2022

Interdisciplinary Study of Combating Hybrid Threats

Walzer, Lawrence M.; Karimova, Tahmina T.; Hancock, Michelle L.

Monterey, California: Naval Postgraduate School

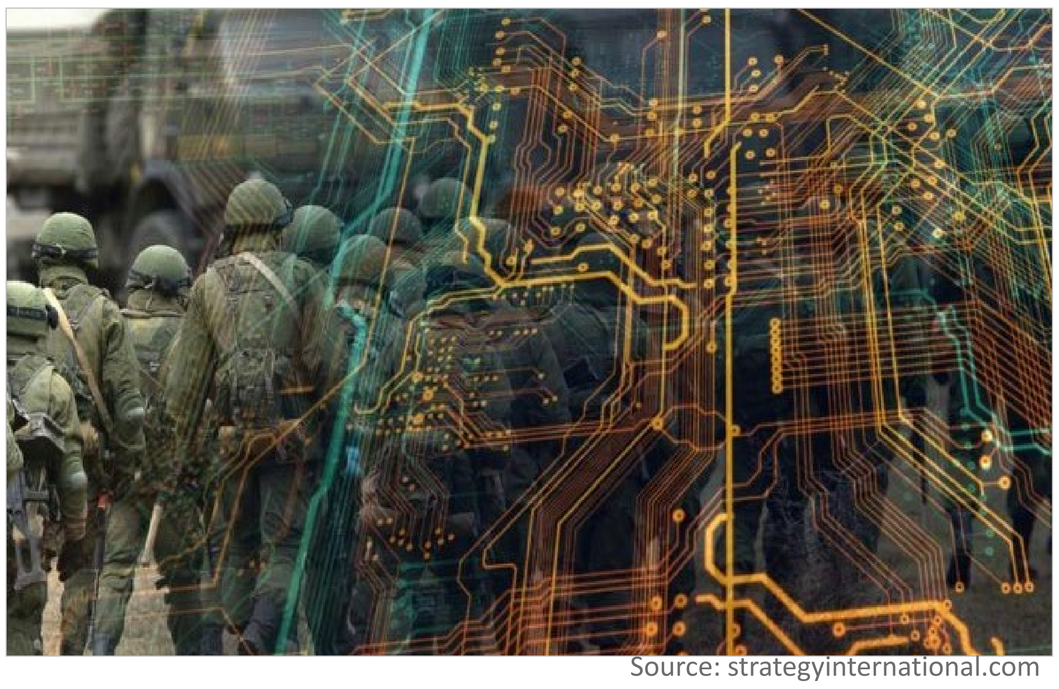
https://hdl.handle.net/10945/71830

INTERDISCIPLINARY STUDY ON COMBATING HYBRID THREATS

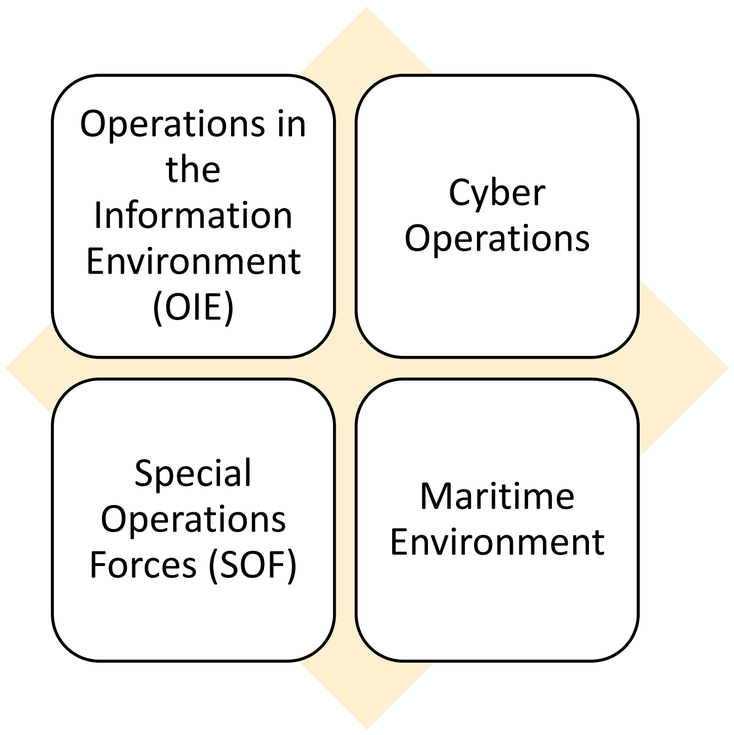
Naval Postgraduate School

Abstract

Our nation and allies are coming under increased attack by states and non-state actors who employ non-attributable actions below the threshold of war in order to weaken our competitive advantage across all domains, exploit our vulnerabilities, steal intellectual property, or undermine the cohesiveness of our alliances. These hybrid threats can be in the form of hacking networks, cyber-attacks against critical infrastructure, disinformation campaigns, electoral interference, etc. These unconventional actions cannot be answered with conventional military forces. This research effort conducted qualitative and quantitative research and analysis on DOD capabilities and gaps for countering hybrid threats, especially in the wake of Russia's ongoing war in Ukraine.



Source: strategyinternational.com



Domain Focus

Research Questions

The Interdisciplinary Study on Hybrid Threats sought to answer three broad questions on hybrid threats:

- *What are the current hybrid threat challenges?*
- *How should we respond to them?*
- *What do we need in order to execute an effective response?*

The conducted research helped address the primary objective of the research through the following steps. First, we arrived at a common understanding on the concept of hybrid threats. Second, we conceptualized an analytical framework to support designing actions to address and combat hybrid threats. Lastly, we identified key issues and capability gaps for further research.

Key Findings and Recommendations

The project confirmed the main hypothesis that adversarial powers will continue exercising their power through irregular means of influence, manipulation, and malign competition below the threshold of war to weaken our competitive advantage across all domains, exploit our vulnerabilities, and undermine the cohesiveness of our alliances and partnerships. The current Russia war in Ukraine provides a unique opportunity to further assess effective ways for the U.S. Naval Forces and the Department of Defense as well as allies and partners to optimize their toolkit and advance capabilities and capacities to combat adversary use of hybrid threats in strategic competition.

Key findings and recommendations of the FY22 research project highlight the following:

