

[Advertise](#) [Contact Us](#) [Subscribe](#)**SPACE NEWS**
NEWS YOU CAN USE.**SPACE NEWS.**
NEWS YOU CAN USE.The world's only publication solely
dedicated to covering the space industry

Subscribe > click or call toll-free 866-429-2199

Google Custom Search

Search

[Home](#) [Launch](#) [Contracts](#) [Civil](#) [Military](#) [Satellite Telecom](#) [Earth Observation](#) [Venture Space](#) [Policy](#) [Profiles](#) [Commentaries](#)

Advertisement



SPACE NEWS.
NEWS YOU CAN USE.

The world's only publication solely dedicated to covering the space industry

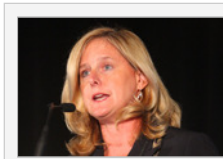
Subscribe >
click or call toll-free
866-429-2199

04/13/10 09:33 PM ET

Government-industry Partnership Targets Cyber-security Threats

By [Debra Werner](#)

COLORADO SPRINGS, Colo. — To address the threat that cyber attacks pose to space- and ground-based telecommunications networks, the commercial firms that make up the National Security Telecommunications Advisory Committee (NSTAC) are testing new mechanisms for sharing information on specific threats.



Kay Sears, president of Intelsat General Corp. Credit: Space News photo by Thomas Kimmell

[Enlarge Image](#)

NSTAC, which includes top executives from network service providers and telecommunications, information technology, aerospace and finance companies, began a pilot program the week of April 12 to create a central repository for information on cyber-security threats in specific sectors. That central repository will acknowledge receipt of information received and maintain a list of liaisons from companies involved, said Kay Sears, president of Intelsat General Corp. of Bethesda, Md., and NSTAC co-chairwoman.

The pilot program is the first step in establishing a government-industry partnership to identify and respond to any activity that threatens communications networks, Sears said April 12 during the National Space Symposium's first full-day session addressing cyber-security issues. "Enhanced space situational awareness will provide a clear and accurate understanding of what is happening in the environment and allow timely and successful decision-making over a broad range of scenarios," she added.

Ultimately, the NSTAC seeks to establish a Joint Coordinating Center to operate around the clock and assist government and industry in preventing, mitigating and responding to cyber-security incidents of national consequence. "The Joint Coordinating Center will be an authoritative venue for operational coordination between government representatives and private-sector owners and operators of critical infrastructure and key resources across all sectors," Sears said.

This effort underscores the growing concern among government and industry officials that space-based communication networks are becoming increasingly vulnerable to attack from adversaries. "Our use of space can be severely limited through intentional and non-intentional jamming, interference and through unauthorized access to our telemetry, tracking and control systems, our teleports, our power systems and denial-of-service interruptions at the data level," Sears said. "The threat picture has really expanded, and cyber is at the foundation."

Moreover, those communication networks underpin critical elements of U.S. financial operations, transportation networks, energy infrastructure and military operations, said Mike McConnell, former director of national intelligence and senior vice president of Booz Allen Hamilton of McLean, Va.

Last year, the U.S. Air Force gave responsibility for addressing threats in cyberspace to Air Force Space Command. In addition, the service established the 24th Air Force at Lackland Air Force Base in Texas to oversee the cyberspace mission. As part of the initial operational capability declared in January, the 24th Air Force commander gained authority over the Air Force network, which means he can determine what hardware and software will be used to improve the network's ability to support ongoing operations as well as to defend against cyber threats, said Gen. Robert Kehler, commander of the Air Force Space Command. Full operational capability will come this fall, he said.

By giving the Air Force Space Command authority over cyber-security issues, the Air Force is recognizing the nexus between the space and cyber-security missions, according to government and industry officials

Advertisement

Receive Our Weekly
Newsletter

A weekly e-newsletter sent out each Friday that
previews the following week's issue of
SPACE NEWS

[DOWNLOADS/](#) [Resource Center](#) >[CALENDAR/](#) [Upcoming Events](#) >[INDUSTRY CONTACTS/](#) [Space Directory](#) >[FOLLOW US/](#) [twitter](#) >

[SUBSCRIBE / SPACE NEWS](#)

COVERING THE UNIVERSE
IS A BIG JOB.



attending the conference. "Space is largely about information flow," said Air Force Lt. Gen. Larry James, commander of the Joint Functional Component Command for Space. "It's making sure the right information gets from the right sensor with the right content to right person at right time."

Cyber-security means keeping that information flowing and protecting the networks that operational commanders rely upon, including communications networks, GPS, missile warning networks and space surveillance networks, James said. In addition, military officials need up-to-date information on the status of their networks, whether they are under attack and how to protect them, he said.

However, that does not mean that the military will be able to defend all communications networks at all times, Kehler said. Instead, the officials will focus on mission assurance by determining which elements are critical to the success of a mission and how those specific elements can be protected, he said.

COMMENTS (0)

You must be logged in to post a comment: [Log In](#) | [Register](#)
[Post a Comment](#)

POST A COMMENT

You must be logged in to post a comment: [Log In](#) | [Register](#)

You are currently not logged in.
You must be logged in to leave a comment.

User Comment Guidelines: It may take up to a minute for your comment to appear. Posting of comments requires membership in the Imaginova Community, which is subject to our [Terms of Service](#). Imaginova reserves the right to remove, without notice, any comment for any reason whatsoever.

[Home](#) [Launch](#) [Contracts](#) [Civil](#) [Military](#) [Satellite Telecom](#) [Earth Observation](#) [Venture Space](#) [Policy](#) [Profiles](#) [Commentaries](#)

IMAGINOVA

SPACE NEWS

ORION

[About Us](#) | [Contact Us](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertise With Us](#) | [DMCA/Copyright](#) | [Subscription Agreement](#) | [Archives: 05,06,07,08,09](#)

© Imaginova Corp. All rights reserved.