Spectacular Drone Strikes and the Future Sanctuary of the U.S. Homeland

MICHAEL POZNANSKY AND ERIK SAND

August 27, 2025

How vulnerable is the continental United States to drone attack? Could a wily adversary cause vast destruction of military assets on U.S. soil at a fraction of the cost it would take to replace them? Ukraine and Israel's stunning drone attacks against high value targets deep within Russia and Iran, respectively, in June 2025 raise serious questions about whether the United States homeland will remain a sanctuary. America has long enjoyed the advantages of favorable geography. Aside from nuclear-armed missiles, the continental United States has largely remained out of reach of conventional kinetic attacks from major adversaries.

While fears about the revolutionary potential of these drone attacks — Ukraine's Operation Spider's Web and Israel's Operation Rising Lion — are understandable, they are potentially overstated. On the one hand, they clearly show that even inexpensive, short-range drones can be used to cripple critical infrastructure deep inside enemy territory, a feat that would have previously required tools like long-range precision missiles or exquisite cyber capabilities. And yet, their spectacular nature is precisely what makes them so extraordinary. They are hard to pull off and hard to repeat.

The key lessons lie in what made them possible in the first place. These strikes were more than a matter of buying cheap drones and hitting hard-to-reach targets. They relied on detailed intelligence, elite special operations forces, and extensive logistical coordination, all hallmarks of state actors with impressive organizational capacity. In this sense, they resemble high-end cyber operations — and large intelligence operations more broadly. While cheaper, less impactful cyber tools are widely available, the most bespoke and consequential operations largely remain the purview of highly capable state actors. These drone attacks also resemble cyber operations in that they are burned once deployed. This makes them most useful for a first strike in the opening stages of a war or during protracted conflict. Drawing the right lessons from these operations is essential for right sizing the threat and mitigating damage should a highly capable adversary attempt to pull off such an attack against the United States.

Growing Threats to Sanctuary

With massive oceans on each coast and friendly neighbors to the north and south, the continental United States has long had sanctuary from conventional attacks. The challenge of generating military effects across large distances meant nuclear-armed ballistic missiles were the primary way America's rivals could threaten its homeland. Nuclear weapons compensated for conventional intercontinental ballistic missiles' chief weakness — their lack of precision — but their practical military utility was limited for a variety of reasons.

This picture has changed in recent years. Emerging technologies are shrinking the globe and chipping away at sanctuary from non-nuclear attack by major adversaries. Many have warned that cyber tools make it possible for states to reach into the territory of rivals from thousands of miles away, wreaking havoc on cities, ports, and bases. The 2018 *National Defense Strategy* identified cyberspace, along with other non-conventional threats, as a major challenge to the sanctuary of the homeland.

With respect to kinetic weapons, the revolution in the precision of intercontinental ballistic missiles is perhaps the greatest threat to physical sanctuary on the horizon. As one of us argues in a forthcoming article, "Strategy in the New Missile Age," technological improvement will soon enable great powers to build conventional intercontinental ballistic missiles that are both relatively cheap and precise enough to be militarily relevant — at least with good intelligence, reconnaissance, and surveillance and against unhardened fixed targets as well as, potentially, relocatable targets. Air-launched cruise missiles, including from long-range bombers, represent another potential threat to physical sanctuary.

What made the recent Ukrainian and Israeli operations so spectacular is that they used short-range drones in ways that approximated long-range strike capabilities. The result was consequential kinetic effects deep inside enemy territory. Ukraine's gambit, known as Operation Spider's Web, used over 100 cheap, pre-positioned drones to target multiple Russian airbases housing nuclear-capable bombers across five different time zones. The drones relied on commercial autopilot software known as ArduPilot and used AI for targeting. Ukraine estimated that they caused $7 billion in losses for Russia.

Less than two weeks after Ukraine's operation, Israel carried out its own stunning attack against Iran. Operation Rising Lion entailed many moving parts, including the assassination of Iranian nuclear scientists. Most germane here was Israel's use of drones pre-positioned at key locations. When the military operation commenced, small drones disabled air defense and ballistic missile launchers in Iran, contributing to Israeli air superiority.

