Asymmetric Threats in an Era of Great Power Competition
Sponsored by CACI International Inc, The Center for Security Policy, and the Institute for the Study of War
Report 2, January 2020

Information Operations in the Cyber Age

The information space is to policy as terrain is to war. It shapes and channels policy. It represents the collective brain of a society. When it comes to war, this collective brain can influence what to fight for, when to fight, how much to sacrifice, and when to stop fighting. These decisions are determined by politicians and policymakers whose perceptions are shaped by the information available to them, so directing the information flow is an essential aspect of waging war.

Information operations – defined here as the attempt to influence the mindset of an adversary group or population – have been used throughout history to affect the outcomes of war. Today's sophisticated information operations are facilitated by the ubiquity of the Internet and social media, and the resulting changes to the media landscape. Detecting and countering the flow of adversary information has become increasingly challenging. Up until recent times, information operators had to physically penetrate the territory of their target. This was a difficult undertaking that carried a high risk of detection and interception. In the cyber age, physical penetration is no longer necessary, and adversary communications can target almost anyone, anywhere.

> Up until recent times, information operators had to physically penetrate the territory of their target. In the cyber age, physical penetration is no longer necessary, and adversary communications can target almost anyone, anywhere.

The rise of the Internet and social media resulted in the "democratization" of news, which meant the decentralization and proliferation of information sources. With a vast array of media companies and websites competing for clicks, the rush to publish first has sped the news cycle to a dizzying pace. News organizations – even respected ones – have little time to properly vet the veracity of news stories and the credibility of their sources. Compounding this challenge is the problem of technical anonymity. News outlets regularly receive unsolicited information from anonymous sources. In the past, journalists and news organizations that received anonymous information knew the giver's identity and protected it. Now that "news tips" are electronic, the identity of sources is much more difficult to verify, enabling adversaries to inject information into the discourse. Fake media outlets are set up to give the appearance that the "news" is coming from multiple sources and is therefore more trustworthy. Adversary narratives then enter into the general information space, exerting influence and shaping perception and ultimately policy.

Defending against information operations is more difficult than ever; however, the relative ease of executing operations in the cyber age is countered by the risk of detection. When that occurs, the blowback it causes can nullify any effects and even worsen the initial situation. For example, the uncovering of Russian information operations in the Ukraine and U.S. led to a public outcry and the heightened perception that Russia is an untrustworthy adversary, undermining Russia's objectives.

As the U.S. focuses on recognizing and defending against information operations that are run against us, government agencies need to think through and plan the best reaction when adversary operations are detected. When and why should the adversary's cover be blown? What objectives would it achieve? What sort of counter information campaign should take place? Since the U.S. is the target of information operations by multiple countries, it is essential that our response and mitigation be skillfully planned.

NOTE: This report is from the presentation of Dr. Frederick W. Kagan, director of the [Critical Threats Project] at the American Enterprise Institute.