ALPINEMACRO
A Unique Mind On The Markets

INNOVATION THEMES & STRATEGY

November 6, 2024

The Unseen Battle: The Growing Unconventional Warfare Threat

In This Report

It is no secret that the current perilous geopolitical climate has thrust the globe into a re-armament super-cycle not seen since the Cold War. The ongoing conflict in Ukraine, a destabilized Middle East, and escalating tensions between BRICS and the West are driving military expenditures to unprecedented levels. This year, global defense spending is projected to surpass last year's record of $2.44 trillion.

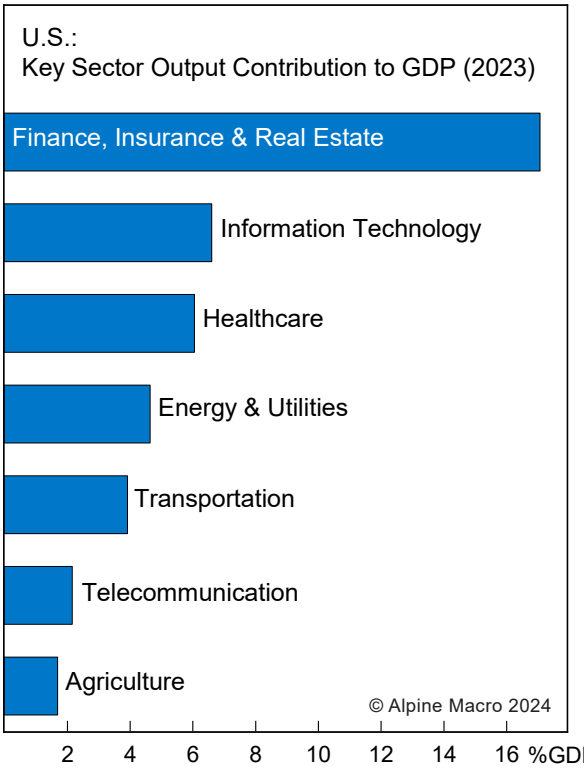
While the possibility of full-blown combat between global powers cannot be dismissed, we believe that the most pressing threat lies in unconventional warfare fought on novel fronts that challenge traditional military responses. This is known as "gray-zone" aggression.

The Wests' renewed focus on enhancing conventional combat capabilities has left it ill-prepared to counter nontraditional tactics and weapons that seek to destabilize society and incite chaos. Indeed, retired U.S. Vice Chairman of the Joint Chiefs of Staff Gen. John E. Hyten has warned that U.S. is largely failing to address "hybrid" warfare threats coherently.

Unlike conventional warfare, which is often centered on geographical gains or inflicting enemy casualties, unconventional tactics target an adversary's homeland and aim to disable critical infrastructure, cripple GDP, and disrupt societal functions (**Chart 1**). Notably, striking first is prioritized in unconventional warfare as the impacts are often devastating.

In our view, the most dangerous unconventional warfare attacks include a paralyzing cyber-attack on part(s) of critical infrastructure, both kinetic and non-kinetic weapons capable of destroying critical space assets, an electromagnetic pulse (EMP)

Chart 1 Critical Infrastructure Is A Vulnerable GDP Lynchpin



 COPYRIGHT © 2024 ALPINE MACRO

attack[1], or an assault on either subsea power or internet cable infrastructure.

Adversarial capabilities across unconventional warfare are becoming increasingly advanced. For instance, the head of U.S. Space Command has noted both China and Russia's progress in nuclear and space weaponry has been "breathtakingly fast", while the director of the FBI has warned that Chinese hackers are strategically planting threats across critical infrastructure to "wreak havoc" on U.S. soil in the event of heightened U.S./China contention. Notably, China has combined space, information and cyber warfare operations to form a new branch of the PLA dubbed the "Strategic Support Force".

