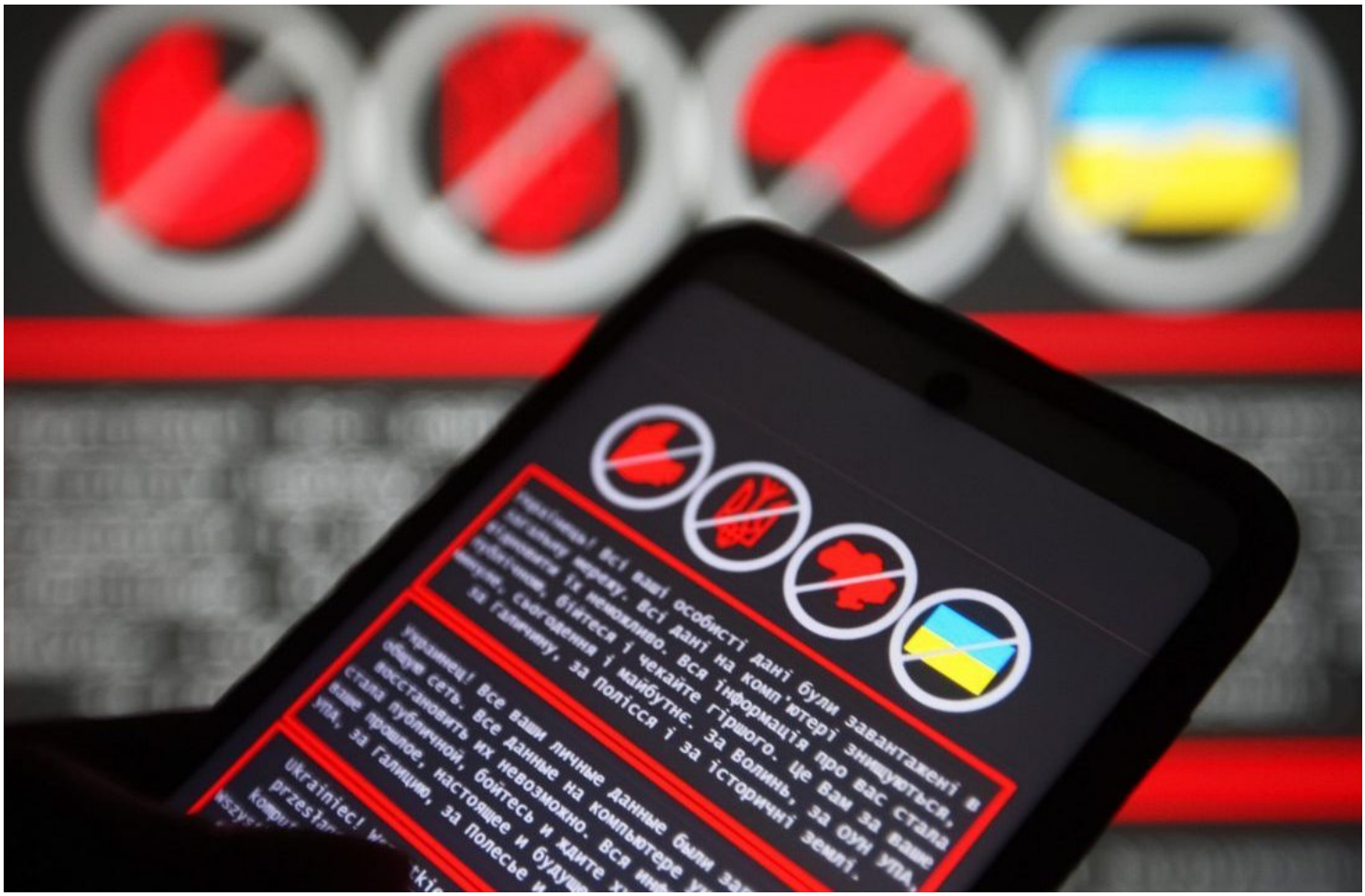
Russia Won't Play the Cyber Card, Yet

By Jan Kallberg

March 30, 2022

Russia has three means to bolster its international image and project strength — conventional forces, cyber, and nuclear weapons. Only one has been used so far, and for good reason.



