Office of Information Operations Policy (OIOP)

Fundamentals of Operations in the Information Environment (OIE)

DoD IOCR at the Naval Postgraduate School

Tuesday-Thursday, 23-25 January 2024

Course Description and Schedule

As the United States' National Security Strategy shifts from the Global War on Terror (GWOT) to Strategic Competition and Integrated Deterrence with nation-states, the importance of leveraging and competing against operations in the information environment (OIE) is more salient than ever. As our fighting men and women across all branches adjust to the revolution in military affairs, the need for practitioner education and influence tradecraft is paramount, primarily for the growing influence and power of the People's Republic of China (PRC). The DoD Information Operations Center for Research (IOCR), housed in the Defense Analysis Department at the Naval Postgraduate School, stands ready to support the Office or Information Operations Policy (OIOP) and all other DoD agencies designated to campaign and compete in and with OIE approaches.

Objective

The influence and information centric operation three-day event intends to educate strategic level information tradecraft for strategic competition, with a primary focus on the PRC's growing global influence, as well as the Russian Federation's continued aggression in the information space. We hope to give information professionals and practitioners the critical thinking skills as to why and how U.S. adversaries conduct these operations and encourage independent thought as to how to integrate, conduct, counter and deter information warfare actions and activities to defend and support national security objectives.

Background

As the United States shifts its strategic vision from combatting non-state extremist groups through the global war on terror (GWOT) to strategic competition and integrated deterrence, the need to have a clear, swift, and adaptive information strategy is more important than ever. Gaining and maintaining the information advantage against these rivals presents significant challenges that the United States must address.

Current U.S. national defense strategy contains four defense priorities to be achieved through strategic competition and integrated deterrence:

- Defending the homeland, paced to the growing multi-domain threat posed by the PRC

- Deterring strategic attacks against the United States, its Allies, and partners.

- Deterring aggression, while being prepared to prevail in conflict when necessary – prioritizing the PRC challenge in the Indo-Pacific region, then the Russian challenge in Europe

- Building a resilient Joint Force and defense ecosystem.[1]

The role of information in the integrated deterrence concept is crucial. According to the 2022 NDS, "deterrence depends in part on competitors' understanding of U.S. intent and capabilities. The Department must seek to avoid unknowingly driving competition to aggression. To strengthen deterrence while managing escalation risks, the Department will enhance its ability to operate in the information domain – for example, by working to ensure that messages are conveyed effectively. We will work in collaboration with other U.S. Federal departments and agencies along with Allies and partners." [2]

Joint-Publication 3-04, "Information in Joint Operations", outlines the structure and permissions of operating in the information environment for the DoD, in order to contribute to integrated deterrence against the PRC and Russia. It has designated various forces into a combined concept of conducting information operations and achieving information advantage. Psychological operations forces, civil affairs and public affairs officers, electromagnetic spectrum forces, cyberspace operations forces, and space operations forces all have a role to play in the information environment. How should these tools be utilized in order to puch back against PRC influence?

The DoD Information Operations Center for Research (IOCR) directs and runs the courses and research for the 698 – Information Strategy and Political Warfare - curriculum. Our center is primarily focused on the information strategies of U.S. adversaries, including China, Russia, Iran, North Korea, and various violent extremist groups. Additionally, as required by our charter, we sponsor, direct, and engage in inter-agency collaborations throughout the year as well as produce publications intended to guide national defense strategy. As we are sponsored by ASD-P-SOLIC, most of our committee/workshop memberships are joint as well.

The IOCR is located in the Department of Defense Analysis at the Naval Postgraduate School and is therefore well-positioned to instruct active-duty officers across the force. The 698 curriculum is a 1.5-year Master of Science Degree-seeking program for special operations forces, and already has the personnel and expertise to offer the Joint Force the knowledge it needs in teaching the skills and techniques needed for 21st century strategic competition.

Pre-reads: JP 3-04, National Security Strategy, and the 2023 Strategy for Operations in the Information Environment (SOIE)

Schedule of Events (ALL TIMES EST)

Day 1, Tuesday January 23

0800-0820: Introduction/Schedule overview (Maness, in-person)

0820-0940: Overview of Operations in the Information Environment (Barry, Acosta, Whiskeyman, in-person)
Overview of JP 3-04, National Security Strategy, and the 2023 Strategy for Operations in the Information Environment (SOIE)

0940-1000: Break

1000-1050: Introduction to China's OIE Strategy (McClenon: Virtual)
This block will give an overview of the concepts and organizations involved in Chinese information operations and will situate Chinese OIE strategic thinking in the context of China's national humiliation/national rejuvenation narrative.

1050-1100: Break

1100-1150: Introduction to Russian OIE Strategy (Maness: in-person)
This block will cover an overview of the history and current doctrine of the Russian Federation for the cyber and information environments.

1150-1300: Lunch

1300-1350: Cyber Strategy and Deception (Maness, in-person) Introduction to cyber strategies, such as disruptions, short and long-term espionage, degradations, and deception and how they affect the information environment. How are cyber technologies fundamentally changing the information environment and is the United States prepared?

