

## Imposing Costs in the Indo-Pacific: Lessons from Operation Spider Web

### Description

In June 2025, Ukraine launched over 100 drones to strike five air bases and a number of long-range bombers deep in Russian territory. Ukraine launched the drones simultaneously using a mix of remote control and artificial intelligence (AI) targeting software to destroy several Russian strategic bombers, and covertly smuggled drones inside Russia via modified trucks with hidden launch compartments. Dubbed [“Operation Spider Web,”](#) the operation stands as one of [the most sensational instances in recent history](#), and stands apart for the use of conventional weapons to destroy nuclear-capable delivery platforms.

At first glance, using AI-enabled conventional weapons to strike infrastructure that enables nuclear operations may seem like a novel concept. For years, however, Chinese strategists have [debated](#) the impact of drone warfare on nuclear survivability. Ukraine’s successful operation likely validated the already strong fears of Chinese experts alarmed by the threat drones pose to nuclear forces. The United States and Indo-Pacific partners would be wise to learn important lessons from Spider Web in order to impose costs on China’s nuclear forces if future scenarios required it.

### China’s Lessons Learned from Operation Spider Web

Chinese experts have long [noted](#) concerns over non-nuclear weapons threatening the survivability of China’s nuclear weapons. Since the United States demonstrated its superiority in precision-guided warfare during the 1990s, Chinese defense planning has focused on the threats of U.S. precision-guided munitions to high-value assets. China’s National Defense University has observed that precision strike capabilities can be used to [strike](#) an adversary’s nuclear forces. Other observers similarly [argue](#) that non-nuclear strategic weapons, such as long-range precision strike weapons and weapons from space, will threaten China’s nuclear survivability.

Analysts from the *PLA Daily*, the official mouthpiece of the People’s Liberation Army (PLA), [identified](#) the use of drone swarms as a viable operational concept in 2021, [referring](#) to saturation attacks that overwhelm adversary defenses to pre-emptively attack nuclear and non-nuclear mobile missile launchers and auxiliary nuclear infrastructure. Although other Chinese academics have [argued](#) that the remote locations of nuclear delivery systems may limit the effectiveness of drones, Operation Spider Web likely validates the viability of such an operational concept in practice.

In the eyes of Chinese commentators, Operation Spider Web [challenges](#) the conventional assumption that only long-range strike capabilities can meaningfully threaten air bases deep in adversary territory or meaningfully challenge their strategic deterrence capabilities. Analysts in Xinhua highlight that this blurring of frontlines and rear areas in warfare [brings with it](#) a decreasing technical threshold for executing such operations and increased difficulty in counter-unmanned aircraft systems (counter-UAS) requirements.

Complicating matters further, Chinese researchers have noted that drones attached to fiber optic cables do not rely on radio, rendering ineffective the traditional forms of counter-UAS warfare, such as electronic interference and jamming. Operation Spider Web effectively [eroded](#) Russia's strategic nuclear deterrence and represented a "systems breach" that exposed systemic cost asymmetries between Russia's expensive air-defense platforms and Ukraine's low-cost drones. Even with range limitations for fiber-optic drones, Operation Spider Web was novel in its ability to penetrate deep into adversary territory at a low cost while damaging Russia's strategic bomber fleet. As a result, one associate professor at Renmin University's School of International Relations [predicted](#) that Operation Spider Web would set a precedent for non-nuclear countries to develop capabilities to strike strategic nuclear forces.

## Imposing Costs on China's Strategic Rear

Because Chinese strategists are concerned with drones' effectiveness in targeting strategic platforms, the United States should consider integrating drones into U.S. nuclear signaling to force China to invest in expensive defensive countermeasures at comparatively lower costs to the United States. For instance, China [has been developing](#) an "underground great wall" consisting of 3,000 miles of underground tunnels to launch ballistic missiles and reinforce China's secure second strike capability, and more recently, China has been [building](#) a military facility in Beijing, on track to be 10 times larger than the Pentagon, that will serve as a nuclear bunker and command center. To support nuclear counterstrike capabilities and command and control, the Department of Defense [assessed](#) that China "will likely continue to develop and expand its [underground facility] program to support its expanding forces and military modernization."