Across the political landscape and in the media, both in North America and Europe, there is a recently established assumption that Russia is poised to unleash its full range of cyberattacks in the Russian-Ukrainian war as retribution for Western support of Ukraine. According to these commentaries, digitalized Russian fury could easily spill over to Western countries and provide us with a hint of a cyber crescendo. But the predictions of Russian cyber doomsday don't add up.

There have of course been cyber-attacks during the past month of full-scale war. But the most significant of these, the digital assault on Ukraine's Internet company, Ukrtelecom, was a tactical/operational move seeking to limit the Ukrainian military's command and control, which is dispersed and utilizing Internet apps to create ad hoc command and communication networks. The Russians want to degrade and disrupt the Ukrainian ability to direct its forces and to communicate. The attack on Ukrtelecom is surgical, a precision strike, but it is one single event without a strategic objective.

The lingering threat of offensive cyber operations is one of Putin's very last cards — together with nukes. There is no rational reason that Putin's Russia would play this without some reasonable prospect of geopolitical gain. The use of cyber capabilities exposes techniques and programs to potential enemies and opens up the attacker to countermeasures. A failure would add to the disastrous debacle of Russia's joint conventional military operations, and leave the country with very little to demonstrate its supposed superpower status beyond weapons of mass destruction.

Russia has reached an operational stalemate in its invasion of Ukraine, but unleashing its advanced cyber capabilities at this stage against Western targets will not win the war. Such attacks will only increase the support for Ukraine without bringing Russia any tangible battlefield advantage. It would also open the Kremlin to counter-attack by Western cyber agencies.

Western commentaries predicting a Russian cyber-onslaught rest on a general assumption that advanced offensive cyber capabilities can be replaced once used. In reality, this assumption is illogical: there is no hidden cyber armory from which new weapons can be fetched and reloaded for continued cyber bombardment. Exploits, once used, are often parried quickly, and they cannot thereafter be expected to have the same effect as when first unleashed.

Each advanced and sophisticated offensive cyber weapon represents an investment that, in many cases, is a one-shot ability to exploit a vulnerability. Striking targets in America and the rest of NATO utilizing advanced offensive cyber weapons, without any other goal than to degrade and disrupt, is wasting offensive cyber power. Russia is therefore unlikely to utilize its offensive cyber arsenal in a conflict where there is no value to a cyberattack, especially when its objectives can be achieved by the use of kinetic methods: for example through the use of airstrikes, Kalibr cruise missiles, and indirect fire.

Russia will use advanced strategic cyber at well-defined critical junctures. For example, as a conflict in Europe might unfold and to drag in NATO, Russian forces would seek to delay the entry of major US forces through cyber-attacks against railways, ports, and electric facilities along the route to the port of embarkation. Those seven days of delay would give Russia additional time to achieve its ends in Europe and would enable the submarines of the Northern Fleet to reach wartime positions in the Atlantic. Strategic cyber supports strategic intent and actions.

All cyber-attacks are not the same, and just because an attack originates from Russia doesn't mean it is directed by strategic intent. Naturally, the Kremlin would allow cyber vandalism and cybercrime groups (both well represented within its borders) to run rampant in the West, because these are ways of striking the adversary. But these low-end activities do not represent the Russian military complex's cyber capabilities, nor do they reflect the Russian leadership's strategic intent.

The recent cyberattacks in Ukraine have been unsophisticated and have had close to no strategic impact. The distributed denial-of-service (DDoS) cyber-attacks are low-end efforts, a nuisance that most corporations already have systems to mitigate. Such DDoS attacks will not bring down a country or force it to submit to foreign will. These are very significantly different from advanced offensive cyber weapons. Top-of-the-range cyber weapons are designed to destroy, degrade, and disrupt systems, eradicate trust and pollute data integrity. DDoS and website defacements do not even come close in their effects.

A Russian cyber-offensive would showcase its full range of advanced offensive cyber capabilities against Ukraine, along with its tactics, techniques, and procedures (TTP), which would then be compromised. NATO and other neighboring nations,

including China and Iran, would know the extent of Russian capabilities and have effective insights into Russia's modus operandi.

From a Russian point of view, if a potential adversary understood its TTP, strategic surprise would evaporate, and the Russian cyber force would lose the initiative in a more strategically significant future conflict.

