BACK TO COMMERCIAL SPACE

View Edit Delete Revisions Clone

Opinion: Why Government Needs Trusted Industry Partners For Satcom

Rebecca Cowen-Hirsch April 27, 2020

Credit: U.S. Defense Department

If you envision the information assurance of satellite communications (satcom) as a Venn diagram, then cybersecurity for information technology systems would represent one circle, and satellite security would represent the other. The intersection of these circles would depict a point in which we apply a threat-based, risk-management approach to both, so that we protect satcom as a critical node on the entire network, incorporating required resiliency and response capabilities.

Space is vital to national security and requires a common response: resilience, speed and agility delivered as end-to-end capabilities. Furthermore, it necessitates deploying a defense-in-depth approach that views each satellite (and the network to which it connects) as a critical node on the network. Elected officials in the U.S. and leaders at the Pentagon are calling for fewer government stovepipes and more industry collaboration to build an integrated architecture that leverages commercial satcom as a foundation to effectively meet the requirements for protected military satellite communications (milsatcom).

Given the unique, global demands on the military, users require assured access. “Assured” means in part that there is no doubt about obtaining global availability, maximum capability or optimal flexibility at any time. These attributes are readily supported by trusted commercial providers and, when integrated into a unified satcom architecture, can greatly increase the security and operational efficacy of the critical infrastructure employed globally for mobile national security communications.

The intersection of space and cyberspace matters more than ever. Through industry's ongoing partnership and collaboration with government leaders, which encompasses balanced risk-sharing and mutual investments, trusted commercial satcom owner-operators can innovate to complement milsatcom with enhanced protection and greater interference mitigation capabilities.

The resulting end-to-end, defense-in-depth model distinguishes these companies from those that simply provide commodity satcom bandwidth without the requisite investment in the core components within the intersection between space and cyberspace. Inmarsat, for example, is taking what works in terrestrial cybersecurity and elevating it to the space domain to protect the entirety of a satcom network that supports critical infrastructure users around the world. We are doing so because we recognize that the space environment is far from benign.

It is essential that the commercial industry support a wide range of sectors in addition to the government, with each having unique requirements and security solutions. Companies must ensure the protection of internal and customer data by making cybersecurity a top priority, for their own network efficacy as well as economic viability.

With this, they deliver cyber-resilient digital services and mission-critical communications to global customers by:

•Embedding threat-based risk management into the development and deployment of satellite systems, products and services while sustaining a demonstrable framework for effective, efficient and adaptable responses;

•Delivering operational resilience by proactively identifying, managing and responding to cyberthreats with people, processes and technologies; and

•Fostering a culture in which employees embrace security and are prepared to respond to cyberthreats they may encounter.

As a consequence, commercial satellite communication systems are better positioned to meet globally recognized standards of the Pentagon and other government departments and agencies. Such systems are able to support strong cryptography methods for tracking, telemetry and command. They apply information risk management/security controls in accordance with policies.

Operating models are available today—such as satcom as a service—that address the intersection of space and cyberspace as a key element of the managed services provided. Designed for seamless global mobility and assurance, they provide a critical end-to-end communication infrastructure that is owned and managed by a single, trusted commercial operator. They include the resilient space and robust ground segment elements, as well as type-approved terminals that deliver defense-in-depth capabilities that are an integral part of an integrated architecture to ensure the viability and information assurance of the satcom network in total.

As we operate in an increasingly contested space domain, the commercial industry is demonstrating how we meet the current and future needs of government users. It takes a significant financial investment to be strong, yet this is an investment worth making, as those who depend on satcom for their critical missions deserve our best. We simply cannot afford to put our customers at risk.

—Rebecca Cowen-Hirsch is senior vice president of government and strategy and policy at Inmarsat Government.