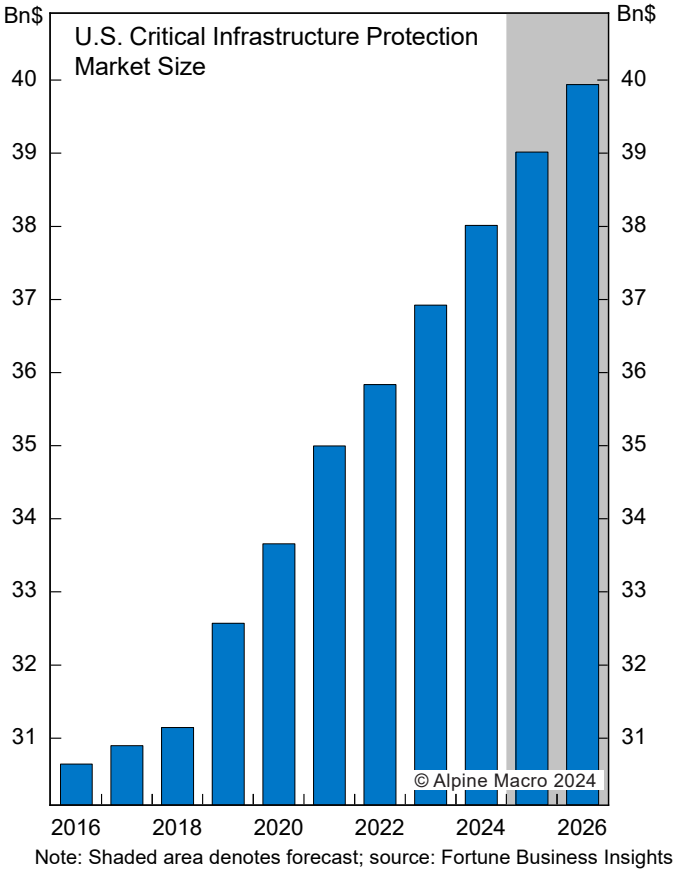
Accelerating Western adoption of technologies that enable proactive protection of vital national assets within critical infrastructure offers a unique way to diversify defense-sector investment (Chart 2). This report will examine the main threats associated with unconventional warfare and highlight the technologies that are most effective in countering them.

Looming Cyber Threats

The digitalization of essential infrastructure made almost all critical systems vulnerable to cyberattacks (Chart 3). The initial strike or "first shot" of unconventional war is likely to be a cyberattack. Cyberattacks on critical infrastructure are the "new geopolitical weapon," notes a new report from

1 An EMP releases a burst of electromagnetic energy, typically generated by a high-altitude nuclear explosion, that can disrupt or damage electronic devices and systems by frying the circuit board.

