Integrating Cyber Into Multi-Domain Operations

Morgan Ericsson – Mentors: Dr. Clemente Izurieta, Yvette Hastings

Introduction

- Modern military operations increasingly rely on cyberspace and digital networks to support communication, intelligence, and command functions
- U.S. doctrine recognizes cyberspace as a key domain within Multi-Domain Operations (MDO), but its operational role remains unclear for military planners
- This lack of clarity creates challenges in effectively integrating cyber capabilities into joint operations

Purpose:

- This study examines how cyberspace capabilities contribute to MDO within existing doctrinal mission structures

Methods

Approach

- Qualitative analysis of U.S. military doctrine and policy documents related to cyberspace operations and MDO
- Close reading and evaluation of doctrinal publications to identify how cyber capabilities are defined and employed

Framework

- Evaluation of cyberspace activities within three doctrinal mission categories:
  - ➢ Offensive Cyber Operations (OCO)
  - ➢ Defensive Cyber Operations (DCO)
  - ➢ Department of Defense Information Network (DODIN) Operations

Case Study Integration

- Use of selected real-world cyber operations to assess how doctrinal concepts are applied in practice
- Comparison of observed cyber effects with doctrinal expectations

Results

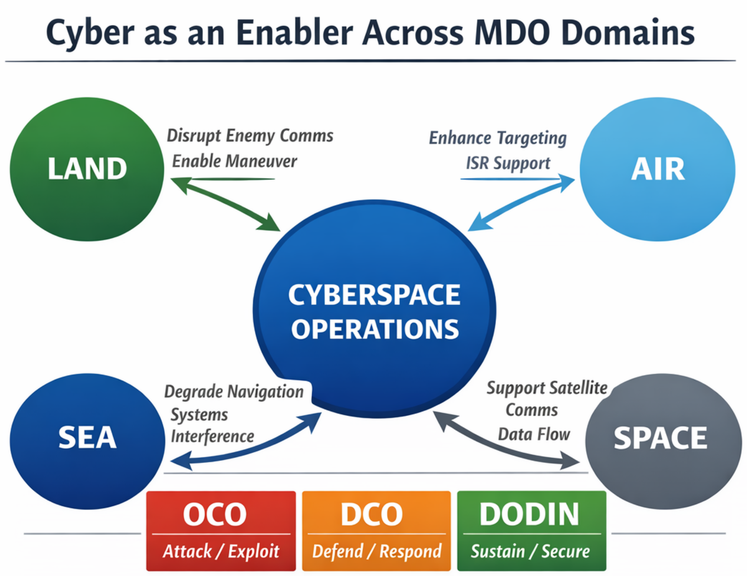

Fig. 1: Framework illustrating how cyber operations are integrated across MDO domains of land, air, sea, and space.

Case Study Evidence*:

(Case studies include both U.S. and foreign cyber operations to evaluate how doctrinal mission categories are applied across real-world conflicts)

1.US - Operation GLOWING SYMPHONY (2016)

- USCYBERCOM disrupted ISIS media and communication networks (OCO)
- Limited adversary coordination
- Demonstrated offensive cyber as a direct operational capability (DODIN)

2.RU - Russo-Georgian War (2008)

- First seen case of coordinated cyber and kinetic attacks (OCO)
- Cyber attacks preceded and supported conventional military action
- Disrupted communication and information flow

3.RU/UKR - Russia-Ukraine War (2022-Present)

- First LSCO (Large Scale Combat Operation) involving persistent use of cyber
- Russian OCO targeting Ukrainian Infrastructure (power grid, media, etc…)
- Ukraine utilizing DCO to maintain network resilience

Discussion

Interpretation

- Cyber capabilities consistently function as an enabling domain within MDO
- OCO, DCO, and DODIN correspond to distinct operational roles, but are not always clearly integrated into planning
- Real-world cases show cyber effects are persistent and integrated, not isolated actions

Implications

- Lack of doctrinal clarity creates challenges for commanders and planners
- Cyber capabilities risk being underutilized or misapplied in MDO environments
- Effective operations require synchronization of cyber with land, air, sea, and space domains

Suggestions

- Refine existing doctrine to explicitly define how cyber effects are planned, requested, and integrated alongside kinetic and non-kinetic operations

Acknowledgements

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.

References

1. National Security Archive. (2020, January 21). *U.S. Cyber Command after-action assessments: Operation Glowing Symphony*. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony
2. Army University Press. (2011). *Cyber operations in the Russo-Georgian War*. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20111231_art013.pdf
3. U.S. Department of Defense. (2023). *2023 DoD cyber strategy summary*. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF