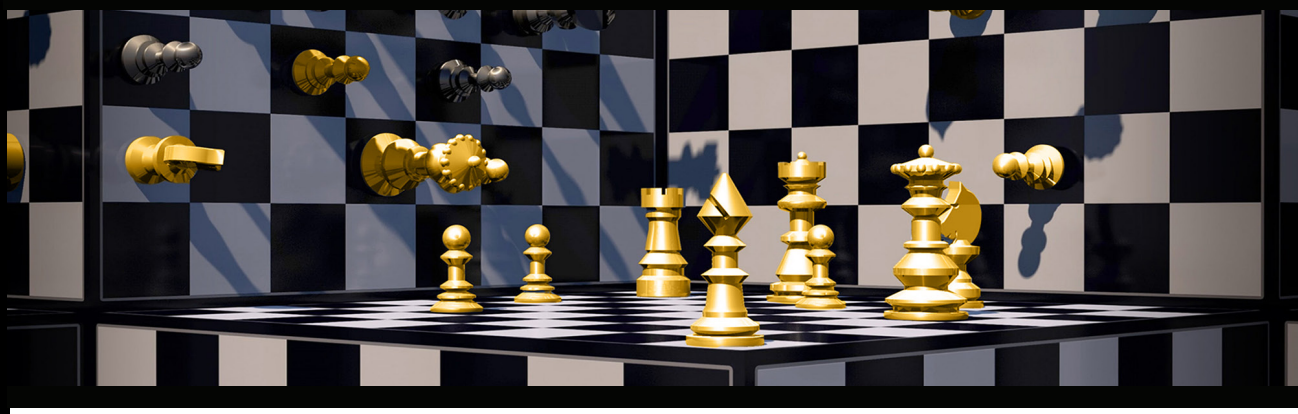

25 September 2023

PERSPECTIVES

Influenced by Disinformation: What the U.S. Can Do to Counter Disinformation Operations

Del Sanders and Peter Roberto

In February and March of 2022, as Russian troops crossed into Ukraine, Russian misinformation concurrently crossed over social media platforms to support them. Russia attempted to promote the idea that Ukraine housed bioweapons plants for the U.S. While the idea was swiftly debunked, it gained traction amongst conspiracy theorists in the U.S. The prevalence of these conspiracy theories in public debate eroded the public's faith in U.S. institutions, capitalizing on disunity amongst Americans, lack of government efficiency, and lack of institutional transparency. The ability to influence a myriad of population sectors worldwide is the "go-to" tool of 21st century warfare for U.S. competitors. The U.S. must recognize that refilling stockpiles, maintaining nearly 800 bases in 70 countries, and reorganizing the Navy's carrier posture is not enough to compete in 21st century warfare. Irregular warfare strategies replaced the overt wars of the 20th century. Although the U.S. outspends any country in defense expenditure, increased global connections evened the playing field, enabling irregular warfare operations, especially disinformation campaigns, that cause as much or more damage than a HIMARS barrage. The U.S. must engage Russia, and eventually China, in the information realm, which it all too often confronts from a cyber defense context and not offensive cyber or influencing sentiment. With new tools like "deep fakes" becoming increasingly common on social media, the U.S. must reorganize its efforts to protect and actively cultivate its reputation and control its influence against its competitors. This article outlines three ways to enable the U.S. to effectively compete against adversaries in the information wars.

Russia is a prominent player in the information domain and China is an active learner, both taking advantage of the U.S.'s lack of preparation in the field. Russia has implemented disinformation campaigns since the Cold War, and these activities were revived amidst the various Russian incursions into Ukraine. Russia uses different online groups to implement its recent campaign of lies, including hacktivist groups and the aptly named "Internet Research Agency" formerly owned by notorious Wagner Group founder Yevgeny Prigozhin. In addition, China launched numerous disinformation campaigns against the U.S. and its allies via the People's Liberation Army. These groups take advantage of the U.S.'s hesitancy to engage strongly in the information operations realm and its common doctrine of viewing cyberwarfare in defensive terms, focusing on denial-of-service attacks. U.S. adversaries also exploit

its declining international reputation to expand their influence abroad. To account for the evolving media and technological landscape, the U.S. needs a counter-disinformation strategy that reflects its contemporary position on the world stage, while also reminding the world of our positive values and past achievements.