Chart 2 Growing Trend Of Hardening Critical Infrastructure

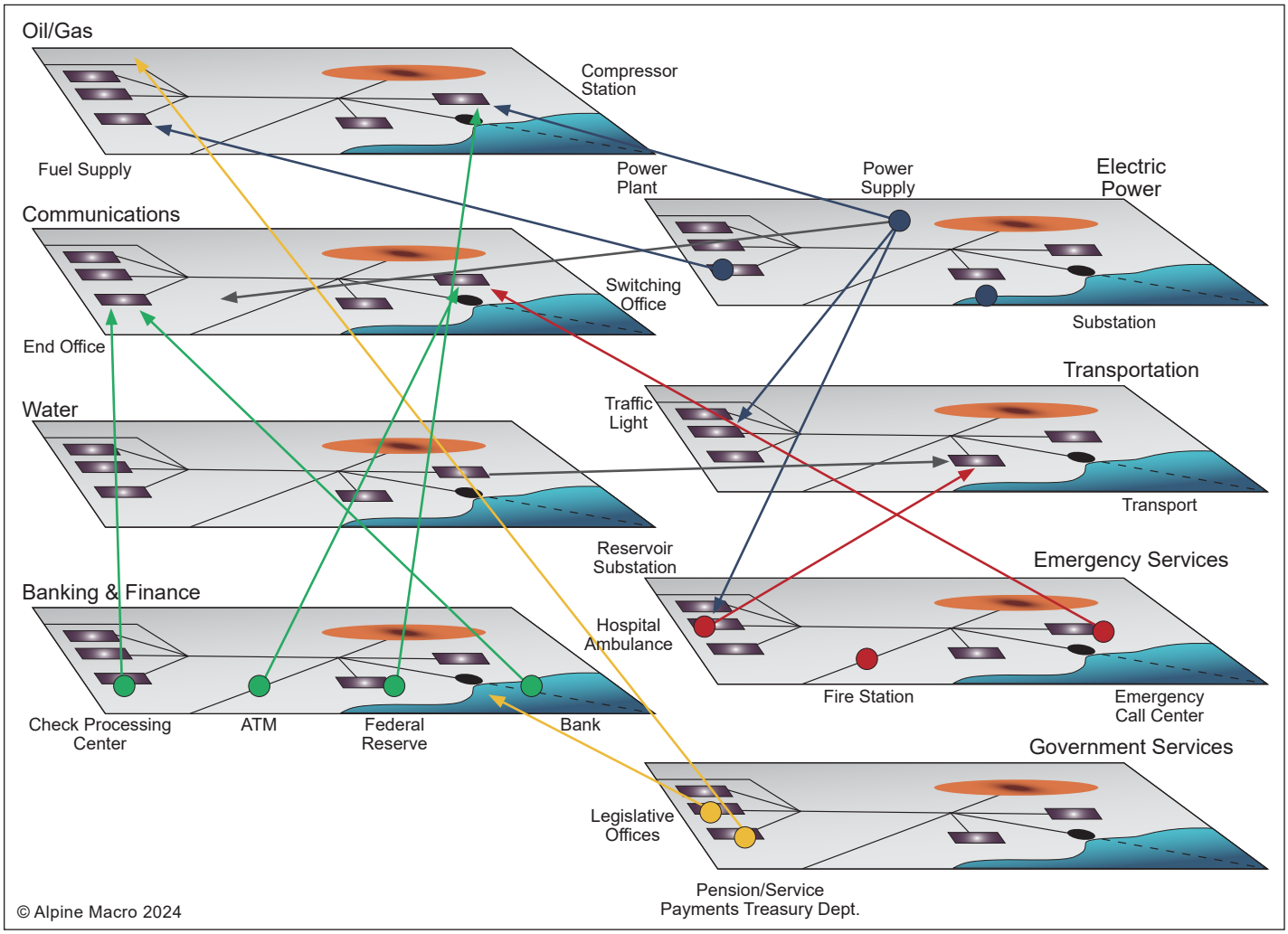


Note: Shaded area denotes forecast; source: Fortune Business Insights

cybersecurity firm KnowBe4. The "threshold" for launching a cyberattack is significantly lower than traditional combat as it does not require boots on the ground and focuses on disrupting civilian life instead of inflicting casualties. Furthermore, swiftly identifying the perpetrator is exceptionally challenging, possibly making counteracting often impossible.

Cyberattacks on critical infrastructure are rapidly increasing. Between January 2023 and January 2024, there were 420 million cyberattacks (roughly 13 attacks per second) on critical infrastructure globally. The U.S. was the primary target, where attacks on critical infrastructure increased by 30%

Chart 3 Digitalization Has Fueled Interconnectedness of Critical Infrastructure



Source: EMP Commission

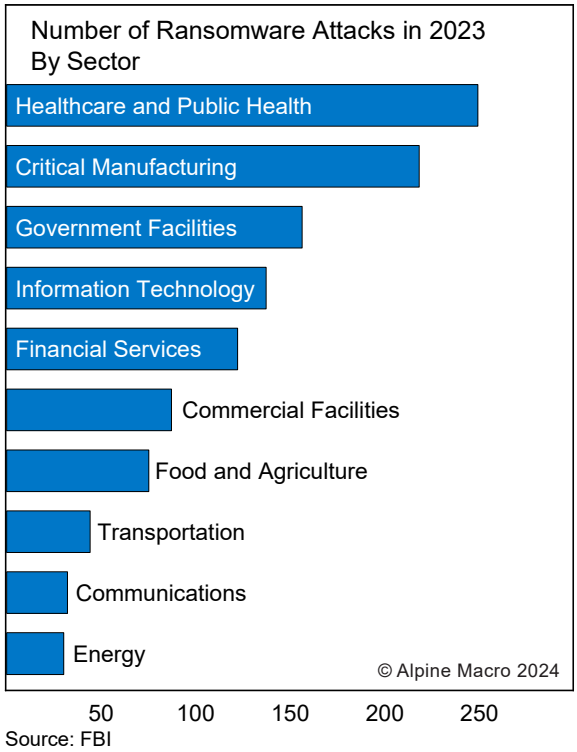
last year (**Chart 4**). FBI data shows that over 2 in 5 ransomware attacks reported to the FBI in 2023 targeted organizations in a critical infrastructure sector (**Chart 5**). 14 out of 16 critical infrastructure sectors fell victim to an attack.

