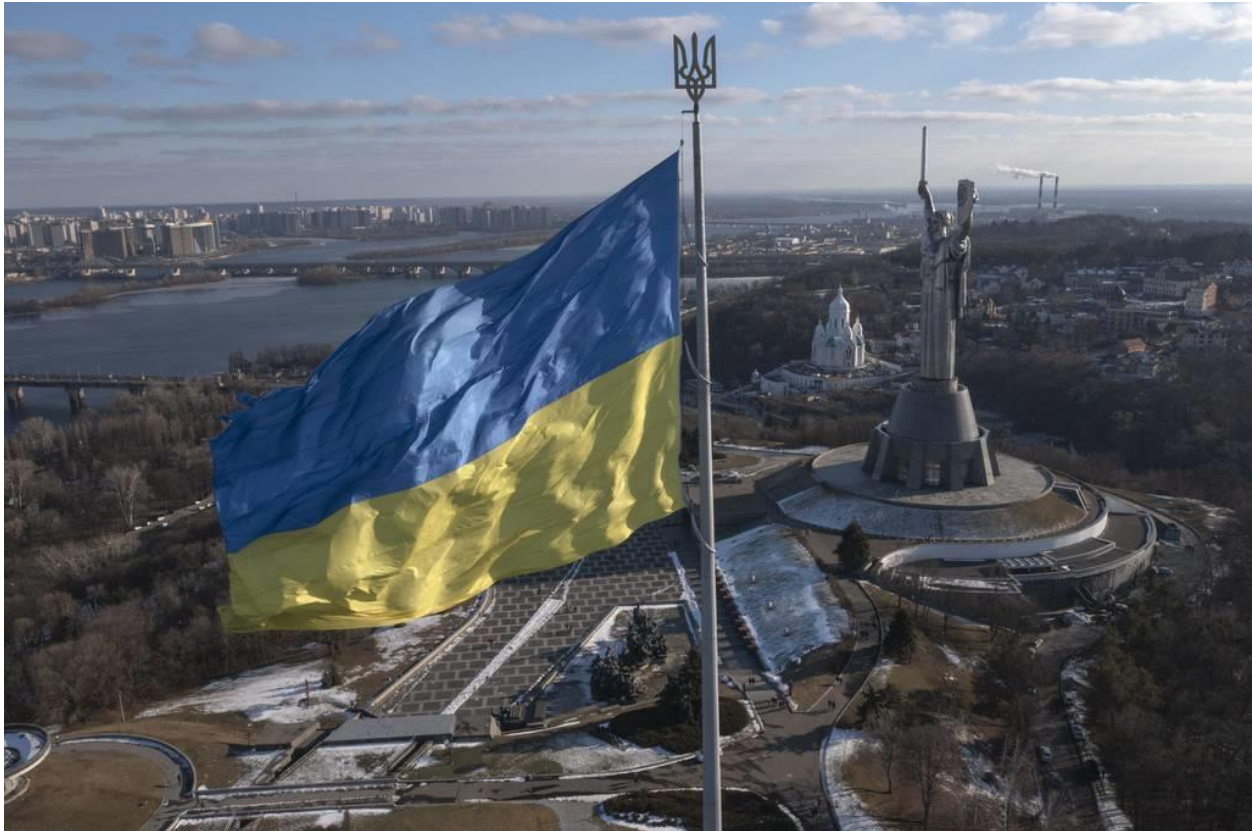


Cyber

Experts urge caution in assessing Ukraine cyberattacks

By [Mark Pomerleau](#)

Feb 16, 11:55 AM



DDoS incidents in Ukraine could signal a larger event is coming, but experts are still cautious. (Efrem Lukatsky/AP)

WASHINGTON — Cyber incidents in Ukraine this week raised fresh alarms amid concerns Russia may invade the nation imminently, however, experts said they're cautiously awaiting more details about the cyber activity.

[The distributed denial of service \(DDoS\) incidents](#) — which essentially flood internet sites with an unusually high amount of

web traffic, rendering them useless — hit at least 10 Ukrainian websites, including those of the Defense Ministry, Foreign Ministry, Culture Ministry and Ukraine's two largest state banks. Denial of service attacks don't require the incredible sophistication or painstaking access to networks needed for most data theft or deleterious cyberattacks, making them a common tactic among criminal organizations.

Ukrainian Information Ministry's Center for Strategic Communications and Information Security suggested Russia could be behind the Feb. 15 incident, but didn't provide details.

"It is possible that the aggressor resorted to tactics of petty mischief, because his aggressive plans aren't working overall," the statement said.

The Pentagon and U.S. Cyber Command deferred comment on the cyberattack to the National Security Council, which did not immediately respond to a request for comment.

Despite these incidents not yet being attributed to an actor, experts are worried they could signal an uptick in activity in eastern Europe amid the Russian troop buildup.

"Overall, this is telling us that more is starting to go down in Ukraine. I think this may very well signal the beginning of a Russian attack on Ukraine," Tatyana Bolton, policy director of the Cybersecurity & Emerging Threats team at the R Street Institute think tank, told C4ISRNET. Bolton is also the former director of the [Cyberspace Solarium Commission](#), a bipartisan organization created in the 2019 defense policy bill to develop a multipronged U.S. cyber strategy.

Bolton noted there's no direct indication Russian entities are responsible. However, the targets affected are what one might see during the beginning of a coordinated military campaign, she said.

Timothy Jones, vice president of systems engineering at Forescout, an enterprise defense company, cautioned that while the initial DDoS incident may not seem sophisticated, it could get worse and more complex.

With denial of service attacks, "sometimes the full extent isn't really seen right away. We're just starting to get some of the reports out," said Jones. "Maybe they're doing stuff in the background that we're not necessarily looking at yet, or hasn't really been felt."

Using denial of service indicates some level of restraint, which Bolton described as a bit atypical for Russia.

"Usually, [DDoS] doesn't take you offline for more than a day," she said. "It can be more serious, but it's not like encrypting all their files or deleting all their files. Those would have really been significant attacks. But the concern is also, what's next? Is this a smokescreen for a larger incident or attack?"

The critical infrastructure sector — such as energy companies — were not targeted, which could signal that if Russia was behind the incident, they either view the banking sector as more critical or they are following general rules of warfare by not knocking out power to the civilian sector in the dead of winter, Bolton added.

DDoS is a tactic the Russians have been accused of using previously.

In mid-January, Ukraine blamed Russia for a cyberattack that temporarily disabled about 70 Ukrainian government websites simultaneously. During last month's attack, an announcement posted stated that Ukrainians should "be afraid and expect the worst."

Russia launched one of the most devastating cyberattacks ever on Ukraine in 2017 with the NotPetya virus, causing over \$10 billion in damage worldwide. The virus, also disguised as ransomware, was a so-called "wiper" that scrubbed entire networks.

Cristin Monahan of the George Washington University's National Security Archive's Cyber Vault pointed out the Russians hit Estonia with a series of DDoS incidents in 2007 over Estonia's decision to relocate a Soviet war monument, something of a watershed moment in the modern cyberwarfare era.

"The Russians made the point that even without direct military intervention, or even cyber interventions with kinetic effects, they can exert significant pressure on nations in their crosshairs, and Ukraine has received the same message for a number of years," she said.

Monahan added that DDoS incidents rarely result in military intervention, implying the U.S. is not likely to physically engage with Russia over the loss of banking services.

The Associated Press contributed to this report.

About [Mark Pomerleau](#)

Mark Pomerleau is a reporter for C4ISRNET, covering information warfare and cyberspace.