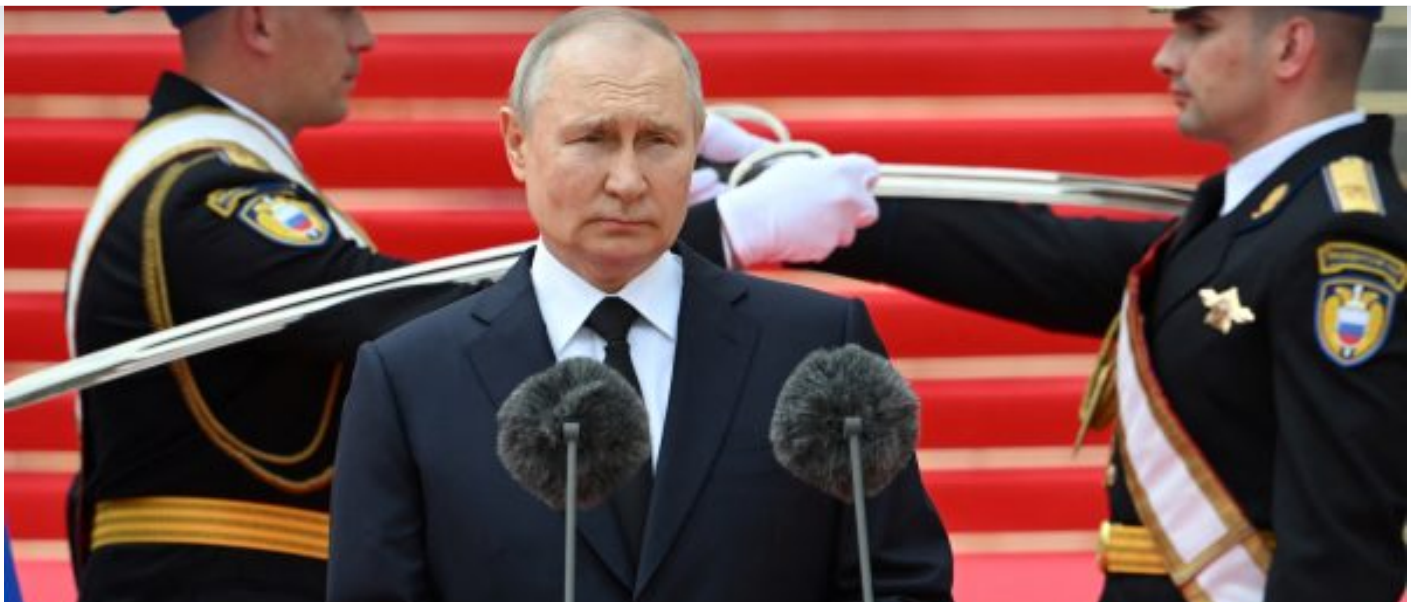
Understanding the Russian point of view is essential because it is the Russians who conduct their offensive actions. This might sound like stating the obvious, but currently, the prevailing conventional wisdom is a Western think-tank-driven context, which in my opinion, is inaccurate. There is nothing for the Russians to strategically gain by unleashing their full, advanced cyber arsenal against Ukraine or NATO at this juncture. In an open conflict between Russia and NATO, the Kremlin's calculation would be different and might well justify the use of advanced cyber capabilities.

In reality, the absence of cyber-attacks beyond Ukraine indicates a very rational Russian fear of disclosing and compromising capabilities beyond its own. That is the good news. The bad news is that the absence of a cyber-offensive does not mean these advanced capabilities do not exist.

Jan Kallberg, Ph.D., LL.M., has been focused on cyber for several years. He is a faculty member at New York University and George Washington University. Professionally he holds the CISSP and CISM cybersecurity certifications. His works have appeared in Joint Forces Quarterly, Strategic Studies Quarterly, IEEE Security & Privacy, and IEEE Access. Follow him at cyberdefense.com and @Cyberdefensecom.

The views expressed here are personal opinions and do not reflect any employer's position.