Energy infrastructure is particularly vulnerable and is experiencing a growing number of attacks. According to the IEA, the average number of cyberattacks against utilities worldwide each week more than doubled between 2020 and 2022, before doubling again last year. In the U.S. specifically, 185 reports of energy security incidents were reported to the DOE last year alone – a record high. As we noted in our U.S. power grid report[2], the number of points on the U.S. power grid vulnerable to cyberattack is increasing by 60 per day and now stands between 23,000 to 24,000.

The potential threat to the power grid is significantly underestimated. A report by the Federal Energy Regulatory Commission highlights that at least 30

2 Alpine Macro *Innovation Themes & Strategy* "The U.S. Grid: Revamp Time" (July 31, 2024).

Chart 4 Breadth Of Cyberattacks



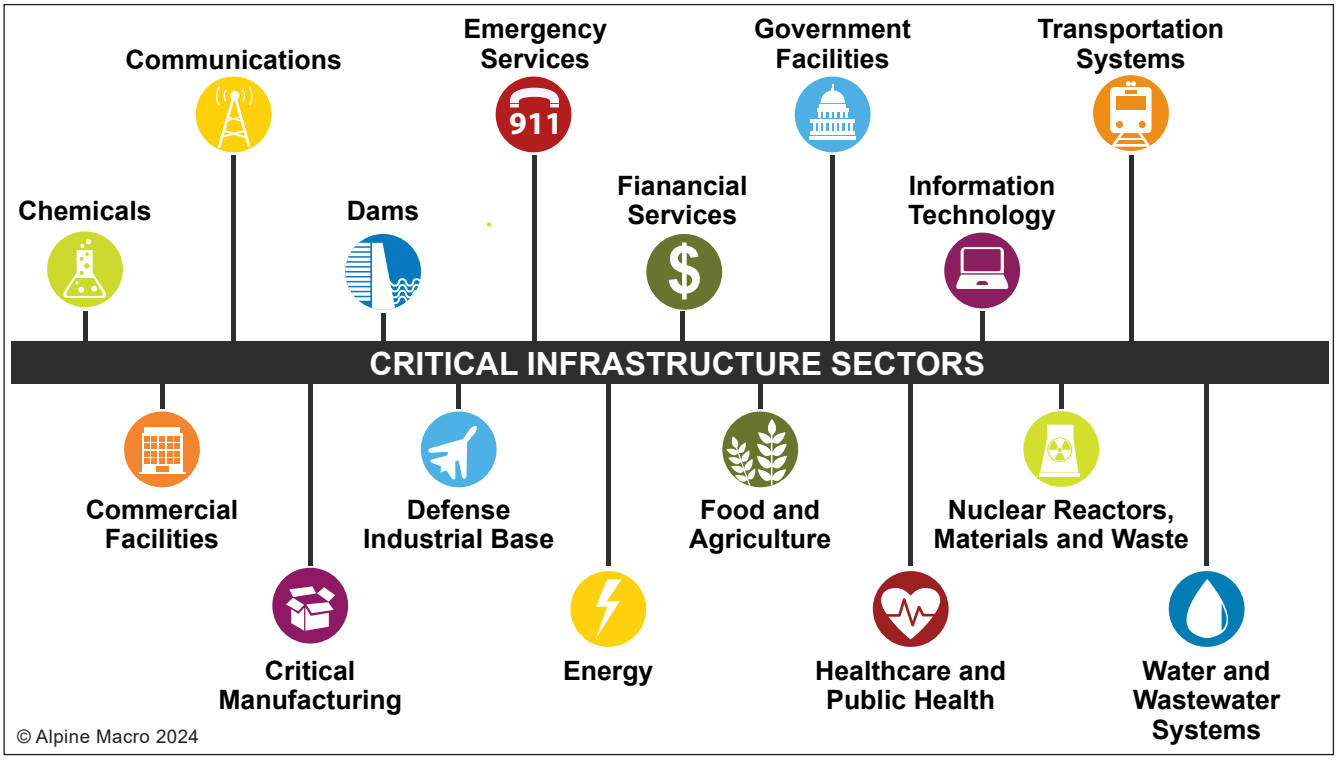
