Ukraine’s Digital Battle With Russia Isn’t Going as Expected

Even the head of the country's online offensive is surprised by the successes—although they’re not without controversy.

Justin Ling

April 29, 2022

When Russian president Vladimir Putin launched his full invasion of Ukraine in February, the world expected Moscow’s cyber and information operations to pummel the country alongside air strikes and shelling. Two months on, however, Kyiv has not only managed to keep the country online amidst a deluge of hacking attempts, but it has brought the fight back to Russia.

Even Ukrainian officials are surprised by how ineffective Russia’s digital war has been.

“I think that the root cause of this is the difference between our systems,” says Mykhailo Fedorov, Ukraine’s 31-year-old minister for digital transformation. “Because the Russian system is centralized. It's monopolized. And it leads to the scale of corruption and graft that is becoming increasingly apparent as the war continues.”

Speaking to WIRED from near Kyiv, Fedorov says his country has been preparing for this moment since Russia first invaded in 2014. “We have had eight years,” he says.

In recent weeks, Fedorov and the Ukrainian government have deployed the controversial face recognition program ClearviewAI to identify killed and captured Russian soldiers. They have deployed thousands of Elon Musk’s Starlink terminals to keep the country connected, even amid Russian bombardment. They have crowdsourced intelligence collection, letting ordinary Ukrainians report troop movements. And, perhaps most critically, they have beaten back aggressive attempts to knock offline their internet, energy, and financial systems.

Fedorov, who also serves as deputy prime minister, ran Ukrainian president Volodmyr Zelensky’s wildly successful election campaign in 2019, winning by nearly 50 points in the second round against incumbent Petro Poroshenko. He did so, in part, by leveraging authentic selfie videos to market the former comedian as an unconventional politician who eschews the normal trappings of politics. It’s exactly that style of video that Zelensky has uploaded regularly from the streets of Kyiv in recent weeks, offering a stark contrast with Putin’s stiff proclamations inside his palatial offices.

Ukraine has brought the war home to Russia in more cutting ways. In March, Reuters reported that Ukraine had purchased face recognition software from American company Clearview AI to identify the bodies of Russian soldiers killed in action—Kyiv later acknowledged that they were using this information to contact the families of the dead soldiers.

“We are pursuing two goals here,” Fedorov says. “First is: We are notifying their relatives, and telling them, basically, that it's not a very good idea to go to war with Ukraine. So that serves as a cautionary tale. And secondly, it's a humanitarian purpose—just telling them where their relatives, or friends, or children are so that they don't try to get this information from the Russian authorities. Because, more often than not, they can't.”

That decision hasn’t come without criticism. Contacting the families of soldiers killed in battle could be seen as harassment. Others have pointed out that being deployed in Ukraine is a PR coup for ClearviewAI, which has been embroiled in scandal over its liberal use by police forces across North America.

Fedorov, for his part, says Russia “can spin this whatever way they want. But the fact of the matter is, there are tens of thousands of Russians dying in Ukraine, and we are just providing this information to their families because that serves, among other things, a humanitarian purpose.”

There is a propaganda element to Kyiv’s use of face recognition technology as well.

“This facial recognition plays to our, let's say, to our advantage in the information space,” Fedorov says. Moscow has projected the image of a professional and volunteer fighting force. “We're trying to say that, for example, Russia is sending conscripts … we are proving that and justifying that with a lot of factual information. We can give you a list of hundreds of people who are 18 and 19 years old, with their names and with their birth dates and how and where specifically, they were conscripted. So that gives some substance to our claims.”

Fedorov says the utility goes beyond just identifying the dead.

“One interesting case study of how we used Clearview AI,” Fedorov says. “There was a man who was found in a Ukrainian hospital, claiming that he was a Ukrainian soldier who suffered from shell shock or some kind of trauma and that he forgot everything. And he was claiming that he was Ukrainian. So the doctor sent the picture to us, and we were able to ID him in a matter of minutes. We found his social network profile, and we established that he was Russian and, of course, he was brought to responsibility.”

Ukrainian officials have said that the frequency of Russian cyberattacks tripled immediately prior to the war, and they have aggressively targeted critical infrastructure since the war began.

But Viktor Zhora, deputy head of Ukraine's State Service of Special Communications and Information Protection, says Moscow may have maxed out its ability to launch attacks. “Russian cyber operations likely reached their full potential," he says.

Zhora told WIRED that years of training, exercises, and cooperation with NATO have made Ukraine far more resilient to cyberattacks. Some attacks are easier to defend against than others—as we spoke, Zhora said he was monitoring an active attack on the state administration of Lviv, which had been publicly announced by Russia hours earlier.

