YOUNG LEADERS PROGRAM

COMMERCIAL CONUNDRUM? POTENTIAL IMPLICATIONS OF USING COMMERCIAL SPACE FOR U.S. NATIONAL SECURITY

BY EVAN WRIGHT

Evan Wright *is a research assistant for the Indo-Pacific Security Program at the Center for a New American Security. He is a nonresident fellow at the Johns Hopkins SAIS Reischauer Center for East Asian Studies, a consultant with the Institute for Defense Analyses, and a Pacific Forum Young Leader.*

Lt. Gen. John Thompson, commander of U.S. Space Force's Space and Missile Systems Center, and Elon Musk, CEO of SpaceX, speaks at the Air Force Association's Air Warfare Symposium in Orlando, Fla., Feb. 28, 2020. Photo by Mike Tsukamoto, Air Force Magazine.

On October 16-17, the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory hosted its 5th annual "Space and U.S. Defense Policy" workshop. The workshop focused on strategic deterrence and how the U.S. can better integrate the space domain into its overarching defense strategy. The private space industry was a frequent topic of discussion, as the U.S. Government may leverage commercial capabilities in its efforts to deter its adversaries, particularly China. This article serves to build upon those discussions by exploring the potential consequences of using commercial providers within the U.S. national security space architecture.

Commercial space companies offer a range of services that may be valuable to the U.S. defense and intelligence community including launch, remote sensing, communications, and satellite servicing. A growing number of companies are entering contracts with the U.S. government to provide such services. For instance, the U.S. remote sensing company Planet announced contracts in 2023 with NASA, the National Reconnaissance Office, and most recently an unnamed Asian government's Ministry of Foreign Affairs. From an American perspective, this is a successful instance of integrated deterrence, utilizing all tools of national power – including cutting-edge commercial technologies – and working with allies and partners to deter aggression. But it also raises questions about the consequences of further integrating commercial space assets into U.S. national security.

This article highlights the need for a national conversation on the implications and challenges the U.S. government and commercial sector may face when using commercial assets for national security. It does so by presenting two questions for commercial stakeholders, defense planners, and policymakers to consider as commercial assets are integrated into U.S. national security space architectures.

How (If at All) Will the U.S. Government Protect Commercial Space Assets?

The Department of Defense's (DoD) obligation to protect commercial space assets is ambiguous at best. The 2020 Defense Space Strategy states that the "DoD will be prepared to protect and defend U.S. and, as directed, allied, partner, and commercial space capabilities and to deter and defeat adversary hostile use of space" as part of maintaining space superiority. The conditionality implied by "as directed" should not be understated. More recently, however, the National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), and U.S. Space Command (SPACECOM) began developing the

Commercial Space Protection Tri-Seal Strategic Framework to share threat information with commercial satellite operators contracting with the NRO "to help ensure effective joint collaboration and cooperation from the minute an event happens." This framework indicates an interest – at least in the intelligence community – to protect commercial assets deemed vital to national security interests; or, at least to help commercial providers protect themselves.

Statements by senior U.S. military leadership may also provide some clues on the DoD's stance on protecting commercial assets. In 2023, the leader of SPACECOM stated that the Secretary of Defense and the President would have to direct SPACECOM to protect and defend commercial assets on orbit. However, the Space Force Chief General recently pointed to the maritime domain as a model, stating that he has "no reason to believe" that the protection of commercial space assets would be different than those at sea.

In other words, the DoD will not automatically defend commercial assets without an order from senior leadership; but there is reason to believe they have an interest in doing so.

Resources and geography are two additional limiting factors to consider. SPACECOM is notably a geographic combatant command and not a functional command, meaning it is responsible for the entire astrographic area 62 miles above sea-level. As such, every single U.S. commercial asset on orbit, including the nearly 5,000 satellites SpaceX has launched since 2019, are under SPACECOM's jurisdiction if the government intends to defend all privately-owned space assets. The DoD may decide they only have a responsibility to protect private assets deemed vital to the U.S. government, however, there is no guarantee they will protect all commercial assets.

