DEFENCE

Battlefield vibe coding and the open source future of drone warfare

After Ukraine used Ardupilot-powered drones to blow up Russian nuclear bombers, what's next for open source combat?

Jasper Hamill
11 Jun 2025 — 6 min read

A Tu-95 bomber is bombed at Russia's Olenya airbase (Image: The Security Service of Ukraine)

In the 20th century, modern warfare had a steep barrier to entry. Yes, one hydrogen bomb could wipe out an entire city in seconds. But there was close to zero likelihood of a terrorist spinning one up in their mother's basement.

Today, it's frighteningly easy for independent actors to produce weapons that were once only available to states.

For instance, the spread of easily manufactured weapons is already threatening to make a mockery of gun control rules. A 3-D printed "ghost gun" was alleged to have been used in the assassination of UnitedHealthcare CEO Brian Thompson, suggesting it could soon become impossible to fully track, monitor and limit the spread of small arms.

On the battlefield, cheap, accessible technology is also proving to be a powerful force multiplier for outgunned and outnumbered warfighters. Last week, it emerged that Ukrainian special forces used drones powered by open source software called Ardupilot to destroy a large number of nuclear bombers.

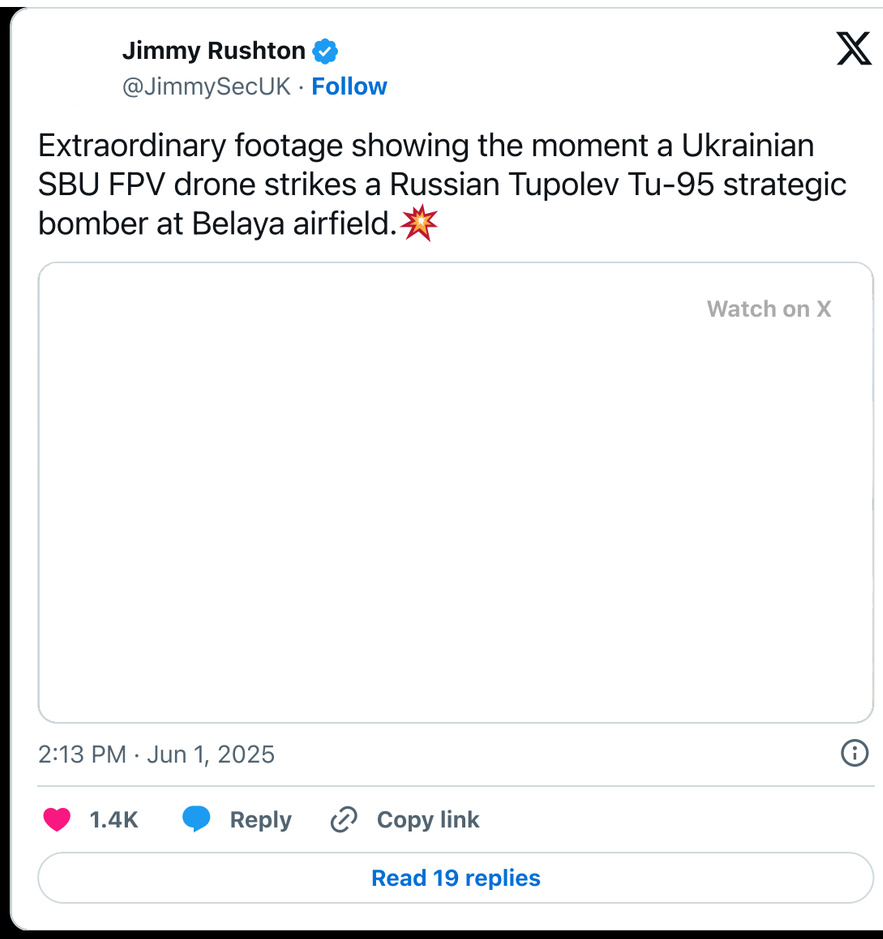
In an operation named Spider's Web that was planned in total secrecy for 18 months, drones targeted airfields in five regions of Russia, including targets as far east as Irkutsk, almost 2,500 miles from Ukraine.

It's not clear how many bombers were destroyed, with President Zelensky reportedly suggesting that up to 40 were blown up and the US claiming about 20 were hit and 10 wrecked.

