Confluence INVESTMENT MANAGEMENT

Bi-Weekly Geopolitical Report

By Daniel Ortwerth, CFA

April 22, 2024

The Changing Face of War

If the United States were at war with another great power, would we know it? How would we know it? These questions might seem absurd but consider that the US has not fought a war against a major world power since 1945. Meanwhile, when the US has engaged in conflicts against weaker and regional powers since World War II, the beginnings and endings of the conflicts have tended to be blurred. Technology has advanced in ways unimaginable to the 1945 mind. This has changed the nature of life, and it has also changed the face of war. In this report, we consider how the contours of that face have changed over time, what it takes to recognize war in the 21st century, and whether the US and its allies might already be at war with China and its allies.

By addressing key elements of technological advancement and geopolitical evolution, we explore how 80 years have changed the face of war. We consider aspects of war that have not and never will change as well as what has changed, and we drive to the bottom line for investors. In our view, that bottom line has remained constant through time as war is expensive, citizens pay the price, and that price largely manifests itself in the form of ***higher inflation and long-term interest rates***. Will the US ever go to war again with another major power in a way that we can recognize? Will we know it when we are there? These questions are harder to answer than ever before, but investors can still prepare.

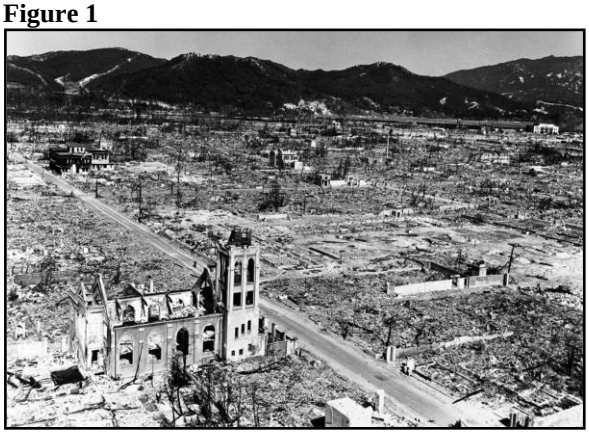
War: Constant Aims, Evolving Means

In his heavily studied and oft-quoted treatise "On War," the preeminent military theorist Carl von Clausewitz provided a simple, ruthless, but true definition of war. For Clausewitz, war is merely a "continuation of policy by other means." He further specifies that, "***War is an act of violence intended to compel our opponent to fulfill our will***." He defines violence in war as the use of "force to injure, abuse, damage, or destroy" someone or something. Clausewitz's central message is that the point and purpose of war is to achieve political goals, especially those related to foreign policy. A government can employ any number or type of policies to assure its security, advance its prosperity, or serve its interests, and war is just one such policy. Regardless of a country's level of technology, type of government, or place in history, the essential nature of the game is the same. War is a violent means of pursuing the goals of national policy.

This insight helps us understand that the underlying principles of geopolitics and war are timeless. Countries employ the full range of instruments of power at their disposal (political, military, economic, etc.) to safeguard their security and advance their interests. These interests inevitably clash with each other, and that leads to war. While the types of instruments are timeless, advancing technology continues to change their forms and capabilities and, hence, the smartest ways to employ them. In the military realm, we still use soldiers, bombs, and bullets, but now we also use satellites, software, and networks to attack each other. ***Attacks using these new technologies may not be as visible as attacks using older***

technologies. They may not even be recognized as an attack, but they are surely felt. Taken to the extreme, one country could conceivably launch an electronic Pearl Harbor on another country, doing real damage, and the citizens of the attacked country might not even recognize it as an act of war. In other words, today's technologies have blurred the line between military and non-military attacks.

Figure 1



Hiroshima, Japan, after US atomic bomb attack (Source: Japaninsides.com)

Technology Through Time. Even Clausewitz, writing 200 years ago, emphasized the impact of technology, as he said, "Violence arms itself with the inventions of art and science in order to contend against violence." Below are several examples of technological advances that have transformed the face of war in the past:

- In the Dark Ages, metallurgical advances produced swords and suits of armor, giving rise to the medieval knight.
- Toward the end of the Medieval Age, the English longbow penetrated armor, rendering the knight obsolete.
- Gunpowder made the firearm possible, changing the range of the fight and the power of the individual soldier.
- The Industrial Revolution enabled the mass production of firearms and other weapons of war, making it a contest of mass of force.
- Air power rendered both forces at the front and production centers on the home front vulnerable to three-dimensional attack.
- Nuclear weapons put the entirety of civilization at risk.
- Space power has transformed the face of war in many ways (which we reviewed in our recent report, "Introducing the U.S. Space Force").

