THE NATIONAL INTEREST

Calls for a Cyber 'No-Fly Zone' Are Reckless and Unrealistic

The war in Ukraine is far beyond the point where cyber operations can shape the conflict in a manner capable of limiting violence.

by Brandon Valeriano

March 25, 2022

President Volodymyr Zelenskyy's impassioned address to Congress added pressure on the United States to provide more support for Ukraine. While President Joe Biden might be able to resist calls for a no-fly zone by remarking that doing so is "called World War Three," pundits will continue to push the West to provide more direct military support to Ukraine during this devastating war.

Providing material support to Ukraine might be entirely within the bounds of historical and legal precedent. However, taking the idea to its logical extreme by suggesting the United States let loose the cyber "dogs of war" is a dangerous move that will likely drag the United States into direct conflict with Russia. Offensive cyber operations conducted by the U.S. military would be grounds for the expansion of the war and would make U.S. facilities legitimate targets during ongoing warfare.

Cyber Options During the War

Three weeks into a war with seemingly little cyber activity, the idea that the United States can launch offensive cyber operations against Russia to stop aggression without triggering escalation is starting to take hold. The key reason why cyber operations have not been utilized during the war is that they have limited coercive and battlefield impacts, which suggests that they can do little to augment the already escalating violence in Ukraine.

Cybersecurity is not magic, yet some seem to talk as if it is capable of achieving dramatic and disparate effects from the distance and relative safety of Fort Meade. The defense and skill of the attacker play massive roles in the equation of cyberwar.

In a quest for some magical cyber capabilities, Fox News White House correspondent Jacqui Heinrich noted that "some members of Congress are beginning to advocate for a non-kinetic no-fly zone—something to the effect of using electromagnetic pulse, sonar, and cyber to keep Russian jets on the ground so they can never take off." Just as there is no such thing as a limited no-fly zone, there is no such thing as a non-kinetic no-fly zone enabled through cyber weaponry.

In another example, when asked on CNN about options if Russia escalates the war further, Gen. Mark Kimmitt (ret.) said, "I know David Sanger is going to disagree with me, but this may be the opportunity for a cyber-attack, one limited in scope but one that clearly sends a message that there will be a penalty if [Russia] use[s] chemical weapons." Even after saying that he knows "there are no magic bullets," Kimmitt offered a fantastical solution to the war in Ukraine.

The Risk of Cyber Escalation

While there is a low risk of cyber escalation historically and logically, this does not mean that launching a cyber offensive comes without the massive risk of horizontal escalation spreading the war to other parties or proxies. When cyber scholars speak of limited escalation risks in cybersecurity, they typically refer to vertical escalation in severity and damage, not the risk of dragging third parties into the conflict, a key danger of using cyber options in support of Ukraine.

Cyber capabilities can serve as tools of conflict management by offering off-ramps and sending signals to the opposition. Yet it is difficult to manage a conflict that has already become a war for national survival. The war in Ukraine is far beyond the point where cyber operations can shape the conflict in a manner capable of limiting violence—Russia is already shelling maternity wards, hospitals, and playgrounds.

The risks of providing direct offensive cyber support to Ukraine are not limited to escalation; they also include the problem of unintended consequences with cyber operations. Cyber weapons are not precise, nor are they really weapons. The idea of targeted and pinpoint accurate cyber operations betrays the evidence that even the most targeted operations, such as the Russian operation against Ukrainian tax software, can spread to a massive extent. Even Stuxnet, a precise operation targeting a non-networked facility in Iran, spread into the wild.

Offering offensive cyber support can also activate proxy and criminal elements. The Conti ransomware group stated that "as a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world." Even more dangerous is the threat that such operations could pose to American allies and partners, including those in private industry. The U.S. government has the resources and ability to protect its interests, but it is not clear that our allies are organized in a manner that can forestall digital disaster.

We Shouldn't Find Out

In Kim Zetter's comprehensive review of U.S. cyber capabilities and their potential to impact Russian operations, Robert Lee, CEO of the cybersecurity firm Dragos and former National Security Agency "hacker," made a key statement on American restraint. "Now is not the time to go poking around. Unless you have a … good need to be there, don't go doing something that could be perceived as escalatory."

"Mess around and find out" has become a popular meme, and the sentiment directly applies to the war in Ukraine. Now is not the time to experiment and find out the limits of Russian aggression. In fact, it is likely there are no limits. While the risks of escalation after cyber action are limited, the context of the war and Russia's belligerence suggest that it is a dangerous time to test the bounds of cyber escalation theory.

Cyber operations are difficult to leverage for effect; academic research shows that they are ambiguous and weak signals. But empirical academic observations do not make for easy policy options. Discussions of how to employ cyber operations during a crisis need to advance to the point where there is a clear and realistic strategy for their impact that does not buy into the hype offered by cyber operations.

Abstract discussions of what can be done to help the Ukrainian people may transform into a moral imperative at some point. However, if that happens, it does not mean that technological tools can be leveraged to minimize violence. There is no sanitizing violence through cyber operations. Cyber operations do not offer a magical solution to the conflict, and anyone selling this bill of goods has clearly moved on from slinging swampland in Florida.

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