Calhoun: The NPS Institutional Archive

DSpace Repository

Faculty and Researchers | Faculty and Researchers' Publications

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/10945/71829

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL RESEARCH PROGRAM
NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

INTERDISCIPLINARY STUDY ON COMBATING HYBRID THREATS

EXECUTIVE SUMMARY

Principal Investigator (PI): Mr. Lawrence Walzer, Energy Academic Group/Center on Combating Hybrid Threats

Additional Researcher(s): Dr. Scott Jasper, National Security Affairs; Dr. Ryan Maness, Defense Analysis (DA); Dr. Shannon Houck, DA; Ms. Rebecca Lorentz, DA; Ms. Cecilia Panella, DA; Mr. Chris Kremidas, Institute of Security Governance; Ms. Tahmina Karimova, Energy Academic Group.

Student Participation: LT Chris Mears, USN, DA

Prepared for:
Topic Sponsor Lead Organization: N7 - Warfighting Development
Topic Sponsor Name(s): CAPT, William Musser, USN, OPNAV N73
Topic Sponsor Contact Information: Phone no: 703-695-6589; Email: 1illiam.g.musser@navy.mil

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

Project Summary

The study sought to answer three broad questions on hybrid threats: what are the current hybrid threat challenges; how should we respond to them; and what do we need to execute an effective response? To answer these questions, first, we analyzed the concepts of hybrid threats through the lenses of the Department of Defense (DOD) policy and doctrine, the European Union, North Atlantic Treaty Organization, and United Nations' guiding documents, as well as adversarial definitions. 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.

This research employed a mixed methods social scientific approach, including qualitative and quantitative analysis to ascertain the current level of understanding of hybrid threats and to identify misunderstandings and knowledge or capability gaps. Concurrently, the research team conducted a literature review on hybrid threats and hybrid warfare to gain an understanding from the actors' point of view and to identify the actors' objectives and intentions. We also incorporated and analyzed case studies, data sets, and playbooks of historic and recent attacks to illustrate the various methods and the effectiveness of hybrid threats and to assess potential responses to these threats.

We found that adversarial powers will rely on irregular means of influence, through subversive diplomatic and military means, below the threshold of war to challenge our competitive edge across all domains, exploit vulnerabilities, and undermine the cohesiveness of national security and international partnerships. The focus of the follow-on study centers on the ongoing Russia war in Ukraine to assess U.S. framework to combat hybrid threats as well as identify effective ways for the U.S. Naval Forces, DOD, and allied partners to enhance capabilities and capacities to deter emerging threats in strategic competition.

Keywords: *hybrid threats, hybrid warfare, cyber security, cyber warfare, disinformation, misinformation, infrastructure defense, infrastructure protection, energy security, information warfare, political warfare*

Background

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. These attacks 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. The Chief of Naval Operations Navigation Plan 2021 states that China and Russia "have strengthened all dimensions of their military power to challenge us and our allies and partners from the seabed to space and in the information domain" (p. 2). To counter this challenge, the Navigation Plan says, "we have to do more than simply employ new capabilities—we must compete in new ways" (p. 4). The Navy's Education for Seapower Strategy 2020 addresses these "new ways" by promoting learning as a strategic advantage—we must provide "naval forces with an intellectual overmatch against our adversaries" (p. 3).

The project combined a mixed approached methodology of collecting and analyzing both qualitative and quantitative data. We also focused on a systematic exploration of each dimension of hybrid

threats, assessing how they can complement each other, and how to counter these threats. The research analyzed most pertinent hybrid threats to the Department of the Navy looked at current capabilities and gaps, what approaches and means should DoN consider for combating hybrid threats effectively, as well as what methods could be incorporated into training and education curricula across the services. This research project examined past and emerging hybrid threats, challenges, strengths, and opportunities for capability improvement across maritime, cyber, Operations in the Information Environment (OIE), and Special Operations Forces (SOF) domains. First, the research team conducted comprehensive literature review and open-source intelligence analysis of interdisciplinary historical examples, case studies, as well as examination of kinetic and non-kinetic actions exercised by adversarial powers in recent years. Then, we assessed emerging hybrid threats challenges and counter-threat opportunities through examination of adversarial doctrine, strategies, policy, current tactics and operations as well as future threats in respective chapter domains (OIE, cyber, maritime, SOF). Finally, the team provided key findings and recommendations for future research.

Findings and Conclusions

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 Russian 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 the allied 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.

Recommendations for Further Research

As the current Russia-Ukraine war continues to pose severe implications to global security, future research needs to be conducted to analyze and compare Russia's use of hybrid threats ahead of and during its war in Ukraine. As Russia continues its war, it will likely seek retribution for massive military aid to Ukraine, so our nation and allies may come under increased hybrid conflict by states and non-state actors who employ non-attributable actions below the threshold of war. Through such actions, Russia seeks to weaken our competitive advantage across all domains, exploit our vulnerabilities, and undermine the cohesiveness within our nation, as well as our alliances and partnerships.

In addition to analyzing Russia's use of hybrid threats in the current domain of conflict, future studies will assess the U.S. framework to combat hybrid threats in the areas of cyber security, information warfare, special operations, and maritime security. Additional research will be conducted to analyze best practices and lessons learned from the current war in Ukraine and identify key takeaways and findings relevant to U.S. Naval Forces and the Department of Defense.

References

Gilday, M. (2021). *CNO NAVPLAN*. https://media.defense.gov/2021/Jan/11/2002562551/-1/-1/1/CNO%20NAVPLAN%202021%20-%20FINAL.PDF

Modly, T. (2020). Education for Seapower Strategy 2020. *Naval War College Review*, *73*(3), 1–19. https://permanent.fdlp.gov/gpo132978/Naval_Education_Strategy.pdf

Acronyms

DON Department of Navy
OIE Operations in the Information Environment
SOF Special Operations Forces