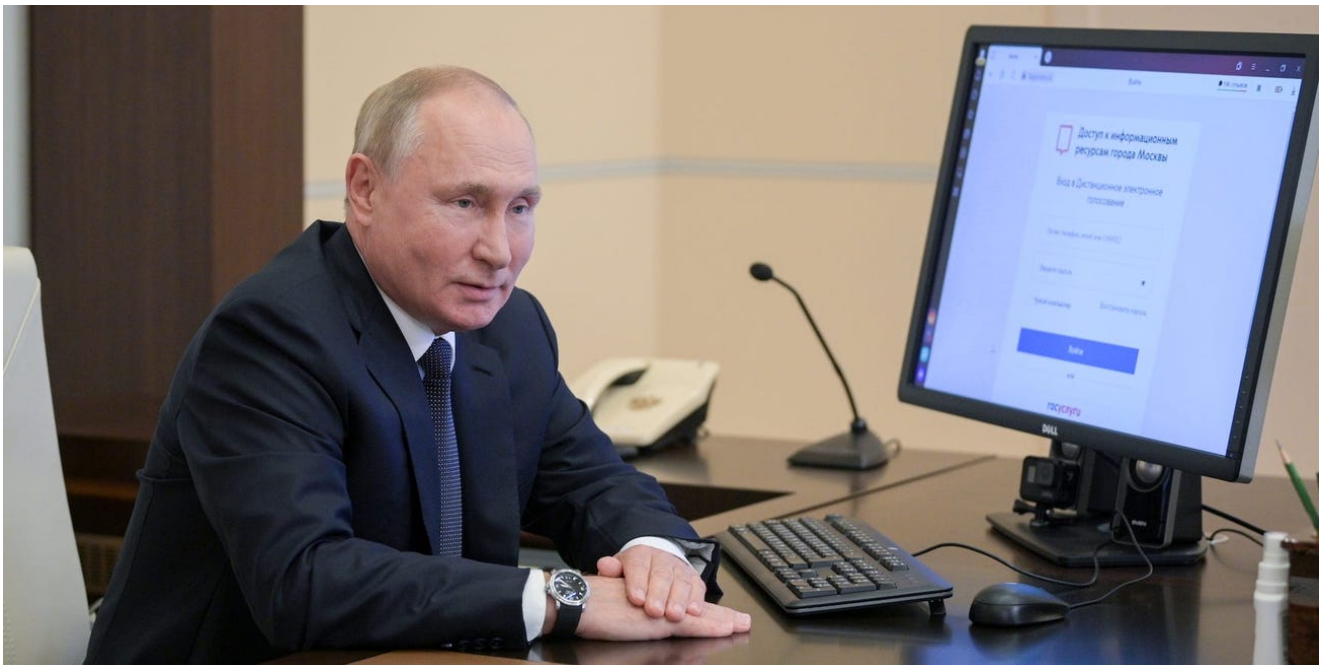
Russia is quietly wielding its cyber weapons as its military struggles in Ukraine

businessinsider.com/russia-quietly-wields-cyber-weapons-as-military-struggles-in-ukraine-2022-5

Stavros Atlamazoglou May 8, 2022, 6:37 PM



Russian President Vladimir Putin takes part in remote electronic voting during parliamentary elections, September 17, 2021.
Sputnik/Alexei Druzhinin/Kremlin via REUTERS

The Russian military is struggling in Ukraine. Two months into the war, it has failed to achieve the quick victory envisioned by President Vladimir Putin and the few advisers informed of the plan.

But Russia's offensive might is composed of a lot more than just troops and weapons. Moscow's cyberwarfare capabilities also make it a force to be reckoned with.

While the Kremlin's conventional forces have underperformed in Ukraine now, it has employed those cyber weapons to great effect in the past.

Ukraine's and Russia's cyber activity

Burnt armored personnel carriers and other destroyed military vehicles in a field in Bucha, Ukraine, April 18, 2022.
Alexey Furman/Getty Images

Russia has lost thousands of troops and dozens of ground vehicles, aircraft, ships, and other pieces of hardware, and much of that destruction has been rebroadcast to the world through social media.