But the fact that Ukrainians were able to strike so deep into Russian territory was a powerful message to the Kremlin as well as the world. It showed that fighters waging asymmetric guerrilla warfare can now use basic equipment to do serious damage at a relatively low cost.

On X, co-creator Jason Short wrote: "Wow. Ardupilot-powered drones just took out half the Russian strategic bomber fleet."

"Not in a million years would I have predicted this outcome. I just wanted to make flying robots," he added.



War, what is it good for?

The answer to that question is, of course, innovation. We're not a fan of conflict here at Machine, but cannot help but note that radar, jet engines, antibiotics, GPS, nuclear energy, duct tape and even computers were all invented or rapidly advanced during wartime, going on to reshape civilian life around the world.

But should we be concerned about the proliferation of weapons of mass or minor destruction? And will open source software developers become a military target in the future?

We spoke to Amanda Brock, CEO of OpenUK, to get a sense of what's next as open source potentially becomes a weapon of war.

Will Ardupilot and other open source software become standard tools on the battlefield?

"The situation between Russia and Ukraine is not a normal one. It's a war. Operation Spider's Web is part of that war. The planes blown up would have been used by Russia to attack and kill Ukrainians. We recently saw a Russian missile in Ukraine badly injure a 29 year old open source contributor and kill his wife. This is the day to day existence and fear under which people in Ukraine live.

"ArduPilot is now 18 years old and will continue to be used across the planet to 'control almost any vehicle system'. Of course there is a possibility that the ArduPilot project - which is made up of key contributions from individuals across the globe, including France, Brazil, Japan, Australia and the UK - may come under a little pressure as a consequence of its high profile use. Cyber attacks on ArduPilot could happen. But cybersecurity is not an issue to open source. All software is vulnerable to these and never more so than in this time of geo-political shift.

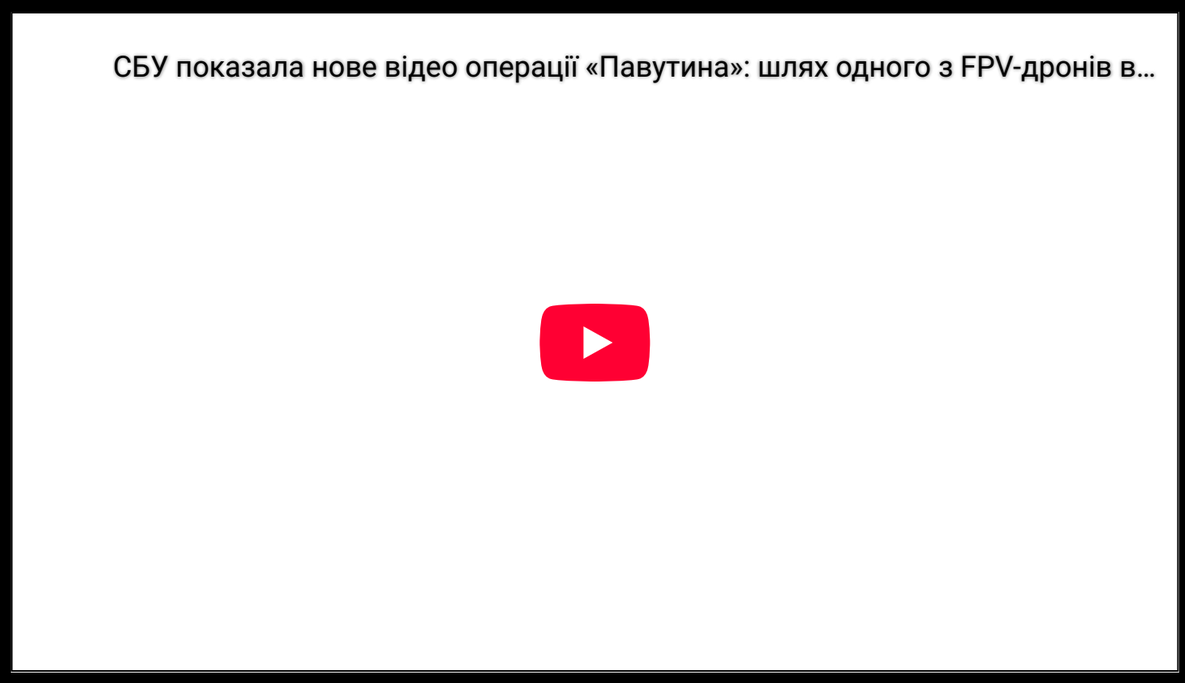
We've seen allegations that China has hidden communications tech in solar devices. Is open source more or less vulnerable than closed military operating systems?