Source: FBI

out of 55,000 substations on the U.S. grid are critical to ensuring energy reliability. If just nine critical substations are taken offline, the U.S. power grid could face nationwide blackouts lasting 18 months or more. Alarmingly, most cyberattacks on energy infrastructure are going unreported.[3]

The most disruptive cyberthreats are "hiding in plain sight" and waiting to be sprung at a time of strategic importance. The U.S. is working to quantify the extent to which Chinese state-backed hacking group Volt Typhoon has placed malware within America's critical infrastructure. Some of the group's malware has been removed. Although the

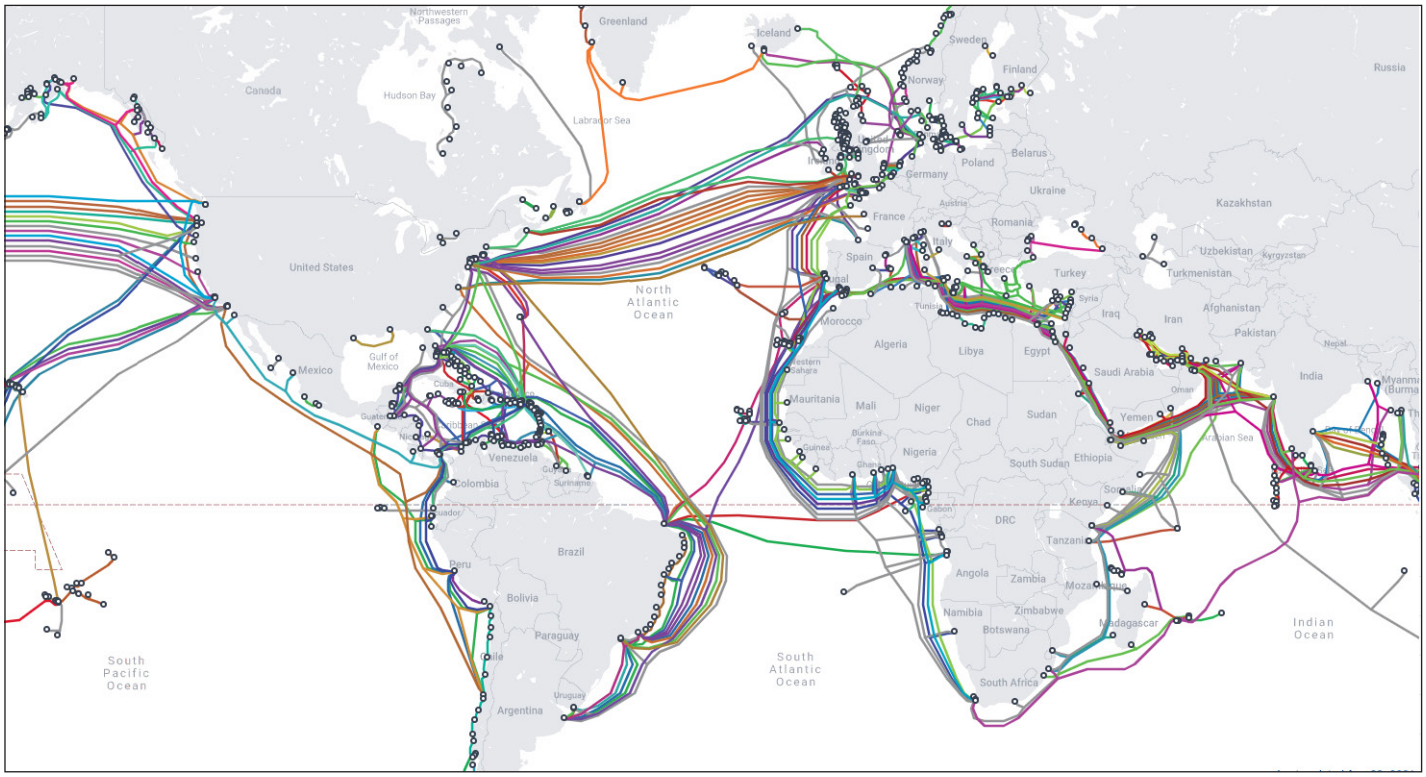
3 A recent FBI infiltration of the Hive ransomware group's infrastructure revealed that only approximately 20% of Hive's victims reported the attacks to law enforcement.

