Fifth PSSI Space Security Conference
Evolution of the Counterspace Threat and Strengthening of International Space Partnerships

Panel 2, "Space Domain Awareness and Hybrid Operations"
Panel Remarks by Dr. Dana J. Johnson, Director, International Outreach and Policy
Office of the Under Secretary of Defense for Research and Engineering
Prague, Czech Republic, June 10, 2019
(5-8 minutes for remarks, followed by Q&A)

Panel 2: Space Domain Awareness and Hybrid Operations *[from conference agenda]*

Theme: The introduction of Offensive Cyber and Counterspace operations into the arena of international conflict has led to situations where activities short of military action are more easily employed by malign actors to accomplish strategic goals without the fear of clear attribution. To an ever-expanding degree, these tools are being used in combination with more traditional forms of non-military activities to coerce behavior that would have previously required more overt aggression. The difference here is in the ability to use non-kinetic cyber and other 'grey zone' actions. Given these realities, what role does space domain awareness activities play in this dynamic, and what new or enhanced capabilities are required to deter or respond to this type of space-related hybrid warfare?

Thank you for your kind introduction, Mr. [Doug] Loverro. I'd also like to thank the Prague Security Studies Institute for inviting me to participate in the Fifth PSSI Space Security Conference. This is my first time back in beautiful Prague since the first PSSI conference in this series in 2011, my second time participating in this conference since 2013, and I am looking forward to our conversations.

Hybrid operations has certainly been at the forefront of recent NATO and European Union (EU) defense deliberations over the past few years and across a broad spectrum of activities, from strategic communications to energy supply and energy infrastructure, to economic and financial infrastructure protection, as well as public health and food security, chemical, biological, radiological, and nuclear-related risks. Protection of space infrastructure (both ground- and space segments) and employment of space-enabled services and applications as instruments to counter hybrid threats, are also included. In many ways these deliberations in Europe mirror many of the resilience, mission assurance, and protection discussions conducted in the U.S. national security community over the past decade or more.

The EU has defined "hybrid threats" as those that

> "combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives. Hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics. They are

> designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create confusion to hinder swift and effective decision-making."[1]

The Prague Security Studies Institute has taken this definition one step further by providing a definition of "space hybrid operations" as intentional, temporary, mostly reversible, and often harmful space actions/activities specifically designed to exploit the links to other domains and conducted just below the threshold of requiring meaningful military or political retaliatory responses."[2] They offer some examples of space hybrid operations, such as:

- Directed energy operations that may result in space debris;
- Orbital operations that generally do not result in space debris, such as rendezvous and proximity operations (RPO);
- Electronic operations such as uplink or terrestrial/downlink jamming;
- Cyber operations, such as attacks on links or user terminals; and
- Economic and financial (E&F) operations, such as investments in segments or key companies of another country's space infrastructure for purposes of influence and control.[3]

Some of these activities are reversible while others are not; some of them are clearly attributable to a bad actor while others may be less transparent. At times we may choose to call out those bad actors in multilateral and bilateral diplomatic fora such as the Conference on Disarmament, while encouraging the international community to pursue voluntary norms of responsible behavior and "best practices" of spaceflight safety in such venues as the United Nations Committee on the Peaceful Uses of Outer Space.

There is another dimension to hybrid operations – the underlying technology areas that provide the foundation for the development of military and other capabilities to counter hybrid threats. The U.S. Director of National Intelligence noted in this year's *Worldwide Threat Assessment of the US Intelligence Community*[4] that:

> "For 2019 and beyond, the innovations that drive military and economic competitiveness will increasingly originate outside the United States, as the overall US lead in science and technology (S&T) shrinks; the capability gap between commercial and military technologies evaporates; and foreign actors increase their efforts to acquire top talent, companies, data, and intellectual property via licit and illicit means."

From the perspective of the U.S. the Department of Defense's Office of the Under Secretary of Defense for Research and Engineering (OUSD[R&E]), headed by Dr. Mike Griffin, this assessment is of direct concern. R&E was established to set the technical direction for the Department of Defense, champion and pursue new capabilities, concepts, and prototyping

---

[1]European Union, *A Europe That Protects: Countering Hybrid Threats*, Factsheet, June 2018.
[2]Jana Robinson, et. al., *Europe's Preparedness to Respond to Space Hybrid Operations*, Prague Security Studies Institute, July 2018.
[3]PSSI, *Space Hybrid Operations: Fact Sheet*, July 2018.
[4]Daniel R. Coats, Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, 29 January 2019.

activities throughout the DoD research and development enterprise, and, most importantly, accelerate capabilities to the warfighter. To accomplish this, R&E is addressing the erosion of U.S. technological superiority by identifying and investing in innovative technologies and processes to sustain and advance the American military. In addition to space, these priorities include hypersonics, artificial intelligence, microelectronics, directed energy, cyber, comprehensive missile defenses, and other areas.

As we all know, military operations across all domains are dependent on timely and assured space effects. Many of the technologies that the United States led in the past, such as microelectronics, are now available to more actors with lower barriers of entry and at an accelerating rate of speed. The space capabilities and advancements made by potential adversaries of the United States and its allies and space partners require us to move quickly to a more dependable and resilient space posture. In addressing this challenge, the DoD seeks to protect legacy space capabilities while shifting to a commercial space paradigm of proliferated and distributed sensors and networks across multiple functional areas such as missile warning, intelligence, surveillance, and reconnaissance (ISR), communications, and potential space-based alternatives to the Global Positioning System (GPS).

DoD's pursuit of space technologies, capabilities, concepts, and prototyping activities are in step with presidential and national level guidance from the National Space Council and the National Security Council; the National Space Strategy, National Security Strategy, and National Defense Strategy; organizational changes as reflected in the establishment of the United States Space Command and the Space Development Agency; and important budgetary investments in technologies and programs. Key to executing this guidance is our international engagement: as stated in the National Defense Strategy, our allies and partners provide complementary capabilities and forces along with unique perspectives, regional relationships, and information that improve our understanding of the environment and expand our options. Science and technology cooperation with allies and partners are an essential, and indeed, foundational, part of strengthening our alliances and attracting new partners, and ultimately deterring and defeating hybrid attacks.

Thank you for your attention.