In irregular warfare the U.S. focus is currently, at best, limited to military information support operations (MISO) regarding the information domain. The U.S. government spends too much energy into the oft-overused tactic of utilizing MISO in a specific locality to maintain or increase positive U.S. sentiment. A way forward in the irregular warfare space is to counter disinformation instead. We can expand beyond the MISO focus and pivot to a full spectrum look in the information domain. The aftermath of the withdrawal from Afghanistan severely diminished the U.S.'s relationship with its partners, which provided an exploitation opportunity for adversaries like Russia. Russia also attacked the U.S. government's internal credibility by promoting various existing conspiracy theories, like QAnon and its international offshoots, within the U.S. A counter-disinformation strategy for the United States must take into account Russia's exploitation of both domestic and international distrust. The U.S. can do so by expanding upon the tools that it has in its arsenal, using a culturally informed and nuanced approach to messaging, and accounting for the cultural divisions in the U.S. within our international narrative.

First, the U.S. and its allies must learn how to weaponize transparency. In the days leading up to Russia's invasion of Ukraine, U.S. officials, armed with intelligence on Russian troop movements, began to warn Ukraine and its allies in NATO, the EU, and across the world about the impending attack. As a result, Ukraine saw an outpouring of support from the international community, one that saw even a rising adversary like China abstaining on UN votes. In addition, the warnings also likely bolstered U.S. support for Ukraine. The United States must learn from this declassification campaign and create a concise and factually accurate strategic messaging campaign against Russian disinformation, including Russia's promotion of conspiracy theories and divides within the United States. This approach allows the U.S. to counter Russian disinformation operations in a way that preserves the democratic spirit of the U.S.

Second, the United States must look at the information, social media, AI, and machine learning space as an opportunity, not an uncharted domain to abstain from out of fear or skepticism. Other states, such as Russia, exploit these tools offensively. Many in the U.S. security sphere are not technologically proficient regarding social media or AI and view these mediums with disdain or skepticism. Instead, we should increase our training and focus on these tools just as much as our adversaries. Additionally, the whole of the U.S. government must become serious about exploiting the information domain and stop viewing every non-military threat through the myopic lens of a cyber attack. The information domain is wildly complex and rapidly evolving, and the United States must facilitate interoperability and communication between the various entities involved in information operations, both offensively and defensively.

Third, the U.S. can further bolster these efforts by having its various special operations forces, who already specialize in information operations, build upon their capabilities. One way is by partnering with private sector partners to identify cultural trends and potential local partners to spread counter disinformation operations. By using tech that utilizes statistical and algorithmic models concerning regression, causality, and natural language processing, Washington can be better empowered to identify influential topics and actors in networks to deal with disinformation accurately. This would amplify U.S. counter disinformation efforts, but when accompanied with special operations deployments, proven statistical solutions can be a force multiplier and allow for greater mission success when they conduct strategic messaging. Furthermore, the U.S. can use the junction of sentiment analysis programs and special operations-enacted strategic messaging campaigns offensively to counter Russian and Chinese influence amongst partner or emerging states. Partners like Ukraine see vast success with this strategy and could offer a path for U.S. policymakers to learn how to navigate the modern media landscape.

The U.S. can forge a new path in combating the waves of online disinformation coming from Russia and other near-peer competitors. Washington must learn to develop new strategies to change the narrative and promote

its interests in an evolving media landscape filled with emerging technologies and irregular warfare doctrines that enable resurgent powers. The days when the might of militaries alone made right are long gone. The ability to influence mass amounts of people is now proving just as influential as a NATO defense commitment, and the United States must treat the information space with the same respect.

About the Authors:

Del Sanders is a M.S. candidate at Seton Hall University's School of Diplomacy and International Relations. Del is a former U.S. Army Intelligence Analyst with 16 years' experience working in Special Operations, a member of the National Security Fellowship graduate program at Seton Hall University, providing research and policy recommendations to the Department of Defense this past academic year, an Associate Editor with the Journal of Diplomacy & International Relations, and currently is a manager at FNA, a learning software company within the national security sector.

Peter Roberto, M.A. is the former Editor-in-Chief of the Journal of Diplomacy & International Relations at Seton Hall University's School of Diplomacy and International Relations. He was a member of the National Security Fellowship graduate program at Seton Hall University, and provided research and policy recommendations to the State Department and Department of Defense. He held internships with The Counterterrorism Group and the U.S. House of Representatives. Peter has been published by the Journal of Diplomacy & International Relations, Foreign Policy Association, HSToday, and Small Wars Journal.

The views expressed are those of the author(s) and do not necessarily reflect the official position of the Department of Defense, Defense Security Cooperation Agency, or the Center for Irregular Warfare.