U.S. policymakers and defense planners should think carefully about which commercial assets should fall under DoD's protection and what the implications may be for commercial companies to provide services for both U.S. civil and military missions. For example, the Sierra Nevada Corporation is expected to bring payloads and passengers to the International Space Station starting in late 2023 using their private spacecraft, the Dream Chaser. Sierra Nevada is also in conversation with the U.S. Transportation Command to use Dream Chaser for military purposes. The company has also provided intelligence, surveillance, and reconnaissance (ISR) technologies for years to the U.S. and foreign governments for maritime security operations. What are the implications of hiring the same provider to send U.S. astronauts *and* military payloads or personnel? Should these companies' foreign sales be a concern? How those red lines are negotiated is crucial, as they will likely affect the industry's future actions, the private sector's risk-sharing calculus, as well as adversary's identification of "legitimate" military targets in wartime.

What Are the Limitations of Using the Private Sector for National Security Missions?

Foreign financial interests are one reason to fear using commercial services for national security. Elon Musk and Jeff Bezos, the owners of SpaceX and Blue Origin, have strong financial interests in China that could encourage their respective space companies to remain neutral or limit services for the U.S. and its partners in a conflict with China. For Musk, China accounted for half of Tesla's vehicle sales and a fifth of its production capacity in 2021. Bezos too has an interest in the Chinese consumer market through Amazon and has already taken steps to appease the CCP by removing customer ratings and reviews on the Chinese-language Amazon site.

Export control laws also limit what national security missions private corporations can undertake. In Ukraine, Musk denied a request by the Ukrainian military to enable Starlink for a drone sub attack on Russian warships near the coast of Crimea outside of Starlink's geofenced area of operations within Ukraine. "If I had agreed to their request, then SpaceX would be explicitly complicit in a major act of war and conflict escalation," Musk stated. SpaceX has also prevented the use of Starlink for long-range strikes and drone control, as such "weaponization" of the communications technology goes against the product's terms of service in compliance with the

International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR).

Policymakers and defense planners should learn from these examples that commercial interests, and commercial industry's ability to operate in particular environments, may not always align with the U.S. government. Ultimately, commercial space companies have a fiduciary responsibility to their shareholders and investors and may, justifiably, avoid missions that could threaten their privately-owned assets or impact their customer base.

Government and industry stakeholders should deepen discussions to create shared expectations of the role commercial services will play in U.S. national security, including during a conflict in space. The Space Force is working on a commercial space strategy as well as a Commercial Augmentation Space Reserve that will help the U.S. government use commercial satellite communications and remote sensing capabilities during crises. However, it would be helpful if commercial companies, particularly startups lacking strong connections to the U.S. government, had an established forum to share their perspectives with the Department of Defense. In civil space, the National Academies already hosts a Space Technology Industry-Government-University Roundtable (STIGUR). Similarly, the Federal Aviation Administration has a Commercial Space Transportation Advisory Committee (COMSTAC) that advises and provides recommendations to the agency. The national security community should consider establishing a national security-focused forum for commercial operators to further develop shared expectations for the role of commercial entities in U.S. defense policy.

Takeaways

Integrating commercial services into the U.S. national security architecture will require ongoing conversations. Government and industry stakeholders should work together to think through the implications of their ongoing and evolving partnerships. An ambiguous stance by SPACECOM on protecting and defending U.S. commercial assets will impact the risk calculus and future actions of commercial providers. Decision-makers should think carefully about what national security missions should be replaced or supplemented by commercial capabilities and under what conditions the U.S. will protect those commercial assets. Likewise, defense planners and policymakers should keep in mind that commercial companies' interests and obligations may not always align with government interests, which will necessitate frequent industry-government dialogues.

Disclaimer: All opinions in this article are solely those of the author and do not represent any organization.