant threat from cyberattacks. The key concern is what a foreign power would do with a disruption. China has already captured defense plans and personal information. So far, it has used this information to improve its own defense materials and to create countermeasures to U.S. defense goods. But the threat of a cyberattack as cover for a regional military operation is perhaps the greatest threat the U.S. currently faces.

#4: Disinformation

Disinformation is nothing new. From time immemorial, governments have tried to fool their adversaries. From America's perspective, Radio Free Europe was broadcasting the truth to those behind the Iron Curtain. To the communists, it was pure propaganda.

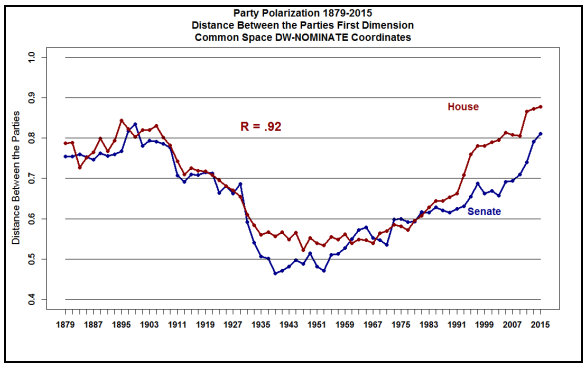
There are two changes that make disinformation more dangerous. First, the technology behind news flow has changed dramatically. During the era of print media, disseminating news was rather expensive. Printing needed to occur. Journalists needed to be hired. The journalists were usually trained and there were standards of conduct that acted as a screen for reports. Although there was a "yellow press"[4] in American history, the Cold War period was probably the golden age of journalism.

By the 1980s, cable news became an alternative to the major networks. The cable news companies discovered that they were able to capture a more reliable viewership by taking a definite slant toward the news. AM radio, as an older technology and because of its low cost, became an avenue of more extreme views. But the real change agent was the internet and social media. The internet allowed for news to be disseminated almost instantly. Social media allows common citizens to post items and videos for all to see. Regular media companies suddenly found themselves competing with citizens and their cell phones. From 1981 to 2014, the number of daily newspapers declined by 25.3%. Social media and news aggregators have the ability to screen news flow based on the viewing habits of the reader. Essentially, if one reads off the internet uncritically, they can live in a virtual news echo chamber. Thus, news, "facts" and viewpoints become hardened.

The changes in news dissemination dovetailed with changes in political polarization.

---

[4] The Spanish-American War was, to some extent, created by the Hearst and Pulitzer news agencies.



(Source: Voteviewblog.com)

This chart is a measure of party polarization; essentially, it measures partisanship. The higher the reading on the chart, the more the political structure is partisan and polarized. Before the U.S. emerged on the world stage, there were strong disagreements on policy. There was less polarization by WWI, and during the Cold War the degree of polarization reached historical lows. In other words, regardless of political party, there was a high degree of bipartisanship.

When the Cold War ended, bipartisanship also deteriorated. Currently, the country is probably the most polarized it has been since the Civil War. Unfortunately, this degree of disunity is dangerous for a superpower because it creates conditions that can distract policymakers from global concerns.

Perhaps the greatest risk to the evolution of American hegemony was the Civil War. Although the British were the undisputed global superpower at the time, the leadership of that nation was watching the explosive economic growth in the U.S. warily. The British probably made a strategic mistake in not supporting the Confederacy because if it had survived the U.S. would have been divided and would never have achieved the same degree of power. According to historians, the political elites favored supporting the South but the public opposed it because of slavery. In addition, Queen Victoria also supported abolition and opposed the Confederacy. The British did offer some support but never enough to turn the tide.

An America divided is susceptible to disinformation. We are living in an era where "false news" is routinely disseminated. In addition, facts have become increasingly tied to social and political positions; in other words, no fact seems to exist outside a social and political context. During the Cold War, the losing political party in an election was in opposition but did work with the winner; in the current environment, the losing party believes catastrophic events are likely and the only way to ensure a better future is to resist the policy goals of the other party.

