CNA

November 2023

Assessing Russian Cyber and Information Warfare in Ukraine: Expectations, Realities, and Lessons

Jaclyn A. Kerr

Distribution unlimited

IOP-2023-U-037223-Final

Abstract

What lessons can be learned from the early phase of the Ukraine war concerning Russia's capabilities, strategy, and approach in cyberspace? To what extent do these point to broader conclusions about the domain's role during above-threshold military conflict? This article examines Russian use of cyber and information capabilities to influence the course of the Ukraine war, analyzing prior expectations, what is publicly known of wartime realities, potential reasons for disparity between the two, and the distinct and sometimes contradictory take-aways that have been drawn within the analytical community. While the lack of consensus among experts this far into the conflict demonstrates the difficulty of drawing conclusions with incomplete and early evidence, it also indicates a division between analyses focused on evidence of Russian cyber activities versus those focused on questions of strategic impact. It likewise highlights the challenges to strategic learning and adaptation posed by the domain's covert nature.

This report is part of a series generously funded by a grant from the Carnegie Corporation of New York.

This work was performed under Specific Authority Contract No. G-19-56503

Cover image: Created by author using DALL-E software.

Approved by: **November 2023**

Colleen McCue, PhD, Acting Research Program Director
Countering Threats and Challenges Program
Strategy, Policy, Plans, and Programs Division

Contents