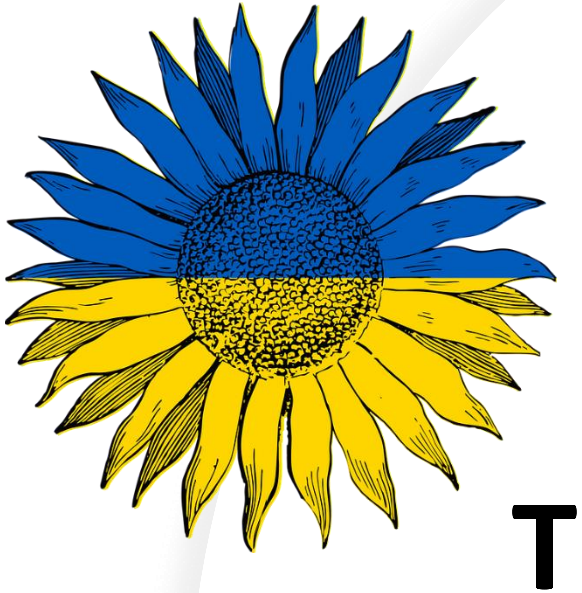


The Missing Cyber Storm: Russian Cyber Operations During the Russo-Ukrainian War

Brandon Valeriano, Marine Corps University, drbvaler@gmail.com
Grace Mueller, Benjamin Jensen, and Ryan Maness

The Coming Cyber Storm/Thunder Run

- "Russian cyberattacks on government and military command and control centers, logistics, emergency services, and other critical services such as border control stations were entirely consistent with a so-called *thunder run strategy* intended to stoke chaos, confusion, and uncertainty, and ultimately avoid a costly and protracted war in Ukraine."

  -Cattler and Black (2022)

Introduction

- Pundits and academics alike came out with grand predictions about the war starting with a “shock and awe” and a “cyber thunder run” enabled by cyber
- “A Russian invasion of Ukraine may redefine how we think about cyber conflict because it will be the first time a state with real cyber capabilities is willing to take risks and put it all on the line.” Jason Healey – Columbia
- The excitement of war took hold for many who predicted that the conflict would be transformed by technology defying an emerging conventional wisdom on cyber operations.
- We review the war at its six-month mark, examining the impact of cyber operations on the course of the Russo-Ukrainian War, exploring the severity of operations, and examine the style and purpose of the attacks
- Debate speaks to core theories and assumptions about the future of war and power of emergent technology.

Overview

- Cyber Strategies/Options
- Russia’s Past Cyber Profile
- Expectations for Russo-Ukrainian War
- Research Methods
- Results
- Discussion

Cyber Strategies

- Disruption
- Espionage
- Degradation

- It is possible to empirical examine cyber operations

Russia's Cyber Profile (2000-2020)

Russia is frequently the initiator, rarely the target

Most cyber incidents are launched for disruption or espionage purposes; more of a nuisance than degrading

Cyber incidents are often not often severe – and never result in concessions made by Ukraine

Private sector actors and government/local authorities are more frequently targeted than military actors

Nearly 1/3 of incidents sought to communicate or manipulate the reception of digital information for malicious purposes

Source: Maness et al.’s (2022) Dyadic Cyber Incident and Campaign Dataset
30 cyber incidents between Russia and Ukraine between 2000-2020

Cyber Incidents in the Russo-Ukrainian War

- SSSCIP Weekly State Reports
  - March 3, 2022 – May 15, 2022
- Microsoft Reports
  - April 27, 2022
  - June 22, 2022
- 47 cyber incidents