"Whilst open source is sometimes perceived - wrongly - as more vulnerable, due to the openly accessible code base, well run open source projects respond to these attacks in a joined up way with the benefit of industry support. This proves the adage that 'many eyes make bugs shallow'.

"The transparency of open source gives it an opportunity to engender trust that is critical to our digital future.

"ArduPilot could be used by Ukraine again, and could equally be used by Russia. Anyone can use open source software for any purpose, unless restricted by law. The open source community and its licensing make no judgement on who uses the software or what for... we leave that to the law makers and regulators. Laws trump licensing.

"The free flow enabled by anyone being able to use the code for any purpose is one of the key reasons for the success of open source software in the last decade. Once possibly perceived as created by hippies in their basement it is today the standard way code is developed in even our largest companies. Today the majority of the software in commercial software stacks is open source."



Should the people working on Ardupilot be worried about becoming Russian targets?

"Open source projects like ArduPilot are one kind of open source, created by individuals in a community of volunteers. Chris Anderson, one of the three co-founders of the project and former editor of Wired magazine, actually describes it as having come into existence in his basement 18 years ago.

"I would hope that rather than a threat, the public focus on the project may create more interest in its functionality and perhaps see more people want to participate in it and use its outputs. Certainly we see very positive use cases of drones, like transporting blood between hospitals in London."

Will governments seek to stop people from using open source software if its dual-use capabilities tip further towards military applications?

"The rules in this situation are the rules of a war and those are very different. Trying to stop the use of open source because of the drone attacks is like saying there's been a knife attack, so we are going to ban knives. It's about a particular use case of something that is otherwise beneficial.

"Today, open source software provides the infrastructure underlying our digital economy. It's like the base of a pizza in many ways: everyone is focused on the toppings, but remove the base and you are left with a sloppy mess.

"Any attempt to stop the usage of open source would be extremely unwise and have a significant detrimental impact on the average person. The world would become a difficult place to live in - our transport systems, retailers and utility providers are all dependent on open source for their digital infrastructure.

"Perhaps the question we ought to ask ourselves is a different one. What value does open source bring society? Recent research has shown that open source software generates trillions of dollars in value and it certainly saves us huge amounts of money.

"In the UK we've demonstrated 27% of our digital economy is generated by open source - and I suspect it is a lot more in reality. But, it's not just about generating value. 92% of all commercial software today depends on open source software to function. Maybe it's time to recognise the huge contributions that those contributing to open source bring to society."

Could this mean more restrictions on open source?

"I've heard people come out with truly nonsensical suggestions in the UK, like requiring certification of individuals' right to code. This kind of suggestion completely mis-understands how software works. The same people want to be paid to certify those individuals, which is not exactly a surprise.

"AI enables something called vibe coding where natural language prompts rather than coding instructions are being used to create code. We are only going to see more people generating code.

"Any restrictions that might be appropriate are not restricting the creation of code or innovation, but rather considering the use cases of the code. In most cases we already have applicable laws for those use cases."

Do you have a story or insights to share? Get in touch and let us know.

Follow Machine on X, BlueSky and LinkedIn

READ MORE

Adapting to Digital Darwinism: Will AI create a permanent new class divide?

"LLMs, GenAI, predictive analytics and intelligent automation are pushing...

Microsoft blames China for SharePoint ToolShell attacks, governments and nuclear weapons agency targeted

Fear turned to panic as scary 9.8 CVSS vulnerability came under active exploitati...

Crazy game: Remembering Ozzy Osbourne's mysterious lost video games

We dig into the forgotten and semi-mythical titles starring the legendary Prin...

UK public bodies to be banned from making payments to ransomware gangs

"These new measures help undermine the criminal ecosystem that is causing harm...

Subscribe to Machine

Tech | Science | Ideas

jamie@example.com Subscribe