The Washington Post

Putin's invasion of Ukraine didn't rely on cyberwarfare. Here's why.

Erica D. Lonergan, Shawn W. Lonergan, Brandon Valeriano, Benjamin Jensen

March 7, 2022

The ongoing conflict in Ukraine has perplexed observers expecting to see the cyber dimension unfold differently. When Russia began to mass troops along Ukraine's borders, analysts predicted that cyber operations would be critical to Putin's military strategy.

One headline offered that the Russian invasion could "redefine cyberwarfare." Former White House cyber expert Jason Healey hypothesized that "it will be the first time a state with real capabilities is willing to take risks and put it all on the line."

Despite these predictions, the expected "shock and awe" Russian cyber campaign in preparation of the invasion of Ukraine never emerged. Moreover, while the conflict will undoubtedly evolve, cyber operations don't appear to be playing a decisive role on the battlefield.

Surprised? We're not. Academic research explains why cyber operations are poor tools of coercion — whether used independently or as part of conventional warfighting.

What clues do earlier Russian cyber operations give?

Scholarly research details Russia's long history of cyber operations against Ukraine. Russia's 2014 annexation of Crimea included cyber operations in parallel to kinetic ones. Distributed denial of service attacks, for instance, strategically flooded Ukrainian networks to crash operations. In 2015, Russia carried out a cyberattack against Ukraine's power grid. And in 2017, Russia unleashed the data-wiping NotPetya virus, malware that targeted Ukrainian servers initially but quickly spread around the world.

Russia's land grabs in Ukraine could break the international order

Yet experts who inferred from Russia's past behavior that the current conflict would be a "Cyber Pearl Harbor" moment may have been drawing the wrong lesson. There is little evidence that cyber operations provided Russia with an operational advantage in 2014 — let alone highly synchronized combined arms warfare. And the power grid attack — in the dead of winter — did not cause any deaths, and service was restored within hours.

Russia's current cyber efforts have had little impact

Many of the recent cyberattacks aimed to fragment the trust Ukrainians have in their government — and these information operations clearly haven't been effective. In mid-January, Microsoft and other monitors reported that destructive malware, "WhisperGate," was targeting Ukrainian organizations.

In a different operation, Russian-linked hackers reportedly defaced 70 Ukrainian government websites. In mid-February, the U.S. and U.K. governments attributed disruptive attacks to Russia, with follow-on attacks Feb. 23. The same day, "HermeticWiper" malware was discovered operating in a number of Ukrainian commercial and government systems.

Hacktivists are engaging

Hacktivists, proxy groups and freelancers jumped in quickly — on both sides. Ukraine, lacking mature offensive cyber capabilities, appealed to the public to help marshal an "IT Army." The Ukrainian government used Twitter to share a list of Russian targets and, later, Belarusian targets.

But Russian ransomware operators also offered their services, threatening to retaliate against governments that sought to punish Russia. These appear to be loosely controlled proxy groups, not a unified effort. A Ukrainian member of the Russian-linked Conti ransomware group, for instance, reportedly leaked the group's internal chat logs to counter the pro-Russian effort.

Why isn't cyberwarfare decisive?

Cyber operations in combat contexts may not be as prolific or decisive as many expect, as demonstrated by evidence not only from Ukraine, but also from Afghanistan, Iraq and Syria. The U.S. military, for instance, discovered that dropping "cyber bombs" on the Islamic State netted ambiguous results.

The Ukraine crisis is now a nuclear crisis

Cyber operations are a form of modern political warfare, rather than decisive battles. These operations don't win wars, but instead support espionage, deception, subversion and propaganda efforts.

Here's why the current cyber operations are neither as easy nor as effective as the conventional wisdom would suggest. First, the global tech sector plays a major role in cyberdefense, with firms such as Microsoft, Alphabet and others working overtime to identify threats to Ukraine, patch vulnerabilities and share information. Additionally, in anticipation of Russian cyber action, the United States and Britain dispatched cyber defensive teams to Ukraine in December. Reporting suggests that U.S. cyber mission teams continue to support Ukraine's cyberdefense from Eastern Europe.

Second, preemptive actions may have boosted Ukraine's resilience. Ukrainians were downloading encrypted communications applications such as Signal and offline maps — but the Ukrainian military also relied on old-school wired communications.

Third, low-cost cyber operations readily available to hacktivists and proxy groups — like the denial-of-service attacks or website defacements — disrupt and distract more than they create

tangible battlefield gains. In contrast, offensive cyber operations tailored to shut down another country's command-and-control or air-defense systems, for instance, can be challenging. It takes years of investment and human capital, pre-positioned access points and a mature, well-resourced organization to plan and carry out this type of complex cyber campaign.

And even the most sophisticated offensive cyber operations can't compete with conventional munitions. It's far easier to target the enemy with artillery, mortars and bombers than with exquisite and ephemeral cyber power. Notwithstanding any cyber vulnerabilities, it's much simpler for Russia to launch an artillery barrage at a power substation than to hack it from Moscow. Russia's airstrikes against a Ukrainian television tower may be a case in point.

Could the cyber game change?

The cyber dimension of this conflict may yet change, of course. But the fact that cyber operations are not always easy, cheap or effective in managing destruction at scale means they're unlikely to produce the game-changing moment in modern warfare that many anticipated.

Cyberweapons may be used beyond the battlefield, however. There is still a risk that Russia may conduct retaliatory cyberattacks against the United States and its allies. Russia probably has already pre-positioned accesses that it could exploit to conduct disruptive attacks. There is a long history of countries — Russia included — responding in cyberspace to actions like sanctions and indictments.

Most importantly, cyber experts may be missing the forest for the trees, given the large-scale interstate war unfolding at the moment. The success or failure of theories of cyberwarfare have minimal relevance when considering the humanitarian catastrophe and enormous toll that combat inflicts — not to mention the risks of nuclear warfare.

Brandon Valeriano is a senior fellow at the Cato Institute and a distinguished senior fellow at the Marine Corps University.