Technology in Our Time. Among the themes and trends that emerge from this historical review of advancing technology's impact on the face of war, citizens and investors would be wise to recognize how one more line seems to have blurred — that which separates the battlefront from the home front. Once upon a time, war took place on a battlefield, often far from home. In World War II, strategic bombing brought the destruction of war to the home cities of most of the countries that fought in the war. How far might this trend go?

Examples of New Technologies

As a first step in considering potential answers to this question, two 21st-century examples provide a glimpse of the possibilities.

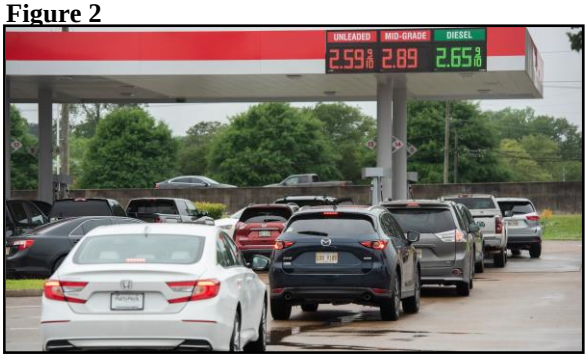
Stuxnet. In early 2010, authorities in the Iranian nuclear program suddenly removed and dismantled roughly 1,000 centrifuges that were being used to enrich uranium, ostensibly for "peaceful" purposes but generally suspected to be a key part of the country's efforts to develop nuclear weapons. They removed the centrifuges because they had been destroyed when their control systems, infected by a computer virus, ordered them to operate in a self-

destructive manner. This damage critically set back the Iranian nuclear program. Although no one has ever taken responsibility for the virus (known as Stuxnet), emerging evidence has credibly attributed its development and employment against the Iranian facility to a collaboration between US and Israeli intelligence agencies and Siemens, the manufacturer of the centrifuges. Was this an act of war? At any rate, the three parties have neither confirmed nor denied association with Stuxnet.

Colonial Pipeline. In May 2021, the Colonial Pipeline, which carries roughly half of the East Coast's petroleum products from the Gulf Coast to locations as far north as New Jersey, shut down for five days. This occurred because a criminal hacking group called Darkside infiltrated Colonial's computer systems and installed "ransomware," a type of software that holds a system hostage until, for a ransom (in this case $5 million, which the company did pay), the necessary decryption software is provided. Once the company paid the ransom and received the decryption software, movement of fuel was restored just as shortages were beginning to be felt. In this case, the perpetrators were determined to be independently acting criminals; however, the incident prompted the Biden administration to step up its activities in the realm of cybersecurity as it relates to critical infrastructure.

For years, the US intelligence community has been warning of the ability of state actors (e.g., Russia, China), with far more capability than a criminal outfit such as Darkside, to execute crippling attacks on national infrastructure. In fact, the Biden administration has also revealed that hackers sponsored by the Chinese government have executed similar attacks on US infrastructure earlier this century. (Please see our previous articles addressing the Colonial Pipeline event, here and here.)

Figure 2



Northeast gas lines after Colonial Pipeline cyberattack (Source: Clarionledger.com)

Cold or Hot War: The Next Blurred Line

If the line between battlefront and home front is blurring, what about the most fundamental line of all — the line between peace and war? The geopolitical confrontation between the US and the USSR from 1945 to 1991 was called the Cold War because the two sides, despite their long stand-off, never used military force directly, although they did occasionally use confrontational policies against each other. For instance, in 1980, the US responded to the Soviet invasion of Afghanistan by imposing an embargo against all exports of US corn, wheat, and soybeans to the USSR. Still, none of these nonmilitary actions actually inflicted violence upon the other. As the name suggests, the Cold War straddled the line.

This reflection begs two questions: If one country commits nonmilitary ***violent*** action against another country, and it causes damage, be it physical, economic, or otherwise, is it an act of war? If so, does this cross the threshold of becoming a "hot" war? The simple but unsatisfying answers to these questions are that we do not know. According to the internationally recognized Law of Armed Conflict, or LOAC (also called "International Humanitarian Law"),

war is defined as a "phenomenon of organized collective violence that affects either the relations between two or more societies or the power relations within a society." Literally interpreted, the Stuxnet and Colonial Pipeline examples would seem to fit the LOAC definition; however, these kinds of cases are also subject to considerable variation in interpretation. Moreover, the country that has suffered the attack must grapple with serious questions concerning the risks of escalation if it responds with countermeasures of its own. These are new, uncharted waters. We cannot draw upon historical precedent to predict how the US would have responded if, for instance, China or Russia had committed the Colonial Pipeline hack, without any recourse to decryption software, and just left the pipeline shut down as fuel shortages rippled across the East Coast. We do feel confident that, whatever form it would take, it would not fit neatly into any historical mold; we would not be calling it a second Cold War.

