What Ukraine’s Drone War Means for US Military Vulnerabilities

As I’m sure you heard, Ukraine leveraged drones to spectacular effect in Operation Spider’s Web, destroying an estimated 34% of Russian airpower deep in Russia. Operation Spider’s Web used 117 Ukrainian first-person-view drones to destroy over 40 Russian war planes, across five different times zones. (Wikipedia, Operation Spider’s Web, 2025)

Drones were remotely launched from hidden compartments built into trucks that were prepositioned within range of Russian airbases. The complex asymmetric attack used Russia’s highway and internet infrastructure against it to damage planes 2,700 miles (4,300km) away from Ukraine. The name was apt, as the spider-like drones are reported to have unfurled thin fiber optic cables, not unlike a spider spinning a web. It is also apt in another regard, as the complexity and scope of the mission was indeed impressive, taking so many Russian planes off the board at so many different air bases, again, like a spider’s web.

Video of the attack, from both the Ukrainian drones and also from Russian sources, is spectacular. Russians are calling the attack Russia’s Pearl Harbor. It resulted in the greatest loss of aircraft in a single day since WWII when Germany attacked Russia and destroyed between 1,200 and 2,000 aircraft on the ground, earning a 40-second slot in state-controlled Russian news television, which has kept negative reporting on the war with Ukraine buttoned up tight. (Cole, 2025)

Ukraine claimed that truck drivers exfiltrated prior to the strike, which was triggered remotely. It could have been even worse than it was. At least one of the trucks was reported to have exploded before the attack.

Military planners had theorized variations of this type of attack, and Operation Spider's Web was certainly not the first time that drones were used in combat, or the first time that hidden compartments were used to conceal weapons, or the first time a countries infrastructure was used against it (certainly our air travel infrastructure was used against us on 9-11) but I think it was the first drone attack to provide proof of concept of how vulnerable modern militaries are to this type of drone attack, at this time.

Nassim Taleb, author of The Black Swan: The Impact of the Highly Improbable (Taleb, The Black Swan: The Impact of the Highly Improbable, 2007) and Antifragile: Things That Gain from Disorder, (Taleb, Antifragile: Things That Gain From Disorder, 2014) has pointed out that after a Black Swan occurs (a Black Swan is an event that we fail to predict that harms us), hindsight being what it is, people tend to convince themselves that they were always aware that it would occur all along. I'm not sure which cognitive bias this is, or if it has been named yet, but he's absolutely right and we should be careful not to do that with Operation Spider's Web.

What Can the USA Learn from Operation Spider's Web?

I would argue that we can learn quite a bit from it because we have some of the same vulnerabilities. Here are the principal points:

1. **Get Ready for Asymmetric Warfare**

If you Google the definition of asymmetric warfare, the answer will be that it is when there is a material difference in power and strategy between two enemies. In this case, Russia is much more powerful than Ukraine, forcing Ukraine to adopt guerrilla warfare strategies and “think outside the box” to defeat their more powerful enemy. (Wikipedia, Asymmetric warfare, 2025)

As the USA is arguably the world’s only remaining superpower, although China appears to be trying to change that, any war we fight is likely to involve asymmetric warfare on the part of our enemies. If China attacks Taiwan, the US would be the underdog (due to China’s extreme proximity to Taiwan and our great distance) and it would be the USA using asymmetric warfare strategies against China.

But, according to Stephen J. Blank, an expert on the Soviet bloc of the Strategic Studies Institute and author of Rethinking Asymmetric Threats, asymmetric warfare is a buzz word which is in vogue in Washington lately, and as a consequence, the meaning is easily lost. He says it is simply a new word for a very ancient strategy, one that goes all the way back to Sun Tzu, author of The Art of War, which is, “All warfare is based on deception.” (Blank, 2003)

The next war we fight probably may have surprisingly little in common with past wars. Small arms and artillery may play a reduced role or may play practically none at all.

2. Prepare for Our Enemies to Use the Same Strategy Against Us

Worryingly, China has been buying up land directly adjacent to US Air Force bases and this may be precisely why. Although China could launch a similar attack on a much larger scale. Imagine that instead of 117 Ukrainian quadcopters, the USA is attacked with it was dozens of swarms, each comprised of thousands of Chinese drones, and each swarm has its own objective. They could destroy much more than a few dozen airplanes. They could send us back to a pre-industrial revolution footing.

We’ve seen how the US government reacts to Chinese balloons flying over our country, including sensitive military installations. They bumble around and have meetings about legalities and potential consequences until it crosses the entire continental US and only shoot it down after it reaches the ocean on the other side, after it has accomplished its mission. Well, that’s how the Biden administration handled it, anyway. My hope is that President Trump would act decisively.

And we’ve seen how the USA reacts to mass sightings of unidentified drones. We do the same things we did about the balloons … nothing, until it is too late. Nobody’s authorized to do anything about them. If the government doesn’t get that sorted out, in a hurry, they will utterly fail at protecting Americans against the next spectacularly effective drone attack.

3. Prepare for Our Enemies to Use Other Asymmetric Warfare Strategies Against Us

But the next asymmetric warfare attack against the USA might not use drones.

It may be in the form of a ship borne HEMP weapon that knocks out the electrical grid in nearly the lower 48 states as well as parts of Canada and Mexico. Or it may be a cyberattack, nuclear weapons detonated inside US cities, a kinetic attack on the grid, a biological attack, an information war, or it could use unmanned systems, or it could use drones in a radically different way.

Or maybe it will be a hybrid of cyberwarfare, psyops and information war that turns half of our nation against the other half, goading us into a civil war so we do their job for them, and they step into the winners' circle unchallenged.

Any attack that knocks out our electrical grid, turns off the internet, and if they do that, the USA is the most automated country on the planet. We will grind to a halt. We can no longer farm without the internet, GPS, lasers and all kinds of contraptions. We can't buy anything or sell anything or pump gas or refine oil or ship products or provide healthcare or sell medicine or even treat drinking water without the power grid and the internet anymore. Cities will no longer receive shipments of everything you need to live.

What You Can Do About It

There are two separate ideas here. One is what the government needs to do to prepare for asymmetric warfare, and the other is what YOU need to do to prepare for asymmetric warfare. You can't control whether or not the government shoots down balloons or drones or just lets them spy on us or blow stuff up. But you can do something about being without medicine, drinking water, food, gas, electricity, and so on.

You can prepare all the same stuff that will make you prepared for all most threats! Sure, depending on the specific threat, there are some things you might want to do. In a nuclear war, you would want a radio, radiation meter, dosimeters, potassium iodide, a fallout shelter and so on. But regardless of the threat, you must meet your core survival needs: security, medical, shelter, water, food and so on.

If you provide for your core survival needs, you will increase your odds of survival regardless of the threat. Once you do that, then you can start preparing for the threats that you know about. Then, chances are, you'll be prepared, come what may.

References

Blank, S. J. (2003, September). *Rethinking Asymmetric Threats.* Retrieved from defense.gov: https://media.defense.gov/2023/May/04/2003215284/-1/-1/0/1418.PDF

Cole, B. (2025, June 2). *Russian Aviation’s Darkest Hour Since WWII Gets 40-Second TV News Slot*. Retrieved from newsweek.com: https://www.newsweek.com/russia-drone-ukraine-ww2-2079812

Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable.* New York: Random House.

Taleb, N. N. (2014). *Antifragile: Things That Gain From Disorder.* New York: Random House.

Wikipedia. (2025, May 22). *Asymmetric warfare*. Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/Asymmetric_warfare

Wikipedia. (2025, June 2). *Operation Spider’s Web*. Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/Operation_Spider%27s_Web