Commentary on these operations has rightly pointed to their spectacular nature, emphasizing the distance at which attacks occurred from their perpetrators' bases as a major achievement. In *Foreign Affairs,* Michael Horowitz, Lauren Kahn, and Joshua Schwartz argue that these strikes showcase how vulnerable expensive systems are "to cheap, precise mass capabilities, no matter how deep into a country's territory they are." Writing in *War on the Rocks*, Michael Hunzeker and Yuster Yu observe that "Ukraine's daring, multi-axis strike showed that drones can serve as a cheap and effective way to conduct highly precise 'long range' strikes (by virtue of having been covertly pre-positioned near Russian bases far from the front) with little to no warning." Katja Bego of Chatham House notes that Ukraine's attack in particular "offered a glimpse into the future of warfare, transformed by access to cheap, widely available technology such as small drones, in which anything, anywhere can become a target."

Recentering Hidden Constraints

There is no question that Ukraine and Israel's operations were breathtaking in scale and scope. They were also ingenious in design and execution. But that is precisely the point. Their sheer logistical complexity makes them less like increasingly precise intercontinental ballistic missiles and more akin to high-end cyber and intelligence operations. As with the use of drones on the frontlines in Ukraine,

malicious cyber operations occur constantly. But the most destructive and costly attacks are exceedingly hard to pull off. They take months and sometimes years to plan. They require highly specialized intelligence including a detailed understanding of usually closed and hardened networks. An unexpected change in the environment — such as an inopportune software update or a password change — can jeopardize entire operations. In other words, they are complex, logistically taxing, and necessitate many things all going right in succession. These attributes aptly describe Ukraine and Israel's operations.

According to President Volodymyr Zelenskyy, Operation Spider's Web unfolded over the course of a year and a half from start to finish. That puts the initial inception date around late 2023 or early 2024. The drones were smuggled into Russia and inserted into wooden cabins with detachable, remotely controllable roofs that were loaded onto trucks. The unsuspecting Russian drivers received phone calls telling them where to stop upon nearing their intended targets. The AI systems were reportedly trained on decommissioned Russian bombers housed in military aviation museums in Ukraine to aid in target recognition and the identification of weak points.

The Israeli operation was similarly complex. Israel's spy agency, Mossad, started planning for the use of drones as part of a broader operation several years back. Israeli intelligence knew where Iranian missiles were located "but needed to be in a position to attack them given the country's size and distance from Israel." Israel smuggled the parts for quadcopters along with explosives into Iran over the course of months. They used "suitcases, trucks, and shipping containers" in conjunction with unwitting business partners as part of the effort. Once the materials were in country, "Agents on the ground would collect the munitions and distribute them to the teams. Israel trained the team leaders in third countries, and they in turn trained the teams." In other words, in both cases there was a lot that had to go right to pull off these operations — and a lot that could have gone wrong.

None of this should be taken to mean that a similar attack on critical targets, including military bases inside the United States or abroad, is out of the realm of possibility. It is not. But emphasizing these operations' revolutionary nature without accounting for their complexities and the organizational prowess on display paints a misleading picture. For its part, Israel's Mossad is among the most capable intelligence services in the world, particularly in the Middle East. And while Ukraine is much weaker than Russia, certain cultural and linguistic similarities combined with years of hard-fought experience becoming a world-class leader in the use of drones likely contributed to the operation's success. And yet, both countries still spent years preparing and there was a lot that could have ultimately gone awry.

Learning the Right Lessons

What does all of this imply for U.S. strategy? First, while detecting and defeating incoming drones against high value targets at places like military bases is vital, the long lead times involved in the Ukrainian and Israeli operations suggest an opportunity to try to identify and thwart threats far left of launch. What made these operations tactically different, and more difficult to defeat, than traditional sabotage efforts was that no human was needed to gain direct access to the target bases or the supply chains that support them to plant explosives. It is therefore critical to focus on detecting and disrupting plots before they materialize, a relatively traditional counterintelligence task.

