STATEMENT OF

HONORABLE MICHAEL D. LUMPKIN

VICE PRESIDENT

LEIDOS HEALTH

BEFORE 115TH CONGRESS

HOUSE ARMED SERVICES COMMITTEE

**Introduction**

Chairman Thornberry, Ranking Member Smith, and distinguished members of the Committee, thank you for this opportunity to address you today as a private citizen and in a personal capacity on the topic of "State and Non-State Actor Influence Operations: Recommendation for U.S. National Security". My knowledge on this topic stems from my time as an employee of the U.S. government and I currently do not work in the field of information operations nor have I received, directly or indirectly, any compensation for work in the field since departing government service in January 2017. That said, I trust my experience as a career special operations officer, Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, and Special Envoy and Coordinator for the Global Engagement Center (GEC) at the Department of State will be helpful in providing perspective as Congress assesses the U.S. government's strategy, capabilities and overall effort towards countering state and non-state sponsored propaganda and influence operations.

From my time leading the GEC, I'm familiar with the bicameral interest and bipartisan engagement by Members of Congress on these important issues. First established by Executive Order 13721, the mission of the GEC was expanded by the 2017 National Defense Authorization Act (NDAA) to include counter-state propaganda and disinformation efforts, well beyond its original charter which directed the Center to diminish the influence of terrorist organizations such as the Islamic State of Iraq and Syria (ISIS) in the information domain. This congressional mandate was a big step in the right direction; for the first time a single entity was charged with leading, synchronizing, and coordinating efforts of the Federal Government towards countering foreign state and non-state disinformation efforts.

I believe Congress has correctly identified such information operations as an ongoing and persistent threat to U.S. national security interests. Unfortunately, and based on my previous experience in government, I am similarly convinced that we are still far from where we ultimately need to be in order to successfully protect and defend those national interests in the modern information environment.

I am very pleased to be joined here today by General Phil Breedlove and Mr. John Garnaut. I believe we are collectively postured to address your questions on the issue at hand.

**The Current Situation**

Since the end of the Cold War with the Soviet Union, which arguably was the last period in history when the U.S. successfully engaged in sustained information warfare and counter-state propaganda efforts, advances in technology have enabled instantaneous global communications; we are living in a hyper-connected world where the flow of information moves across borders in real time and across traditional and social media platforms. The lines

of authority and effort between public diplomacy, public affairs, and information warfare have blurred to the point where in many cases information is consumed by U.S. and foreign audiences at the same time via the same methods.

While the means and methods of communication have transformed dramatically, most of the laws and policies governing how the U.S. government responds to sophisticated information operations and disinformation campaigns by foreign adversaries have remained unchanged. It is true that there has been some tinkering and tweaking, but nothing substantive or transformational. Put simply, our institutions have not kept pace with the evolving threats.

**Lack of Accountability and Oversight**

Antiquated bureaucratic structures and traditional lines of authority remain a significant impediment to progress. To date, there is not a single individual in the U.S. government below the President of the United States who is responsible for managing U.S. information dissemination and providing strategic guidance for how to confront our adversaries in the information environment. While the 2017 NDAA mandated that GEC lead, organize, and synchronize U.S. government counter-propaganda and disinformation efforts against state and non-state actors abroad, it failed to elevate the head of the GEC to a position of authority commensurate with its expansive mission. The GEC operates at the Assistant Secretary level and lacks the necessary authority to direct the Interagency. In practice, this means that the GEC is considered at best a peer to a half dozen regional or functional bureaus at the State Department and numerous disparate organizations at the Defense Department, to say nothing of the other departments and agencies that have an important stake in this fight. Simply put, although the GEC is directed by law with the mission to lead the Interagency, the practical reality is that its role is reduced to simply a "suggesting" function which agencies can choose to follow or not follow as they see fit. The result is a significant misalignment of responsibility, authority, and accountability which will without doubt continue to hamper efforts until and unless corrected by statute.

To correct this imbalance, I believe that elevating the GEC and it role of leading, coordinating, and synchronizing U.S. government efforts in the information environment to something similar to what the Office of National Intelligence does for the intelligence community would bring the appropriate alignment of responsibility, authority, and accountability while minimizing significant bureaucratic tension and cost.

Such an elevation in stature would enable the GEC to advocate for resourcing levels for the Interagency as well as drive a single information strategy and bring discipline to the whole of government efforts. I know firsthand that many talented people in government are working

these issues thoughtfully and diligently; unfortunately, they are not always working in unison because they are answering to different leaders with different priorities.

**The Limitations of Truth and Bureaucracy**

It is not unreasonable to think that the U.S. will always be at some disadvantage against our adversaries in the information environment. We are a nation of laws where truth and ethics are expected, and rightly so. Our enemies, on the contrary, are not constrained by ethics, the truth, or even the law. Our adversaries, both state and non-state actors, can and will continue to bombard all forms of communication with their messages in attempts to influence public perception, create doubt of our actions or intentions, and recruit people to their cause. We must ensure that we organize U.S. government efforts in such a manner that maximize desired outcomes through discipline, agility, and innovation.

When using the terms agility and innovation, the U.S. government is generally not the first thing to come to mind. This is especially true in the information environment as anyone who has served in government can attest. For example, it remains difficult to introduce new social media analytic tools and forensic tools onto government IT systems because of lengthy and highly complicated compliance processes. Although these tools are crucial to understanding the social media landscape and are required to ensure the U.S. efforts are hitting the right audience with the right message at the right time, we are often hampered by bureaucratic hurdles and outdated systems. Analytic tools are advancing as fast as the information environment itself and any lag in implementation can have a devastating effect.

To be clear, these tools cost money and it takes significant resources to train on these ever-advancing capabilities. While budgets for U.S. government information warfare and counter-propaganda efforts have increased significantly in recent years, they still pale in comparison to the resources applied to kinetic efforts. As single kinetic strike against a high value terrorist can tally into the hundreds of millions of dollars when conducted outside the area of active armed hostilities (when adding intelligence efforts before or after the strike) and in many cases, only have short term affects. While many obstacles can be overcome by new authorities and clarification on lines of authority, we must be clear that, simply put, more investment is also required.

Even when fully resourced and masterfully executed, information warfare and counter-propaganda efforts contain a high element of risk. While bureaucracy in government is necessary to standardize routine tasks, it cannot be left to control the totality of our efforts in the information environment. The bureaucratic standard operating procedure strives to reduce risk to almost zero which, while appropriate in certain circumstances, is not effective in the information space. A failure to accept a reasonable degree of risk can ultimately lead to diluted messaging efforts and result in missing the correct audience with an effective message that shifts their thought and/or behavior to our desired end state. To be successful in this fight we

must learn to accept a higher level of risk and accept the fact that sometimes we are just going to get it wrong despite our best efforts. When we do get it wrong, we must learn, adapt, and iterate our message rapidly to be relevant and effective.

**In Conclusion**

I applaud Congress as whole, and especially the Armed Services Committees of both chambers, for its leadership in seeking to address the urgent threats of disinformation and propaganda campaigns from state and non-state actors. Indeed, Congress has driven the Executive Branch to make real progress. That said, much more still needs to be done in order to even catch up with our adversaries, let alone effectively compete against them.