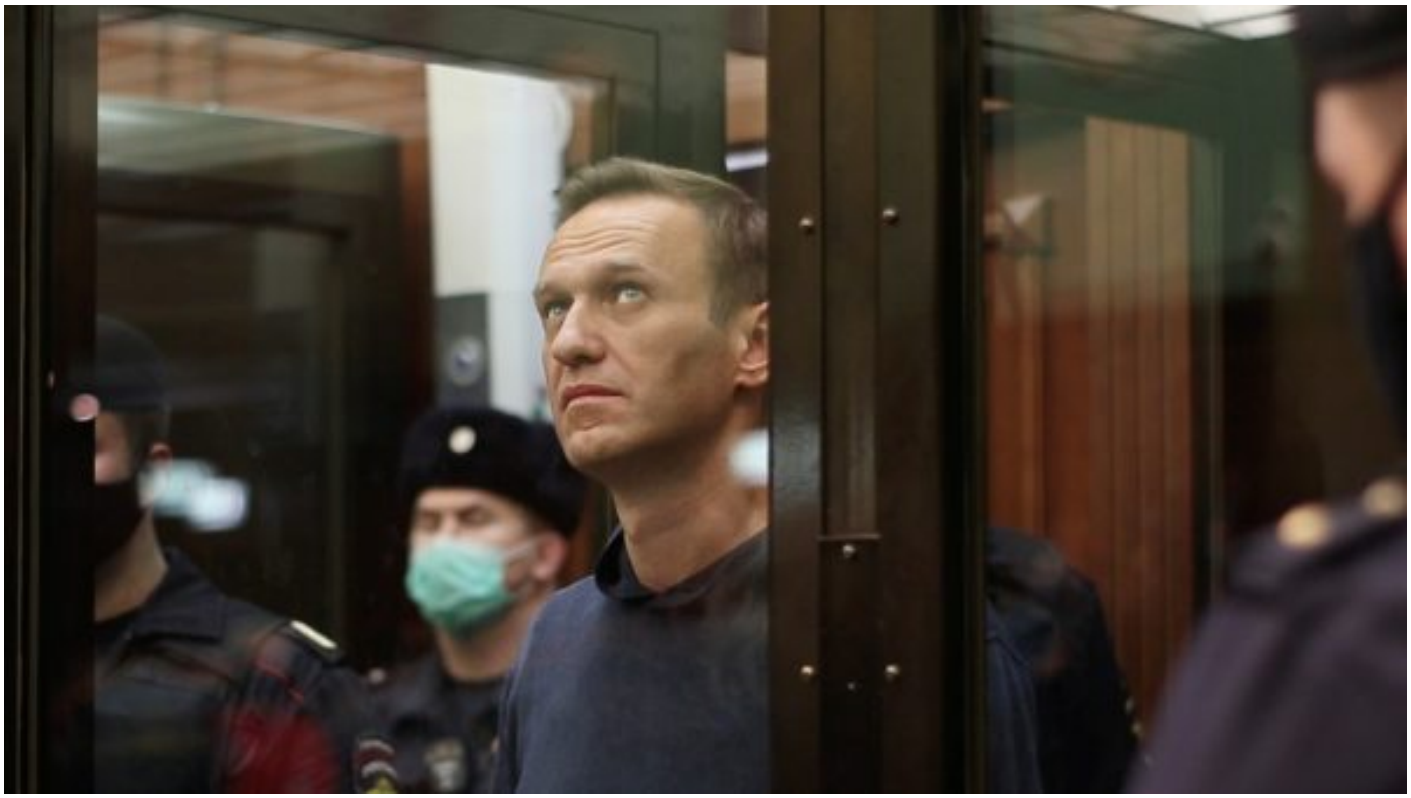
Related Articles



Putin Pitches for the Heart of Victimworld

November 16, 2023

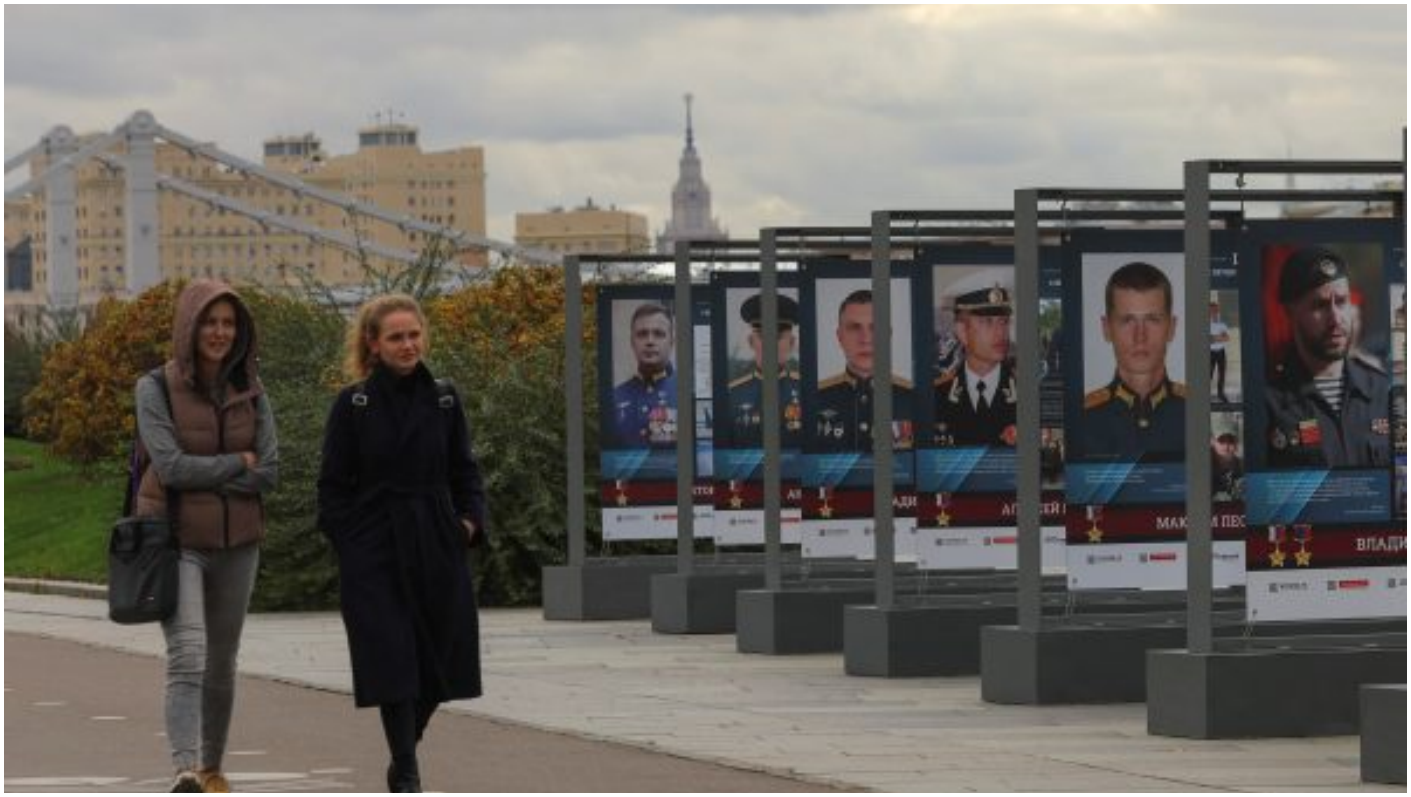
CIVIL SOCIETY EUROPE'S EDGE HYBRID THREATS RUSSIA



Deathly Doses — Putin's Poisoners Go Unpunished

November 16, 2023

EUROPE'S EDGE HYBRID THREATS REGIONAL SECURITY RUSSIA



Women Enter the Putin Regime's Crosshairs

November 16, 2023

CIVIL SOCIETY EUROPE'S EDGE RULE OF LAW RUSSIA

Related Issue Tags

CYBERSECURITY EUROPE'S EDGE RUSSIA

Photo: In this photo illustration, a warning message in Ukrainian, Russian and Polish languages is displayed on a smartphone screen and in the background. Hackers carried out attacks on several of Ukraine's government websites, including the Ministry of Foreign Affairs, the Ministry of Education and Science, the State Service for Emergency Situation, and others, reportedly by local media. This attack, on Ukrainian government web resources, is the largest in the last four years. Credit: Photo by Pavlo Gonchar / SOPA Images/Sipa USA.

Quick Links

Issues

Events

Insights & Analysis

About CEPA

Contact

1275 Pennsylvania Ave NW, Suite
400, Washington, DC 20004

Follow

Privacy Policy