Adapting to this change will require greater coordination between the military, intelligence community, and law enforcement to ensure that adversaries cannot exploit the seams that often exist between them. It will also require creative solutions that reduce the threat surface. The decision in recent years to give the Committee on Foreign Investment in the United States greater ability to veto foreign land purchases near sensitive military sites is looking especially prescient as one such step.

Second, the United States should prioritize making its most exposed assets more resilient. Ships docked at naval bases or warplanes parked on runways, for example, are far more vulnerable than hardened missile silos. This was less problematic in an era where the U.S. homeland was effectively out of reach from conventional kinetic attacks. But that era is coming to a close. Because small drones can necessarily only carry relatively small explosive payloads, even minimal hardening or guidance problems may defeat such attacks.

The adoption of a layered defense is also necessary. U.S. Northern Command, which plays a key synchronizing role in counter-drone defense at home, has expressed interest in mobile flyaway kits, a "rapidly deployable, prepackaged counter-drone technology, along with personnel trained to employ that technology, that can be dispatched via commercial aircraft to get to the installation in need." According to reports, these kits will ideally not only include detection capabilities but also the capacity to bring drones down. The Services should certainly take this interest seriously. The good news is that research suggests the public supports counter-drone operations. But flyaway kits will be more effective with good counterintelligence work to identify threats with enough lead time. Whatever the ultimate answer, reducing the vulnerability of high value assets to direct kinetic strikes from cheap, short-range drones is essential for maintaining a robust deterrent and generating forces in the event of conflict.

Third, there is a pressing need for more research, analysis, and wargaming of this issue. Recent wargames run by the Joint Counter-small Unmanned Aircraft Systems Office and RAND are an important start. Their most recent game, held in March 2025, helped U.S. Northern Command refine its approach and identified the need for coordination from a wide range of entities. Working through relevant legal issues and establishing processes for interagency decisions, which will need to be made quickly, is critical.

Additional investigations to better understand which bases and potential targets are most susceptible to these kinds of spectacular attacks in the first place would be welcome. In their article, for example, Hunzeker and Yu argue that Taiwan is especially vulnerable given its challenges with espionage and smuggling. While the United States may not face these same problems as acutely, it is still a big country with lots of commercial activity and points of entry. Moreover, the United States has bases in foreign countries with their own unique vulnerabilities and weak points. Mapping the landscape and allocating resources appropriately is important given the near-impossible task of defending everywhere at all times.

Fourth, the Pentagon should learn from these cases — not just defensively, but offensively. If conflict breaks out in the Taiwan Strait or South China Sea, the ability to launch precision, deep penetration attacks using small, expendable systems would be impactful. Just as it is critical to map the previously discussed vulnerabilities, it is equally critical to understand where adversaries are most vulnerable to these sorts of attacks and develop strategies to exploit them should conflict break out. As Bego notes, Ukraine's operation against Russia "threaten[ed] to undermine a long-standing strategy of relying on its vast size and strategic depth to shield key military and industrial assets from within striking distance of any front-line on its western border." China, as a large country, may similarly be concerned about the implications of such attacks for its own security. The United States and its allies should take note and prepare accordingly.

Michael Poznansky is an associate professor in the Strategic and Operational Research Department and a core member of the Cyber and Innovation Policy Institute at the U.S. Naval War College. He is the author of Great Power, Great Responsibility: How the Liberal International Order Shapes US Foreign Policy *(Oxford University Press, 2025) and* In the Shadow of International Law: Secrecy and Regime Change in the Postwar World *(Oxford University Press, 2020).*

Erik Sand is an assistant professor in the Strategic and Operational Research Department and a core member of the Cyber and Innovation Policy Institute at the U.S. Naval War College. He is also a research affiliate with the Security Studies Program at MIT.

The views expressed here are the authors' own and do not represent those of the U.S. Naval War College, the Department of the Navy, or the Department of Defense.

Image: Midjourney

Cogs of War

Strategic Outpost

War On The Rocks

What's Going On In Venezuela?

Members

Membership

Get More War On The Rocks

Support Our Mission And Get Exclusive Content

BECOME A MEMBER

Subscribe to our newsletter

Enter your email address

SUBSCRIBE

By signing up you agree to our data policy

Privacy Policy

Terms & Conditions

Sitemap