The China Threat

This conceptual and historical context provides a lens through which to assess the potential threat of "blurred-line" warfare with China, the main geopolitical challenger to the US. Threat assessments conventionally begin with analysis of known capabilities and continue with a consideration of suspected intentions, based on publications and statements made by the leadership of the suspected threat. We follow that method here.

Capabilities. For the last three decades, in addition to its military build-up, China has heavily and steadily invested in a suite of capabilities that could be considered non-traditional or non-kinetic. In military parlance, *kinetic* refers to the use of military forces in ways that apply physical force (bullets, bombs) to cause physical damage. *Non-kinetic* refers to the use of forces (military or non-military) to destroy, degrade, or neutralize enemy resources by means other than physical force. Both Stuxnet and the Colonial Pipeline hack (if they were indeed committed as acts of warfare) would be prime examples of a non-kinetic attack. Chinese investments of this type span a wide range, such as cyber-attack capabilities, lasers capable of blinding satellites, GPS-jamming equipment, and artificial intelligence generators to produce false information. Along with its heavy investments in these areas, in 2015, the Chinese military established a new and independent organization called the "Strategic Support Force" (SSF). The SSF unifies and integrates all of these capabilities into one command structure, and it further coordinates its full suite of capabilities with the rest of the military, the Chinese Communist Party, and the Chinese government. In sum, China certainly has the capability to launch largely invisible, high-tech attacks on the US and/or its allies.

Intentions. In recent publications on national security strategy, military doctrine, and operational guidance, China has provided a blueprint for how it intends to employ these resources. The core operational concept for the Chinese military is called "Multi-Domain Precision Warfare." This concept seeks to incorporate advances in "big data" and artificial intelligence to rapidly identify key vulnerabilities in the US operational system, then combine joint forces across all domains to launch precision strikes (kinetic or non-kinetic) against those vulnerabilities. This concept is nested within what China refers to as a new "Way of War" that views war as an ongoing confrontation between opposing systems rather than a narrower confrontation of military forces. Deeper study of the

documents reveals that these guiding doctrines and operational concepts encompass a broad range of ways to employ any combination of civilian and military resources against a prospective enemy, to weaken it in any way that produces an advantage. Although these documents carefully avoid specific mention of the US, the profiles of a "prospective enemy" unambiguously describe the US.

Taken together, this combination of developed capabilities and stated intentions describe a challenger whose view of what constitutes war and how to wage it go well beyond traditional concepts. We could already be in a state of war without the everyday citizen quite knowing it.

Figure 3

Insignia of China's Strategic Support Force (Source: Ebay.com)

Investment Implications

It bears repeating: ***Higher inflation and interest rates*** are two key hallmarks of a society at war with another major power. Many other factors also cause inflation and rising rates; this is not to say that if rates and inflation are rising, we must be at war. However, if we are at war, we should expect rising prices and higher rates for at least the duration of the conflict. This held true even during the Cold War, a period when, on average, inflation and interest rates were higher than they have been in the 33 years since it ended. If the risk of war has increased, investors should take the prospect of rising prices and rates into account across their investment and portfolio-construction decisions.

There is one scenario in which only inflation would rise, while rates would stay relatively low. During World War II, the Treasury forced the Federal Reserve to fix rates along the entire yield curve (i.e., all maturities) to keep borrowing costs low. To perform this role, the Fed was required to buy up Treasury debt, leading to a massive expansion of its balance sheet. At Confluence, we expect something similar again; however, just because long rates do not rise, that does not necessarily make long-maturity Treasurys a good investment. By artificially holding down bond yields, such a policy would mean that bondholders would lose money slowly in real terms, even if the actual prices of Treasurys do not decline.

Let's return to the original question of whether we would even know it if we were at war, which gives rise to the follow-on question of what to do as investors if we are not sure. Societies think in terms of whether to move their economies to a "war footing," in which resource allocation decisions across industry and finance prioritize defense production above the peacetime priorities of profits and prosperity. In this environment of increasing risk, should society shift to a war footing? In our observation, with trends such as the reshoring of supply chains, increasing attention being paid to the defense-industrial base, and rising support for larger defense budgets, this is already happening. At Confluence, we are incorporating this worldview into the full range of our analysis. In this sense, we are working to help investors shift to a war footing as well.

Daniel Ortwerth, CFA
April 22, 2024

This report was prepared by Daniel Ortwerth 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.