Chart 5 16 Critical Infrastructure Sectors Are Prime Targets Of Unconventional Warfare



Source: Pan-European Training, Research and Education

Chart 6 Subsea Cable Web



Source: Telegeography

Cybersecurity and Infrastructure Security Agency has flagged that traps planted by Volt Typhoons remain undetected and could lead to widespread *"disruption or destruction of critical services in the event of increased geopolitical tensions and/or military conflict with the United States and its allies."* These "undetected timebombs" concern us greatly.

Cable Susceptibility

Subsea cable infrastructure, as well as their cable landing stations, are an attractive target of unconventional warfare tactics. The geographic scope of such infrastructure, comprised of roughly 600 cables stretching almost 1.5 million, makes it nearly impossible to adequately protect it against malicious activity (**Chart 6**). These high-speed fiber-optic underwater "data veins" are the backbone telecommunications and support over 99% of global internet traffic, $10 trillion in daily financial transactions, and essential military and government communications.

Subsea cables are growing more vulnerable daily due to backdoor threats from governments increasing their control over internet firms and more companies using remote network management. Both developments heighten cyber risks by enabling hacking from multiple points at distance. However, the largest threat stems from the recent increase in naval activity, specifically from Russia and China, near critical subsea cables. Russian and Chinese submarine activity, specifically in areas with a

Russia China bad! WHITE PEOPLE BEST

high density of subsea critical infrastructure, has amplified concerns.

The number of "suspicious" tampering incidents leading to internet blackouts cannot be overlooked. Last year, a cable incident blamed on Chinese vessels cut the only two submarine cables that supply internet to Taiwan's Matsu Islands, leaving 14,000 residents into digital isolation for six weeks. Since 2018, Taiwan has experienced over 27 cables subsea disruptions. European nations are also seeing growing cable incidents and disruption in the Baltic Sea region. Russia, whose Navy is highly active in the Baltic region, is prioritizing building up a dedicated military unit surface ships, submarines, and naval drones with specialized cable-tampering capabilities.

China's expanding control of the subsea cable market is also noteworthy and a new threat. Roughly 98% of subsea cables are produced and installed by four firms, with China's HMN Technologies holding the smallest market share. However, the firm has become the world's fastest-growing subsea cable builder; providing 18% of the subsea cables laid and "built or repaired" almost 25% of subsea cables over the past four years.[4] Overreliance on Chinese repair ships from limited alternatives make even Western cables vulnerable to espionage and allows China to collect sensitive data.

Space-Based Weakness

While space appears as a separate domain from Earth, many essential terrestrial technologies rely on space infrastructure. As we noted in our July space memo[5], weather forecasting, remote sensing, navigation systems (GPS), missile defense/detection, and long-distance communication systems are all reliant on space-based infrastructure. As a result, disabling key space assets, in particular satellites, is a prime target in the unconventional warfare arena. Both China and Russia have developed and demonstrated various space weapons.