But Zhora stresses that while it is wrong to overestimate how powerful Russia's cyber capabilities are, it would also be wrong to underestimate its more "sophisticated" operations. "We should continue to observe their potential, like Sandworm, like a Fancy Bear, like Gamaredon, many other groups that are still active, and still very dangerous," he says, referring to a number of Russian government hacker groups.

Brandon Valeriano, a senior fellow at the Cato Institute who specializes in cyber operations, says offensive cyber operations don't mesh well with traditional, kinetic warfare. At best, he says, "they're enabling, they're complimentary … they don't transform it."

Valeriano points to a slowdown in the tempo of Russian-backed cyberattacks targeting the United States as evidence that Moscow's capacity isn't as expansive as some have assessed. "They're not organized for offensive cyber operations in the way that we think they are," he says.

Kyiv's ability to beat back against those operations, Valeriano says, can be attributed to "intense collaboration between Ukraine, Western powers, and NATO." Indeed, Five Eyes signals intelligence agencies have both been providing training and support for Ukraine's cyber defense and have been sharing threat intelligence. (Zhora stresses that information-sharing is a "two-way road.")

Ukraine has been able to defend itself, both in cyberspace and in an outright propaganda war, because it has managed to stay online. For that, Fedorov credits a decentralized network of internet service providers and Elon Musk.

"It wouldn't be possible to restore 10 km of cable connection between villages in Chernigiv region after serious battles so quick," he tweeted earlier this month. "Normally it takes few months." But with one Starlink satellite, he says, five villages were reconnected in a matter of days.

"We have received over 10,000 Starlink terminals to date, and we use those where we have blind spots with, let's say, more traditional coverage," Fedorov says. "So we are trying very hard to restore and protect our landline and mobile connections."

Like any physical infrastructure, those Starlink terminals—which have even managed to keep the embattled city of Mariupol online—have been vulnerable to Russian shelling. Zhora says Russia has managed to hit some of those terminals but has not managed to target the system as a whole. "I suppose that it was coincidence that some shells hit these terminals and locations," Zhora says. "It's not easy to identify and to attack them systematically."

Keeping Ukrainians online is a clear strategic objective for Ukraine. Photo and video evidence of the brutality being doled out by the Russian army has galvanized Western support for Kyiv and led to an unprecedented level of support from NATO to help the country defend itself.

It's also letting regular Ukrainians contribute to the collective defense.

During Zelensky's presidential campaign, Fedorov made particular use of the messaging app Telegram, which is also popular with Russian intelligence operatives. In recent weeks, the app has been leveraged to collect evidence of possible war crimes in towns like Bucha, but also to enable Ukrainians to upload details of Russian troop movements. A Telegram bot collects photos and videos of Russian military movements, verifying Ukrainians through their digital ID,: a project spearheaded by Fedorov.

“Regular internet users—so, basically, civilians—they can go and post photos of what's happening in Ukraine,” Fedorov says.

The Ukrainian security ministry said in a tweet in March that those crowdsourced reports have directly contributed to drone strikes against Russian tanks.

“There are actually very many ways that regular citizens can contribute to the effort,” Fedorov says. One particularly “successful vector,” he says, is basically trolling. His government has been sending users “into the comment sections of posts by some very high traffic Russian influencers and just trying to talk sense into people and telling them that there's actually a war in Ukraine.”

Fedorov is also responsible for Ukraine’s IT Army, a network of cyber activists and hackers who have targeted Russian systems. In recent weeks, they have dumped huge troves of personal information from large Russian corporations.

Russia’s poor information security has also been a significant factor in their fumbled invasion.

A huge number of technology providers, from cybersecurity firms to cloud hosting services, have pulled out of Russia since the start of the war—either due to sanctions or to a concerted push from Fedorov and others in the Ukrainian government. “If the world were able to stop the delivery of these products to Russia, we see that they will have no infrastructure even to organize attacks,” Zhora says.

Russia’s attempts to knock out mobile and internet connections in Ukraine have mired their own communications. Their encrypted radio platform, Era, has been unreliable, leading Russian soldiers to opt for unencrypted platforms. Numerous outlets have reported details of conversations between Russians troops, their commanders, and their families—some even admitting to possible war crimes over unencrypted channels.

While Fedorov’s reform mission has played a large role in modernizing Ukraine, support from the West has certainly helped. SpaceX and the United States have sent some 5,000 Starlink terminals. Fedorov says the European Union has provided some 10 million euros toward computer systems and workstations.

Asked what Ukraine needs as the war wears into its third month, Fedorov mentions satellite equipment, including more Starlink terminals, as well as laptops, tablets, and other tools “to put our civilian infrastructure back online.” He also jokes: “Let's say that the most surefire way to keep us online for a very long time to come is to provide us with artillery, tanks, and warplanes—because that will effectively end the war. And that will remove the problem altogether.”