Online Journal of Space Communication

Volume 3
Issue 6 *Satellite Security (Winter 2004)*

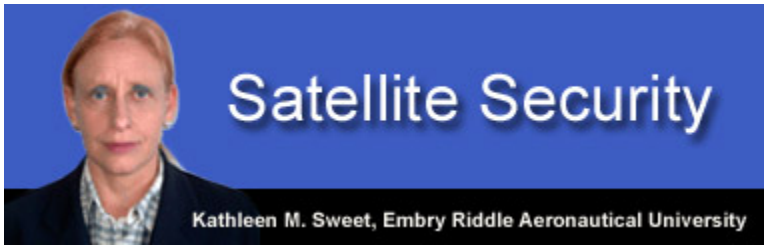
Article 1

June 2021

Issue 6: From the Guest Editor

Kathleen Sweet

Issue 6: From the Guest Editor



Friedrich Nietzsche cautioned "Stare not into the Abyss, lest the Abyss stare back at you." In light of the "war on terrorism" and real threats to national security, the satellite community is faced with few choices but to reorganize and refocus. Problems that for decades plagued the nation's critical infrastructure now haunt the work of scientists and technicians that design, manufacture and implement the equipment supporting satellites. The increased importance of these networked systems has been neglected.

Intelligence on terrorist networks and their interest in destabilizing the economies of the Western world have not been matched by increased understanding of how they might cripple our communication networks. Efforts to enhance intelligence gathering and the government's need to regulate the security of commercial and privately owned assets have raised difficult questions. Balancing the genuine needs of national security and the protection of corporate liberties so rooted in democratic traditions will strain industry resources during the 21st century.

The General Accounting Office (GAO) released a report in October 2002 warning that the nation's commercial satellites have been largely ignored in discussions of critical infrastructure protection and are vulnerable to attack from hackers. Amid heightened concerns about security is the knowledge that space-based communication platforms are also at risk. Terrorists just might divert their current preoccupation with the aviation industry to attempting to bring down our communications networks.

The GAO report entitled "Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed," was completed in August 2002. It found critical vulnerabilities in the nation's commercial satellite network and suggested that federal agencies using commercial satellites may be exposing sensitive data to unauthorized intrusion. The infiltration or destruction of commercial satellites would literally bring the economy of the world to a screeching halt. More than a year has passed and little has been accomplished. Westerners simply take the system for granted. The nation has been riveted by the more publicized threat to aviation.

A previous editor to the Online Journal of Space Communication wrote, "Our 21st Century global economy has its strengths and weaknesses. Positively speaking, we have the technology and know-how to do almost anything. Limitations are

primarily in terms of economics, politics, societal factors, and education." The dangers and realities of terrorism, however, dampen the bright future that technology can offer with the grim prospect of destruction of parts of the system or even worse the whole array.

Despite using encryption to shield communications and physical security to harden ground stations, federal agencies depend on commercial satellite service providers to make available security for tracking, telemetry and control links, satellites and satellite control stations. However, those procedures fall well short of the standards the government uses to secure the military and intelligence satellite network and satellites used in its Global Positioning System.

Federal laws governing satellite system security apply only to satellites used for national security. As a result, government agencies cannot impose specific security requirements on satellite service providers whose equipment is used for other purposes. Sometimes, those commercial entities see issues of security as those that belong on the bottom of the budgetary "to do" list.

The GAO report notes the increased importance of satellite communications to the nation's information infrastructure, and the increasing dependence of the federal government on commercial satellites. Traffic from federal agencies already makes up a significant amount of traffic handled by commercial satellites, and up to 45% of all federal government traffic between the Persian Gulf region and the U.S. is carried over commercial satellite networks. The report recommends expanding the current federal policy governing satellite security to cover commercial satellites used by government agencies.

It also recommends practical ways to better secure commercial satellite communications, such as scrambling telemetry tracking and control communications using cryptography or spread spectrum communications, improving the security of satellites with attack-resistant components, ensuring redundancy in communications networks to guard against the loss of one or more satellites and better securing ground stations. Clearly, the nation's policymakers and industry professionals should take a close look at the findings and consider including commercial satellites as part of the nation's critical infrastructure.

This issue of the Online Journal of Space Communication focuses on matters related to the security of these systems, the laws pertaining to them, the weaponization of space and the potential for infiltration of current systems.

Kathleen Sweet, M.A., J.D., Lt. Col (Ret) USAF
Associate Professor
Department of Security, Intelligence and Globalization
Embry-Riddle Aeronautical University
2300 Willow Creek Road
Prescott, Arizona 86301-3720

Tel: +1 928 445 5173
Email: smsweet@rmsecgroup.com