Hypotheses

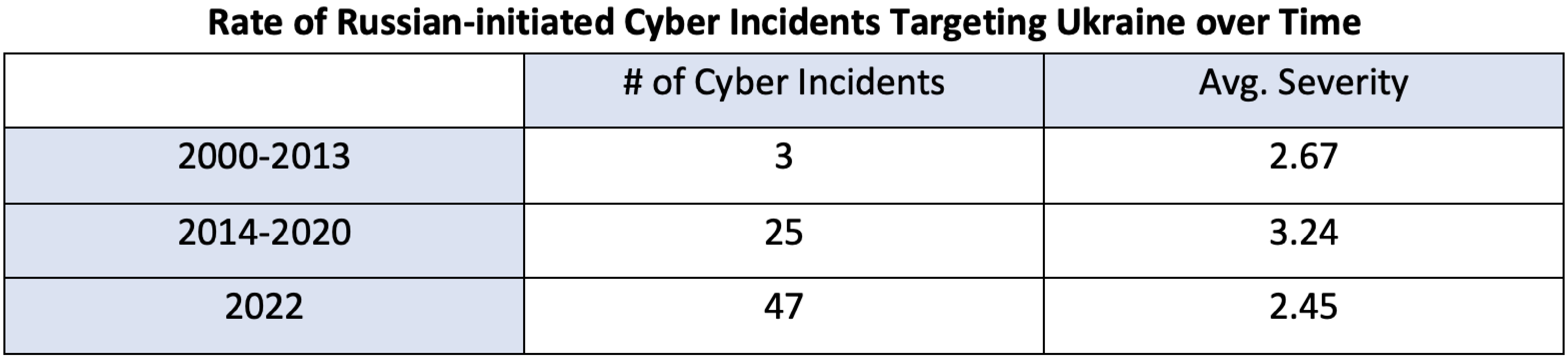
H1: Cyber operations will increase in their rate and severity over the course of the Russo Ukrainian 2022 conflict compared to pre-war sample.

H2: Russia will continue to leverage disruptive shaping activities and espionage to alter the balance of risk calculations prior to and during the conflict.

H3: Cyber operations will continue to demonstrate a limited coercive impact during the war. Targets will shift from civilian to primarily military/government targets to degrade the adversary.

H4: Evidence of multidomain operations during the Russo-Ukrainian war will increase to signify increasing coordination between Russian government/military forces and cyber forces. There will further be evidence of increased examples of cyber-enabled information operations to support the war effort.