1350-1400: Break

1400-1450: Media Interpretation (Iatrou: Virtual)
This discussion focuses on the multitude of filters that alter the characteristics of the perceived environment and subsequently our behavior.

1450-1500: Break

1500-1600: S&T aspects of OIE (5G, AI, Satellites/Space) – Emerging technology and the information environment (Volpe, in-person)
A quick introduction to emerging technologies, such as 5G cellular technology, artificial intelligence, space and satellite internet technology will be the topics of this hour; how dual use nature of modern technology shapes competition.

End of Day 1

Day 2 (narrowed audience with more details and discussion)

0800-0900: Russia's Cyber and Information Warfare (Maness: in-person)
Here we will discuss Russia's contemporary approach to propaganda and information warfare, the psychology behind the effectiveness of falsehood-based propaganda, and some options for and approaches to countering disinformation.

0900-0910: Break

0910-1010: China deep dive (McClenon: virtual)
This block will briefly overview common misperceptions about Chinese information operations, and then highlight a few studies that illustrate the importance of cognitive, social, and psychological differences for understanding and defending against Chinese information operations.

1010-1030: Break

1030-1130: Social Network Analysis (Everton: in-person)
This course examines the underlying nature of trust and influence, especially as they shape and are shaped by social networks. Students will acquire a theoretical foundation for these concepts and how they apply to a broad spectrum of activity, including military operations, underground movements, information and intelligence operations, and governance and the media.

1130-1230: Lunch

1230-1330: Social Network Analysis continued (Everton: in-person)

1330-1430: Psychology of OIE (Houck: Virtual)
What are effective influence techniques and how do you defend against them? By discussing the underlying psychology of influence, participants will gain a deeper understanding of the conditions under which information is most likely to persuade individuals, groups, and nations.

1430-1440: Break

1440-1600: EW and Space shallow dive (Iatrou, Volpe: Virtual, in-person)
In this segment we'll discuss the scope of the electromagnetic operational environment; the operational significance and interplay of electromagnetic radiation, weather and terrain; and the challenges to ensuring our use while denying their use of the spectrum.

How is the space domain changing the information environment? How is AI and satellite technology affecting both intelligence and information?

End of Day 2

Day 3 (same audience as day 2)

0800-0940: Planning and Assessments (Acosta, Barry, Whiskeyman, in-person)
How should OIE planning be integrated with other aspects of operational planning? What special considerations does OIE raise for planning? How can different information-related capabilities work in combination, and how do they relate to each other? What challenges relate to intelligence support to OIE? How can OIE be assessed and evaluated?

0940-1000: Break

1000-1100: Narratives and Influence: A Taiwan case study (McClenon)
This brief will highlight a few examples of Chinese information operations against Taiwan and will overview some of Taiwan's governmental and civil society efforts to defend against information operations.

1100-1200: The Future of OIE (Whiskeyman)

1200-1300: Lunch

1300-1600 (with breaks): Guided discussion on relationship between OIE and Integrated Deterrence (interagency cooperation): Maness, Barry, Acosta, Volpe all in person

End of Day 3

Biographies

Ryan C. Maness (Ph.D., University of Illinois, Chicago 2013) is an assistant professor and the academic associate for the curriculum on information strategy and political warfare (698) at the Naval Postgraduate School. He is also the director of the DoD Information Operations Center for Research at NPS. His research includes operations in the information environment, specifically in cyberspace, cyber strategy, and power dynamics and interactions among states in cyberspace.

Julia McClenon is a cultural and behavioral ethnographer (anthropologist) and sociolinguist, with a focus on Asia, China, and specific diaspora in Asia and America. She is an interagency civil servant with experience in both the Department of Defense and the Department of State. She was previously commissioned as a Foreign Service Officer of the U.S. diplomatic corps. For State Department, she was Chair of the Consul General's Civil-Society Working Group on Religion in China.

Sean Everton is a Professor in the Defense Analysis Department and the Co-Director of the CORE (Common Operational Research Environment) Lab at the Naval Postgraduate School (NPS). He specializes in using social network analysis to track and disrupt dark networks (e.g., criminal and terrorist networks), and he has published in the areas of social network analysis, sociology of religion, diffusion, economic sociology, and political sociology.

Tristan Volpe is an assistant professor in the Defense Analysis Department at the Naval Postgraduate School and a nonresident fellow in the Nuclear Policy Program at the Carnegie Endowment for International Peace. He studies how technology shapes coercion, cooperation, and competition among nations.

Shannon Houck is an Assistant Professor in the Defense Analysis Department at the U.S. Naval Postgraduate School (NPS). She is a Social Psychologist with expertise on the science of influence and persuasion, psychological resilience and resistance, and extremism. Prior to joining NPS, she was a faculty member at Syracuse University from 2016-2020. She is the author of over 40 scholarly articles and book chapters, and her research has been featured on popular news outlets such as the New York Times, Psychology Today, and USA Today.

Steven Iatrou is a Senior Lecturer in the Information Sciences Department at the Naval Postgraduate School. His Research Interests include Command and Control, Mass and Social Media, Social Influence, and Naval Communications Technologies. His Teaching Interests include Information Operations, Command and Control, and Information Systems.