Ukraine's Drone Attack: What It Means

By

Michael Fincher

The recent Ukrainian "Spiderweb" drone attack on Russian airfields that destroyed a number of strategic bombers proved the utility of asymmetric drone warfare. Taking the Russian "Club-K" container concept, with inspiration easily found in modern fiction, the Ukrainians modified shipping containers to house and launch armed drones used in the attack.

The containers were then placed far inside Russia before launching the drones. One hundred seventeen drones were able to strike targets up to 2,500 miles away from Ukrainian territory. The hurdle of communicating with the drones and powering them was accomplished with local SIM cards and solar panels.

While the results are disputed, many Russian aircraft were damaged at a significant cost, especially since production lines for many of Russia's bombers shut down decades ago. There is also the cost of embarrassment and the concern that Russia cannot protect its forces from drone threats. Understandably, there may be a concern that a similar follow-on attack is likely.

Those fears were proven correct, but in another country—Iran. Israel was able to strike numerous military and nuclear installations, as well as target specific individuals in air strikes throughout Iran, with minimal resistance and no known losses.

Despite Israel being only hours into a purported weeklong operation, they revealed they had a network within Iran that used drones to incapacitate anti-air defenses.

Incorporating covert use of drones into suppression of enemy air defense (SEAD) doctrine is a critical development in air warfare. While unmanned aerial vehicles (UAV) used in SEAD was theorized, this is the first time it was employed for that purpose. Unlike Ukraine, Israel used personnel within Iran to operate the drones. While increasing risk to their operatives, it most likely allowed more precise control of pre-placement and planning and minimized communications that could be intercepted or disrupted.

In the future, it is likely that covert pre-placement and distant operation will be used to "shape the environment" for more conventional strikes and attacks. The hurdles to overcome are power supply, detection, and communication. There is also the need to overcome any particular anti-drone technology that may exist.

Regardless, use of drones as a preliminary and surprise strike weapon works. It is a threat that will work particularly well against soft targets as well as military targets. While the US needs to develop its own capabilities, and fast, it absolutely needs to prioritize defeating drones and defending infrastructure from them. Whether they are pre-programmed or operated by fiber optics, radio, or lasers, the US must develop affordable ways to stop them.

The days of relying on a handful of military police to guard installations at home should have ended on September 11, 2001. In some cases, it did, but in others it did not. In the civil sector, not much has changed despite the increasing threat environment.

There are additional challenges that make attacks like Ukraine's asymmetric attack more likely. The United States has seen tens of millions of illegal aliens enter the country, many from nations hostile to the United States. Many that do come legally come from every background imaginable and hold various ideologies, faiths, and allegiances that are not friendly to the United

States. China's extensive use of Chinese students and work visa holders to commit industrial espionage is another example of what can be turned into a fifth column.

Additionally, with only 6 percent of cargo entering American ports facing inspection, ports are also an easy target for exploitation. And as if this were not enough, Americans also allow hostile nations to purchase land next to military installations.

It is only a matter of time until such an attack happens on American soil. A terror attack, perhaps in retaliation for the recent air strikes in Iran or by Mexican drug cartels is possible. More likely and troublesome is the use of drones in conjunction with other strikes on infrastructure and installations, all to cripple the military in advance of conflict in the Pacific. The US Air Force and Navy are particularly at risk, as air frames and ships are expensive and take time to replace. The Navy, for example, struggles to build ships and submarines.

Today, the nation's only defense against this threat is relying on signals intelligence to intercept communications, praying for defectors, and dumb luck. This is certainly no way to plan for asymmetric threats that are predictable. The time to find solutions is now, not after the attack.

Michael Fincher is a Fellow at the National Institute for Deterrence Studies.