This environment allows foreign powers to influence social and political beliefs. It is clear the Russians tried to influence the U.S. presidential election. This should not come as a shock to anyone. The U.S. has done this for years; what Americans see as supporting democracy-loving activists in foreign nations looks much like meddling to foreign governments. In addition, it is routine for other nations to have lobbying efforts in the U.S., ostensibly to affect American policy.

What is surprising is that the Russians seem to have had some success, although we would argue that it probably wasn't as significant as the media is suggesting. We believe the reason the Russians were able to find some traction with the leaks and its behavior is that the political environment allowed it to occur. A political environment in which the other party isn't seen as merely an American with a different political position but one that is perhaps evil allows leaks and disinformation to have power.

Essentially, it appears that our current highly partisan climate has created an environment where disinformation is more likely to be accepted. If this process makes America more divided, it will reduce our ability to project power and exercise hegemony. Although disinformation probably won't bring regime change, it can create conditions under which an aspiring regional hegemon can try to influence American public opinion in a fashion that will reduce the likelihood that the U.S. responds negatively to the aspiring regional hegemon's encroachment. In other words, if Russia wanted to take the Baltics, it may try to use false news and internet dissemination to sway Americans to oppose U.S. and NATO intervention.

Ramifications

This report is something of a thought experiment about how foreign nations can attack a hegemon with extraordinarily favorable geographic conditions. We identified four primary methods—a nuclear strike, terrorism, cyberattack and disinformation. These are not the only methods, but we suspect these are the most likely. Two others that deserve mention are biological/chemical warfare and space. The reason we didn't explore the former is that it is probably similar to a nuclear attack if done in scale; we would know who did it and we would not be surprised to see a state-sponsored biological attack met with a nuclear strike or a massive conventional attack. Of course, a terrorist attack using these methods could be effective but these weapons are notoriously difficult to deploy effectively. And, the U.S. has an advanced medical sector that would probably be able to cope with a small biological attack. A space attack, which could range from attacking satellites to launching weapons, is possible. However, the U.S. is probably as well prepared as any nation for such conflicts and so a pre-emptive strike would probably be met in kind. Thus, for considerations of length, we didn't explore either of these methods in detail.

We are not likely to face a nuclear attack but the other three are quite likely and, in fact, have occurred and will likely continue to occur. Of the remaining three, we are most worried about the two discussed this week. Computer hacking by China and Russia is common; although it hasn't led to anything that threatens civil order, the potential does exist that it could at some point.

Disinformation is another rising concern. Although this method has existed for centuries, the internet allows dissemination without filters. Thus, the ability to affect the unity of the nation and America's capacity to mobilize against enemies to support allies could be compromised.

As noted, we believe a conventional military attack on the continental U.S. is highly unlikely. However, that doesn't mean that aspiring regional hegemons won't use the last three methods to improve their odds of success in local actions. The Russian concept of "hybrid war" uses the last three in combination to undermine nations in its near abroad and weaken any opposition to Russian goals of regional domination. The U.S. may become a more likely target of similar actions in order to distract America from opposing the aims of aspiring regional hegemons to expand their areas of control.

The market ramifications are complicated. Technology security firms should find steady business from the private and public sector. Media companies may face additional burdens of screening news for potential "false news" stories. Overall, though, the biggest impact may be that these factors are part of a trend where the U.S. continues to move away from the

superpower role it has played since the end of WWII. We have documented and discussed these issues at length. The bottom line is that a G-0 world is one that is negative for foreign investment but probably bullish for commodities. The dollar and U.S. financial assets will likely benefit relative to foreign assets.

Bill O'Grady
January 23, 2017

Confluence Investment Management LLC

Confluence Investment Management LLC is an independent, SEC 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.