The rapid advancement of Sino/Russian space-weapon systems has caught the West off-guard. Weapons showcased include grappling arms designed to remove other satellites from orbit, as well as "kinetic kill vehicles" capable of targeting satellites, and space-capable long-range ballistic missiles, and hypersonic glide vehicles. China has also showcased an unmanned and reusable spaceplane. Most disturbingly, U.S. intelligence has noted that Russia is developing "indiscriminate" space-capable nuclear weapon. Putin has already warned that if NATO crosses Russia's "red line", NATO risks losing all 32 GPS satellites at once. Overall, China's space-weaponry is focused on "targeted" attack capabilities due to their dependence on satellite infrastructure, while Russia appears to be taking an indiscriminately destructive approach.

The hardening of space assets is finally being recognized as essential by Western nations. Last year, the U.S. Space Force experienced a sixfold increase in demand for foreign military sales, a growth attributed to the rising significance of space systems across national security and global commerce.

4 Center for Strategic and International Studies

5 Alpine Macro *Innovation Themes & Strategy* "The Intensifying Space Race: Key Insights For Investors" (July 10, 2024).

The EMP "Wildcard"

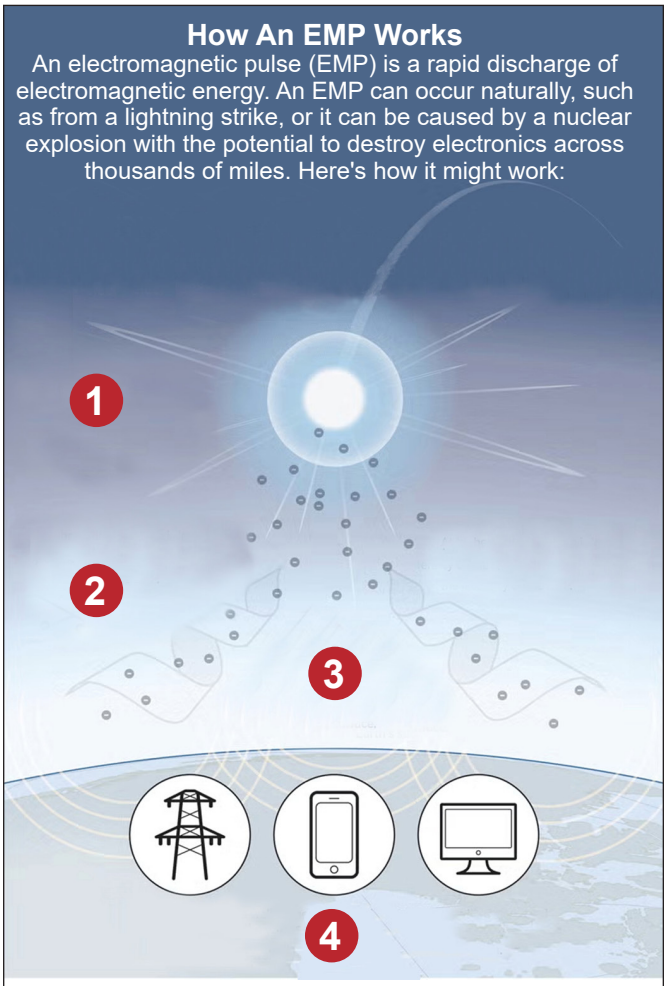
The most paralyzing unconventional warfare weapon is an EMP (Chart 7). Importantly, an EMP could be used in conjunction with the other unconventional warfare tactics above to knock out technology-dependent infrastructure from all sides, crippling the targeted nation(s). Models indicate that the detonation of a high altitude EMP (HEMP) above Chicago could potentially disable the entire electrical grid and critical infrastructure in the lower 48 for over a year.

The concern over EMP use has come back to the forefront. Specifically, pertaining to Russia using a tactical EMP attack over Ukraine to disable critical infrastructure. While we are in the camp that nuclear deterrence continues to remain extremely effective, the bar for an EMP attack is lower. Crucially, in both Russian and Chinese military doctrines, EMPs are not classified as nuclear warfare. Instead, EMP strikes, specifically HEMPs, are classified as cyber warfare.

The nuclear "temperature" is undoubtedly yet again rising. All nine nuclear-armed states are modernizing and/or adding to their arsenals. This marks a shift from the de-arming cycling that proceeded the post-Cold War era. Last year, the nuclear powers spent a combined total of over $91.4 billion on their arsenals – equivalent to $2,898 per second. Yearly spending has increased by 34%. By 2035, China's nuclear arsenal is set to scale to 1,500 warheads up from about 500 today.