These major programs have astronomical costs, giving the United States an opportunity to shift the focus of competition toward more advantageous cost ratios. According to China's Global Television Network, costs to build a subway in China [range](#) from \$72.6 to \$172.4 million per kilometer. China's underground tunnels are missile launch bases [intended](#) to reinforce survivable second strike capabilities, and likely have greater depth requirements and increased costs compared to traditional subway systems.

In contrast, the per-unit cost of deploying drones is orders of magnitude lower than the cost of hardened underground infrastructure. Each drone can serve as a cheap and persistent surveillance or strike threat, forcing China to invest heavily at a disadvantageous cost differential to maintain the survivability of its missile forces. Leveraging drones to encourage China's tunneling proclivities can divert China towards less threatening defensive measures spread across a vast geographic area, pulling them away from the operational scenarios the United States may face on China's eastern seaboard.

Even though drones are unlikely to destroy hardened silos, the United States can integrate drones in its nuclear signaling and strategic forces exercises targeted at vulnerabilities in China's auxiliary nuclear infrastructure. As China [pursues](#) an early warning counterstrike or a launch-on-warning posture, China's fixed ground-based radar systems and remote sensing satellite ground stations are nevertheless vulnerable targets. Similar to China's spy balloon that penetrated U.S. airspace in 2023, demonstrating the ability to penetrate Chinese airspace and hold components of Chinese high-value targets at risk exploits China's existing perceptions on the vulnerability of their critical assets relative to the low cost and flexibility of drone operations. Additionally, publicizing the [deployment](#) of drones equipped with ground-penetrating radar, high-resolution thermal imaging, and advanced Light Detection and Ranging (LIDAR) technology to demonstrate the United States' ability to detect, map, and monitor underground facilities from the air would signal to Chinese planners that their tunnel networks are increasingly vulnerable to detection, targeting, and sabotage, which could force them to consider further investment in costly concealment and redundancy measures.

Chinese analysts have highlighted [the vulnerability](#) of U.S. strategic aircraft stemming from a lack of hardened hangars. According to a [Hudson Institute survey of satellite imagery](#), China has constructed more than 400 aircraft shelters in the last decade, [while the United States has added only 22](#) in the Indo-Pacific over the same period. This disparity underscores how seriously the PLA has worked to mitigate vulnerabilities that U.S. forces have left largely unaddressed.

Although most of China's shelters are concentrated near its coast and the Taiwan Strait, its rapid expansion highlights a critical gap in U.S. infrastructure—one that drones could exploit in a future conflict.

## Conclusion

Operation Spider Web's success was not merely in the destruction of high-value assets, but in its ability to also sow doubt, temporarily distract an adversary and disrupt its planning, and expose the fragility of seemingly secure rear areas. As China is increasingly able to mobilize a greater portion of its massive economy for national defense and strategic competition, the United States must continue to

search for and exploit asymmetries that exploit China's vulnerabilities and force Beijing into expensive or inefficient countermeasures. The heightened threat perception from drone warfare among Chinese analysts, the low cost of building and employing drones, and existing Chinese doctrine on defense and conflict management create conditions for the United States to potentially strain China's defense apparatus and impose costs in a cost-effective manner.

---

*Alexander Richter is an undergraduate at UC Berkeley. He is majoring in political science and economics.*

*Ethan Chiu is a BA/MPP student at Yale University studying Global Affairs and History.*

*Main Image generated by ChatGPT using DALL·E, OpenAI (Sept 17, 2025).*

*The views expressed are those of the author(s) and do not reflect the official position of the Irregular Warfare Initiative, Princeton University's Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.*

*If you value reading the Irregular Warfare Initiative, please consider [supporting our work](#). And for the best gear, check out the [IWI store](#) for mugs, coasters, apparel, and other items.*

---

**Date Created**

2025/10/06