Despite the scale of the destruction, Russia's cyber component hasn't been as robust or as visible as some expected — but it's not absent, according to Michael E. van Landingham, a former Russia analyst at the CIA.

"I don't think Russian cyber activity is more muted than expected," van Landingham told Insider, pointing to "multiple" distributed denial-of-service attacks and "wiper" attacks, which remove data from devices, used by Russia against Ukrainian sectors.

"That said, many had perceptions of a cyber Armageddon bricking US and European computers or destroying Ukrainian critical infrastructure. That probably didn't happen because Putin wanted to fight a limited war in Ukraine," van Landingham added.

The scale of Russia's kinetic operations — troops on the ground backed by aerial and artillery attacks — "obviates the need for the most impactful cyber tools. You can, in a sense, keep your powder dry because you're using so many real explosives," said van Landingham, who is founder of risk-analysis and research firm Active Measures.

Should Moscow choose to escalate in response to US and European security aid to Ukraine, it "has numerous asymmetric capabilities short of nuclear weapons" it can use, van Landingham said.

Earlier this year, the cybersecurity firms Dragos and Mandiant helped uncover a complex malware designed to damage liquefied natural gas plants and other industrial facilities. Those plants would be vital to Europe achieving energy independence from Russia, and "there could be more programs like those out there," van Landingham told Insider.

Russian intelligence agencies have a long history of conducting or sponsoring cyber intrusions.

In March, the Department of Justice charged four Russians with conducting cyber intrusions against US power plants over the past decade on behalf of the Russian Ministry of Defense and FSB.

Russian cyberattacks against Ukraine are also longstanding. For years, Russian intelligence services have targeted their neighbor's critical infrastructure, mapping out nodes and vulnerabilities.

A 2015 cyberattack that cut off power in Western Ukraine — the first such attack known to have brought down a power grid — was attributed to a hacking unit known as Sandworm, believed to be a part of Russia's military intelligence agency, the GRU. The same unit was blamed for the NotPetya malware used against Ukraine in 2017. NotPetya had a global impact, and the US estimated that it caused $10 billion in damage.

Current and former US officials worry that a Russian cyber offensive against US critical infrastructure could escalate or expand to conventional attacks. Russia could also attempt to interfere with or destroy satellites or underwater communications cables, which are not directly cyber-related but support military and civilian communications, van Landingham said.

During their meeting last year, US President Joe Biden told Putin that some critical infrastructure should be "off-limits" to cyberattacks and warned that the US has its own "significant cyber capability."

"There is always concern for what Russian cyber tools the US and Europe have missed, what sort of critical infrastructure effects that could have," van Landingham said.

The US should continue thinking about what the worst-case scenarios could look like and have an appropriate risk-management plan in place, "if not go through a few exercises to stress-test their systems," Herm Hasken, a partner and senior operations consultant at MarkPoint Technologies, told Insider.

"There's no better defense than a vigilant team with a full-spectrum cyber-defense program in place," said Hasken, who has extensive experience with US special-operations forces and in the intelligence community, including time as chief cryptologist for Special Operations Command.

A persistent cyber threat

In early March, the US intelligence community released its annual global threat assessment, which described Russia as a persistent cyber threat.

"We assess that Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. We assess that Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions, as well as a deterrence and military tool," the report said.

US intelligence agencies believe Russia is especially focused on mapping out and then targeting foreign critical infrastructure, including underwater communications cables and industrial control systems, allowing it to hold Western economies and societies at long-term risk.

The threat isn't limited to nation-states. According to the agencies, Russia is targeting and attacking organizations and individuals it sees as threats to its stability. Politicians, journalists, nonprofit groups, and others have also been victims of Russian cyberattacks, and they have seen their data and personal information leaked into the internet.

Stavros Atlamazoglou is a defense journalist specializing in special operations, a Hellenic Army veteran (national service with the 575th Marine Battalion and Army HQ), and a Johns Hopkins University graduate.