The prospect of an EMP attack brings forth severe ramifications. Current missile defense capabilities make it challenging to reliably neutralize a HEMP threat with a high degree of confidence. HEMPs can be deployed with novel launching mechanisms

Chart 7 Electromagnetic Pulse Impact



Source: Heritage Foundation Research

Table 1 Technologist That Build Resiliency To Unconventional Warfare

Threats	Key Technologies
Cyberattack	Next-generation encryption (including post-quantum cryptography), zero trust architectures, cyber-specialized sensors (network, endpoint, cloud), edge computing, defensive AI
Subsea Cable	Cable monitoring sensors, autonomous underwater monitoring/repair vehicles, satellite infrastructure (surveillance and communications systems), self-healing subsea cables, advanced cable manufacturing, ship laying cables
Space War	Next-generation positioning technologies, next-generation satellite missile detection systems, space-based command and control systems, CubeSats, payload launch providers, kinetic and non-kinetic space weaponry
EMP	EMP-rated cables and connectors, EMP-proof coatings and paints, redundant energy grid Infrastructure, hardened smart/microgrids, HVDC lines, satellite communication backups, satellite-based EMP monitoring and sensing

including hypersonic glide vehicles. China has successfully deployed a hypersonic glide vehicle that circumnavigated the entire globe, something no Western power has achieved. Intelligence also suggest China has “super EMP” capabilities, a weapon that generates bursts of energy much stronger than prior versions.

Key Takeaways

The rise of unconventional warfare is creating a disruptive technology-driven investment opportunity for investors seeking to diversify defense sector portfolio positioning. Confrontations in the “gray zone” require proactive hardening of hardware and software across domains not usually targeted by traditional combat. The looming threats outlined above are driving the development of redundant or "backup" systems to serve as fallbacks in case critical infrastructure is compromised.

While the U.S. and Western countries are largely on par with China and Russia in offensive unconventional capabilities – such as cyberattacks, cable tampering, and EMP technology – space weapon systems are emerging as a weakness. This vulnerability raises the likelihood of adversarial attacks on Western space assets, especially given that Western terrestrial technologies are disproportionately reliant on these orbital assets compared to those of Eastern nations.

Table 1 highlights key technologies/products critical to fortifying critical infrastructure and poised to see use cases proliferate. We believe that technologies capable of serving as multi-purpose "hardening tools" against various threats will be prioritized, leading to faster adoption rates. In our view, advanced sensors, space-based systems, and AI-enabled cybersecurity solutions fit this classification well.

Noah Ramos
Global Strategist

EDITORIAL BOARD

Noah Ramos
Global Strategist

Chen Zhao
Chief Global Strategist

Aishwarya Tyagi
Research Analyst

David Abramson
Chief U.S. Strategist & Director of Research

Disclaimer and copyright restrictions © Alpine Macro 2024. All rights reserved.

The information, recommendations, analysis and research materials presented in this document are provided for information purposes only and should not be considered or used as an offer or solicitation to sell or buy financial securities or other financial instruments or products, nor to constitute any advice or recommendation with respect to such securities, financial instruments or products. This document is produced for subscribers only, represents the general views of Alpine Macro, and does not constitute recommendations or advice for any specific person or entity receiving it. The text, images and other materials contained or displayed on any Alpine Macro products, services, reports, emails or website (including this report and its contents) are copyrighted materials proprietary to Alpine Macro and may not be circulated without the expressed authorization of Alpine Macro. If you would like to use any graphs, text, quotes, or other material, you must first contact Alpine Macro and obtain our written authorization. Alpine Macro relies on a variety of data providers for economic and financial market information. The data used in this publication may have been obtained from a variety of sources including Bloomberg Finance L.P., Macrobond, CEIC, Choice, MSCI, BofA Merrill Lynch and JP Morgan. The data used, or referred to, in this report are judged to be reliable, but Alpine Macro cannot be held responsible for the accuracy of data used herein.