



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

Jaclyn A. Kerr

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. CNA's Occasional Paper series is published by CNA, but the opinions expressed are those of the author and do not necessarily reflect the views of CNA or the official policy or position of the Department of the Navy, the National Defense University, the Department of Defense, or the US government.

Approved for public release: distribution unlimited.

11/22/2023

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

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

This document may contain materials protected by the Fair Use guidelines of Section 107 of the Copyright Act, for research purposes only. Any such content is copyrighted and not owned by CNA. All rights and credits go directly to content's rightful owner.

Approved by:



November 2023

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

Contents

Introduction..... 1

Russia’s Approach to Cyberspace 5

 A sophisticated threat actor..... 5

 Ukraine as “test bed” 8

Wartime Expectations and Realities.....10

 Great expectations 10

 Lackluster realities? 12

What Happened: A Bark, but Not a Bite?20

 Conflict-specific explanations 20

 Broader lessons for wartime cyber 27

Conclusion: Strategic Adaptation and the Wartime Cyber Debate32

 Parsing the wartime cyber debate 32

 Information, adaptation, and learning..... 35

References37