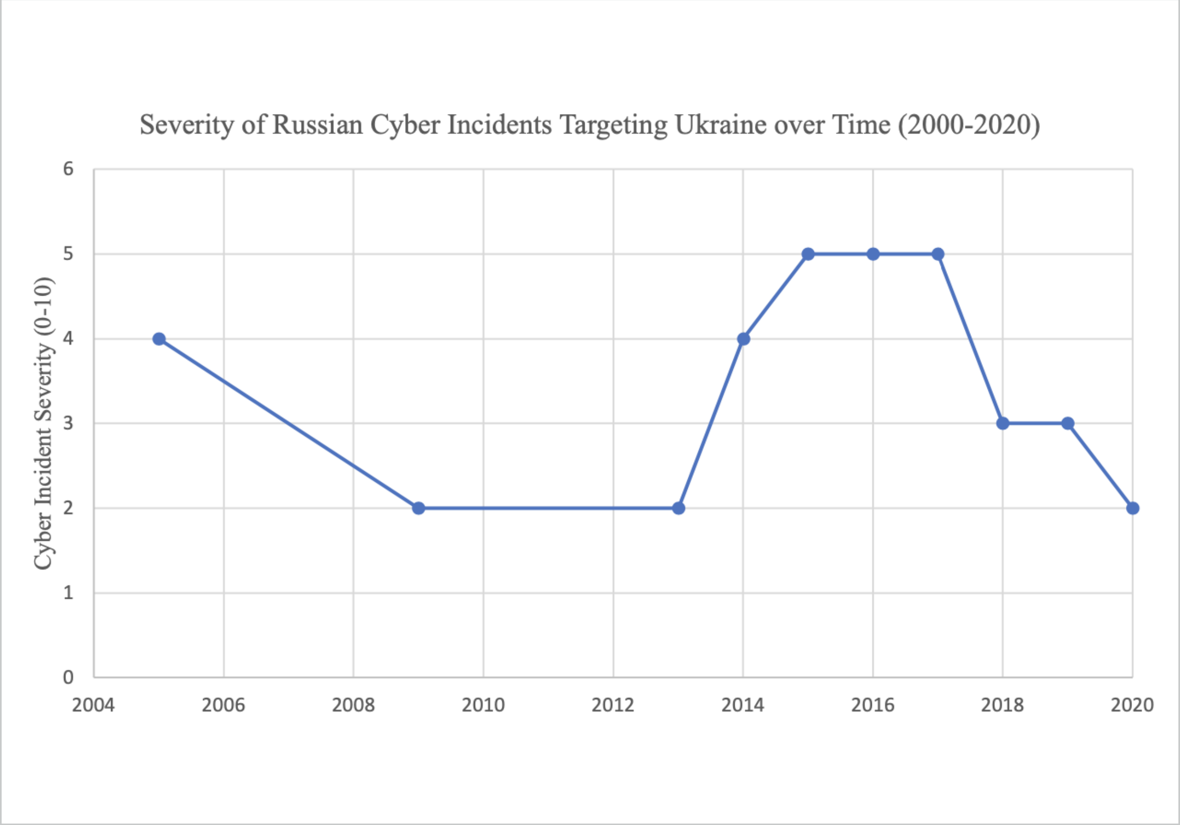
Results: Rate and Severity over Time



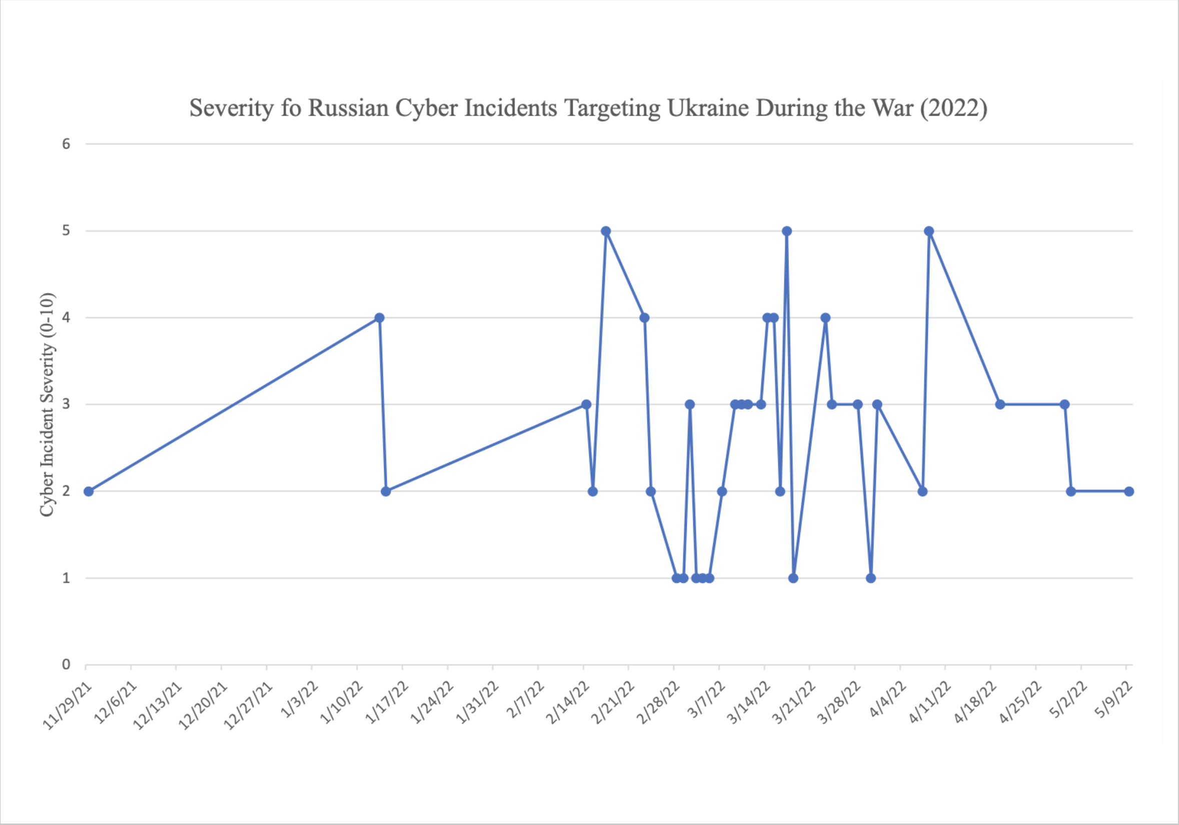
Rate of Russian-initiated Cyber Incidents Targeting Ukraine over Time

	# of Cyber Incidents	Avg. Severity
2000-2013	3	2.67
2014-2020	25	3.24
2022	47	2.45

Results: Rate and Severity over Time (cont’d)

