THE NATIONAL INTEREST

What Ukraine Shows About Cyber Defense and Partnerships

Fixation on the offensive aspects of cyber strategy obscures the key role of the defense in reducing cyber threats.

Brandon Valeriano and Erica D. Lonergan
March 17, 2022

Across two days of Congressional testimony on the intelligence community's latest annual threat assessment, lawmakers peppered Gen. Paul Nakasone, Commander of U.S. Cyber Command and Director of the National Security Agency (NSA), with questions about the role of offensive cyber operations in the ongoing conflict in Ukraine. Much of the focus was on the apparent lack of notable strategic Russian cyber operations against Ukraine's critical infrastructure.

An important question raised by the Ukraine conflict regards its implications for the future of U.S. cyber strategy, particularly the Department of Defense's "defend forward" approach, which was launched in 2018. While much of the debate surrounding this concept has focused on the role of offensive cyber operations, collaboration with allies and partners is a critical but less publicly recognized element of defend forward. According to the strategy, the Department of Defense "will work to strengthen the capacity of these allies and partners and increase [the Department of Defense's] ability to leverage its partners' unique skill, resources, capabilities, and perspectives."

Since 2018, U.S. Cyber Command has reportedly conducted a number of joint cyber operations, ranging from working with the United Kingdom to tackle ransomware groups to conducting "hunt forward" cyber operations with allies like Estonia and Montenegro to defend against shared cyber threats. This collaboration represents an evident path forward for U.S. cyber strategy after the war in Ukraine.

Absence of Offensive Attacks With Strategic Impacts

With many policymakers and experts holding onto ideas about the efficacy of offensive cyber operations during wartime, observers have been perplexed at the lack, so far, of cyber operations launched at scale against Ukraine. This is particularly surprising, given that Russian strategic thinking conceptualizes a role for cyber operations in targeting critical infrastructure and command and control systems as an enabler of or complement to conventional military force.

Indeed, U.S. and European officials alike have noted that cyber warfare has not been a significant feature of Russia's initial campaign. For instance, Nakasone is reported to have testified that although Russia conducted "several" cyberattacks against Ukraine in recent weeks, the level of hacking was not "what we had anticipated" before the war began. Reporters noted that he subsequently clarified that the NSA has observed three to four Russian cyberattacks against Ukraine and warned about the potential for future ransomware attacks. EU officials have likewise noted that they "haven't seen a significant increase in cyberattacks."

The Potential Success of Cyber Defense

A number of potential hypotheses could account for the absence of large-scale cyber warfare in the initial stages of Russia's campaign. As we have noted elsewhere, the logic behind leveraging cyber for decisive effects on the battlefield lacks empirical support. Past behavior demonstrates that while cyber activities can be useful for undermining trust, gaining an information advantage, or causing disruption, they have little impact on the battlefield. One hypothesis in particular warrants further exploration: the role of successful cyber defense and resilience in Ukraine.

A persistent—but erroneous—assumption about cyberspace is that the offense has an advantage over the defense. Many experts depict cyberspace as an "offense-superior domain," where attacks happen quickly and, often, with little warning. But many political scientists are skeptical, particularly given the time, resources, and skill that successful cyber offense—especially at the strategic level—can demand.

Some senior leaders seem to think that the lack of Russian cyberwar is due to the success of Ukraine's defense. Nakasone noted that this success in minimizing cyber activity might be due to "some of the work that others have been able to do to prevent [Russian] actions." However, he did not elaborate on what specific "work" might have been done or the "others" that may have been involved.

There have been numerous media reports indicating that the United States has been assisting Ukraine in its cyber defense efforts for several months. After reporting last December that U.S. Cyber Command would be supporting Ukrainian network operators, the *New York Times* reported on March 7 that "forces from United States Cyber Command known as

'cybermission teams' are in place to interfere with Russia's digital attacks and communications—but measuring their success rate is difficult."

The *Financial Times* notes that "officials in Ukraine and the U.S. are careful to describe the work of the 'cybermission teams' as defensive," with successes reportedly including protecting Ukrainian rail systems as they evacuate civilians and providing support to thwart distributed denial of service (DDoS) attacks. In addition to protective moves by the United States, tech giants in the private sector and Ukraine's "IT Army" appear to be factors in limiting the potential scale of Russia's offensive cyber operations. But it is an open question just how far the United States can go in supporting Ukraine without becoming more directly involved in the war. As Kim Zetter puts it in *Politico*, now is not the time to "poke around and find out."

Implications for U.S. Cyber Strategy

It will take time to sort out the factors that account for the lack of significant Russian cyberattacks in the first few weeks of the war in Ukraine. However, if the evidence ultimately supports Nakasone's initial contention that successful cyber defense—conducted not only by Ukraine but also by "other" parties—played a role in mitigating Russia's cyber threat, then there are two important implications for the future of U.S. cyber strategy.

First, investing in cyber defense and resilience—especially in anticipation of impending adversary actions—is not a fool's errand. Second, there are opportunities for the Department of Defense to build on existing international partnerships as part of its defending forward concept. These tasks are mutually reinforcing; anticipatory defensive measures depend on early warning, which is enabled by the kind of shared understanding of the threat environment that comes with working with other stakeholders—especially allies and partners that may be closer to or have better knowledge of adversary cyber activity.

Therefore, fixation on the offensive aspects of the Department of Defense's cyber strategy obscures the key role of the defense in reducing cyber threats. Indeed, defensive collaboration is a critical enabling factor in the defend forward strategy and should be prioritized even more in the wake of Russia's invasion of Ukraine.

Ukraine is now joining NATO's Cooperative Cyber Defense Centre of Excellence as a contributing participant after a unanimous vote in favor of Ukrainian membership. Moving forward, it is imperative for the United States to take collaboration seriously by institutionalizing multilateral and bilateral agreements with partner states and making such agreements central to its cyber strategy. Shaping the environment in favor of the defense is a path toward stability amid the instability witnessed in outright warfare.

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