- OIE as a field of research and practice is about the ability to coercively impact the receiver through information appeals. It is time the field and practice of OIE moves beyond the surface examinations that typically suffice as research. Rigorous scientific methods are required to examine the data streaming out of open-source intelligence to gather an accurate read on the situation. OIE success needs interagency cooperation, education of the force, and the U.S. leading the narrative of the free societies of the world to push back against the growing influence of China and Russia in the information space.
- The assessed cyber security platforms provide adequate threat detection, enrichment, and assessment capability for a network operating in a logically isolated environment. However, there is a need for further analysis into the threat intelligence baseline used by both security orchestration, automation and response platforms to ensure the current default settings are enabling the type of desired functionality for automated response.
- Maritime hybrid threats present unique challenges due to unclear or disputed territorial waters and exclusive economic zones, the ever-increasing density of global maritime traffic, and presence of state-owned maritime enterprises and maritime militias that can blur the lines between military, law enforcement, and civilian actors. Credible and more resilient deterrence of hybrid threats in the maritime domain should include strengthened maritime governance and cooperation with partners, training and education of U.S. and allied maritime security personnel, greater public-private cooperation, advancement of new technologies, etc.
- By focusing on systemic, technological, and organizational change, the naval SOF community can identify unique injection points into the education pipeline to enable these warfighters to be able to confront the hybrid threat environment and meet mission as laid out within strategic guidance effectively and efficiently. Simply put, intellectual overmatch in a hybrid environment is not a block to check. It is an iterative process that requires our nation to look critically at its naval force education and organization and be prepared to weaponize the SOF-peculiar cognitive edge.

Researchers: Dr. Scott Jasper, National Security Affairs; Dr. Ryan Maness, Defense Analysis Department; Dr. Shannon Houck, Defense Analysis Department; Ms. Rebecca Lorentz, Defense Analysis Department; Ms. Cecilia Panella, Defense Analysis Department; LTJG Chris Mears, Department of Defense Analysis; Mr. Chris Kremidas, Institute of Security Governance; Ms. Tahmina Karimova, Energy Academic Group.

Topic Sponsor: CAPT, William Musser, USN, OPNAV N73. N7 - Warfighting Development

NRP Project ID: NPS-22-N056-A

This research is supported by funding from the Naval Postgraduate School, Naval Research Program (PE 0605853N/2098). Approved for public release; distribution is unlimited.