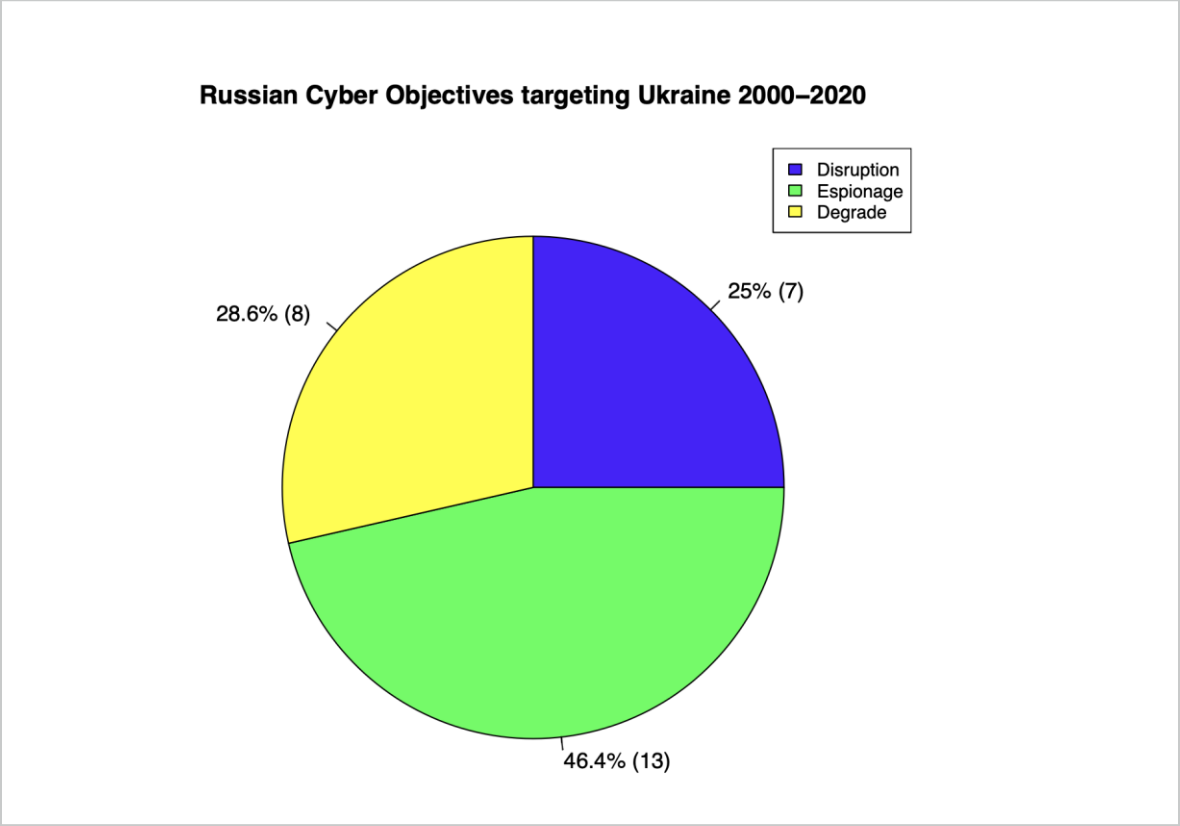


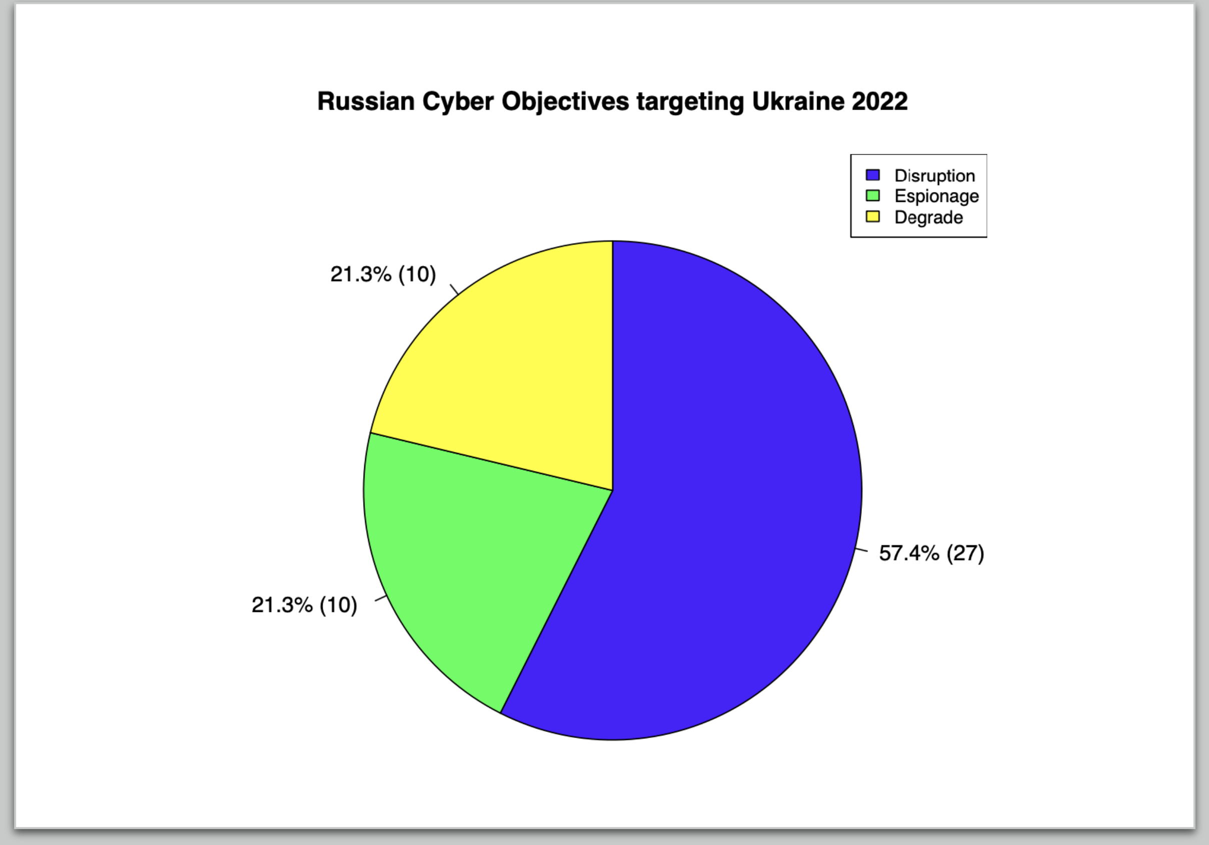
Severity of Russian Cyber Incidents Targeting Ukraine over Time (2000-2020)



Severity fo Russian Cyber Incidents Targeting Ukraine During the War (2022)

Results: Operations by Type

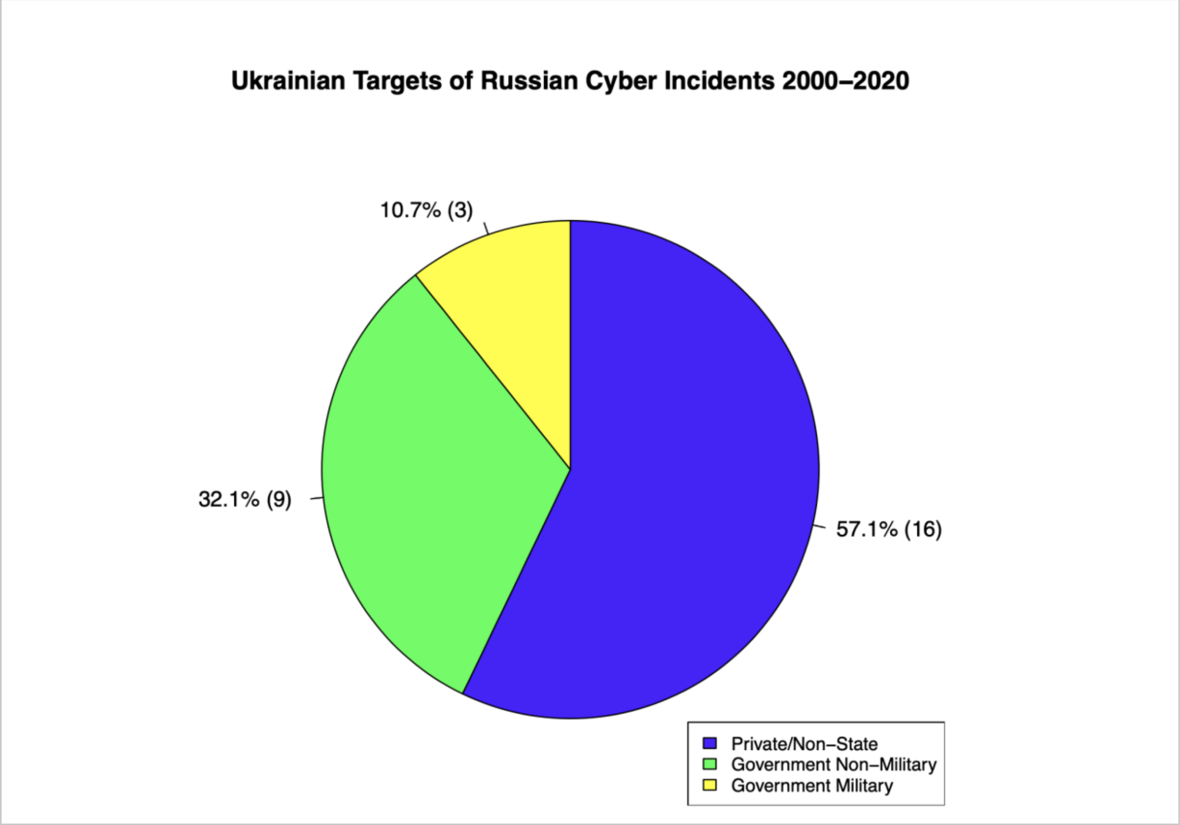




N=28

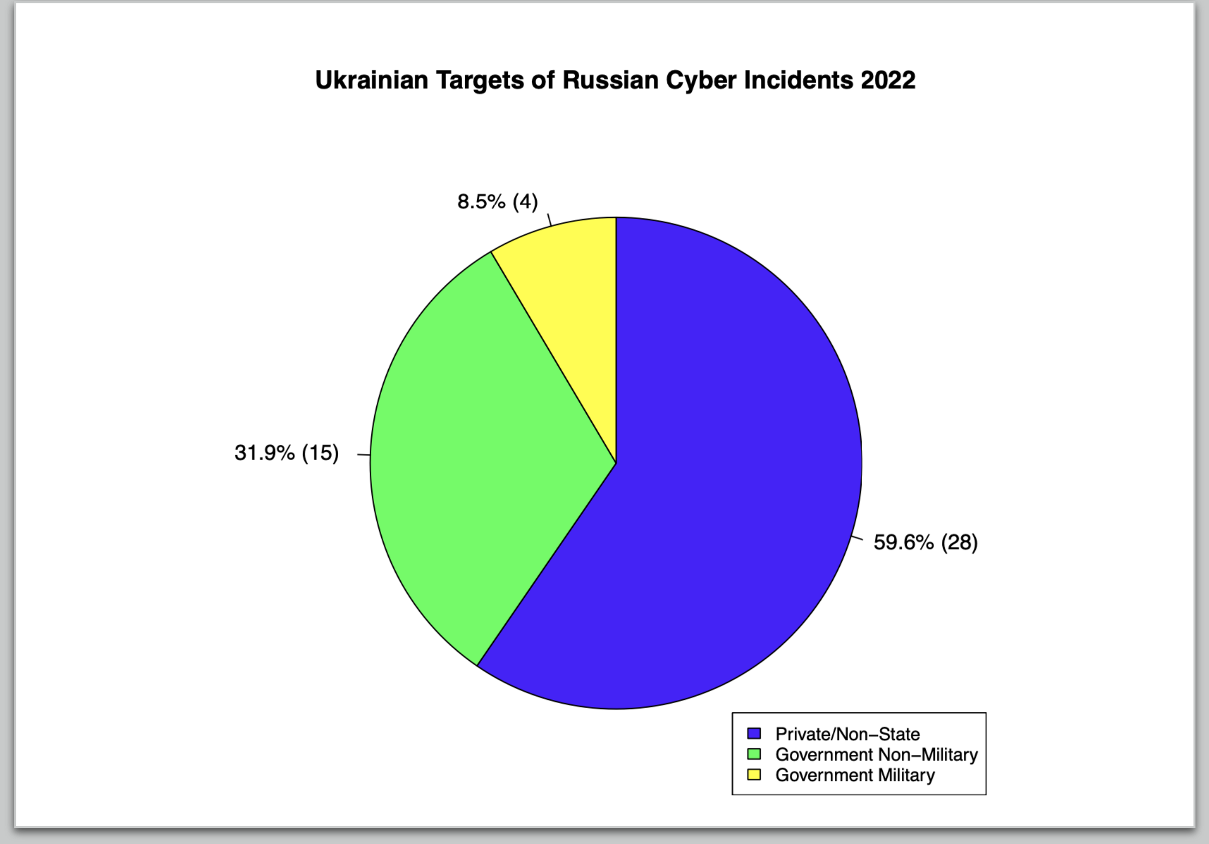
N=47

Results: Targets



Ukrainian Targets of Russian Cyber Incidents 2000–2020

Concessions Made = 0



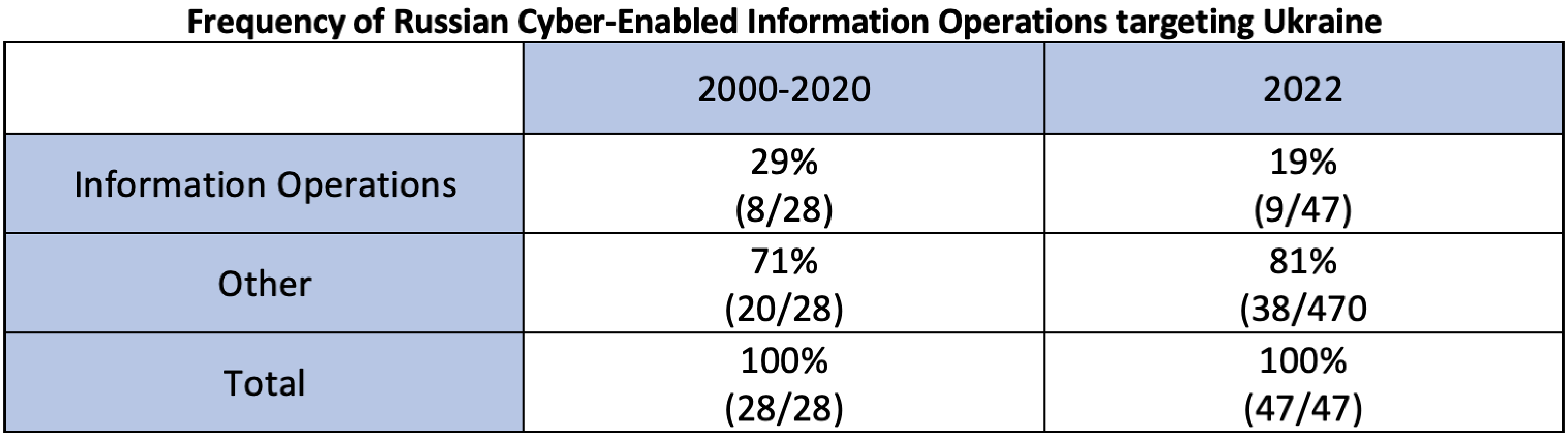
Ukrainian Targets of Russian Cyber Incidents 2022

Concessions Made = 0

Results: Coordination vs. Multidomain Operations

- Complementary or Additive Cyber
- 7/47 (15%) of cyber incidents involved multidomain operations
- Microsoft lists 6-7 coordinated incidents, but among how many total?
- Diversionary?

Results: Information Operations and Ransomware



Frequency of Russian Cyber-Enabled Information Operations targeting Ukraine

	2000-2020	2022
Information Operations	29% (8/28)	19% (9/47)
Other	71% (20/28)	81% (38/470
Total	100% (28/28)	100% (47/47)

Conclusion and Policy Implications

- Overall, we find that while there is an increase in cyber operations during the war, but we do not observe is an increase in the concessions, severity, or a difference in targets or methods of access.
- We find little evidence for coordination between cyber operations and conventional operations in the form of multidomain operations.
- Unfortunately for Russia, cyber operations offer no shortcuts in war.
- The central fact remains, cyber operations do not dramatically aid in the undertaking of military, diplomatic, or espionage operations in the context of war.
- Those that argue for massive transformation and revolution must confront the evidence and reality, not the motivated reasoning offered by those dreaming of a different way of war.

Questions