Highlights from the

NSTAC'S Satellite Task Force

Presented to the

Protection of U.S. space infrastructure,

Space Enterprise Council of the U.S. Chamber of Commerce

and the

Center for Strategic and International Studies (CSIS)

Dr. Allen D. Dayton

15 December 2004

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

What is the NSTAC

The President's National Security Telecommunications Advisory Committee (NSTAC) was created by Executive Order 12382 in 1982

- NSTAC provides critical industry-based advice to the President on matters of **national security and emergency preparedness** (NS/EP) **telecommunications** and **information systems**
- NSTAC is composed of up to 30 chief executives appointed by the President – members include representatives from leading telecommunications, hardware, software and security services, banking, and aerospace companies
- For over 20 years, NSTAC has been a successful model of industry-Government collaboration. NSTAC advice and program support have provided **lasting value and improving response in securing our homeland –**
  - National Coordinating Center for Telecommunications - Information Sharing and Analysis Center (NCC Telecom ISAC)
  - GETS
  - TSP Program

NCS - NSTAC Partnership

The NSTAC forged many partnerships in its 22-year history

Government Interagency

DOS TREAS DOD DOJ DOI USDA

DOC HHS DOT DOE VA DHS

CIA FEMA JS GSA NASA

NRC NTIA NSA USPS FRB FCC

Industry

AMD
AT&T
Bank of America
BellSouth
Boeing
CTIA
CSC
EDS
Lockheed Martin

Lucent Technologies
MCI
Microsoft
Motorola
Nortel Networks
Northrop Grumman
PanAmSat
Qwest
Raytheon

Rockwell Collins
SBC
SAIC
Sprint
Teledesic
Unisys
USTA
VeriSign
Verizon

STF Charge

In January 2003, the Director, National Security Space Architect, requested the NSTAC: "undertake a study on infrastructure protection measures for commercial satellite communications (SATCOM) systems"

In May 2003, the IES established the Satellite Task Force (STF) to:

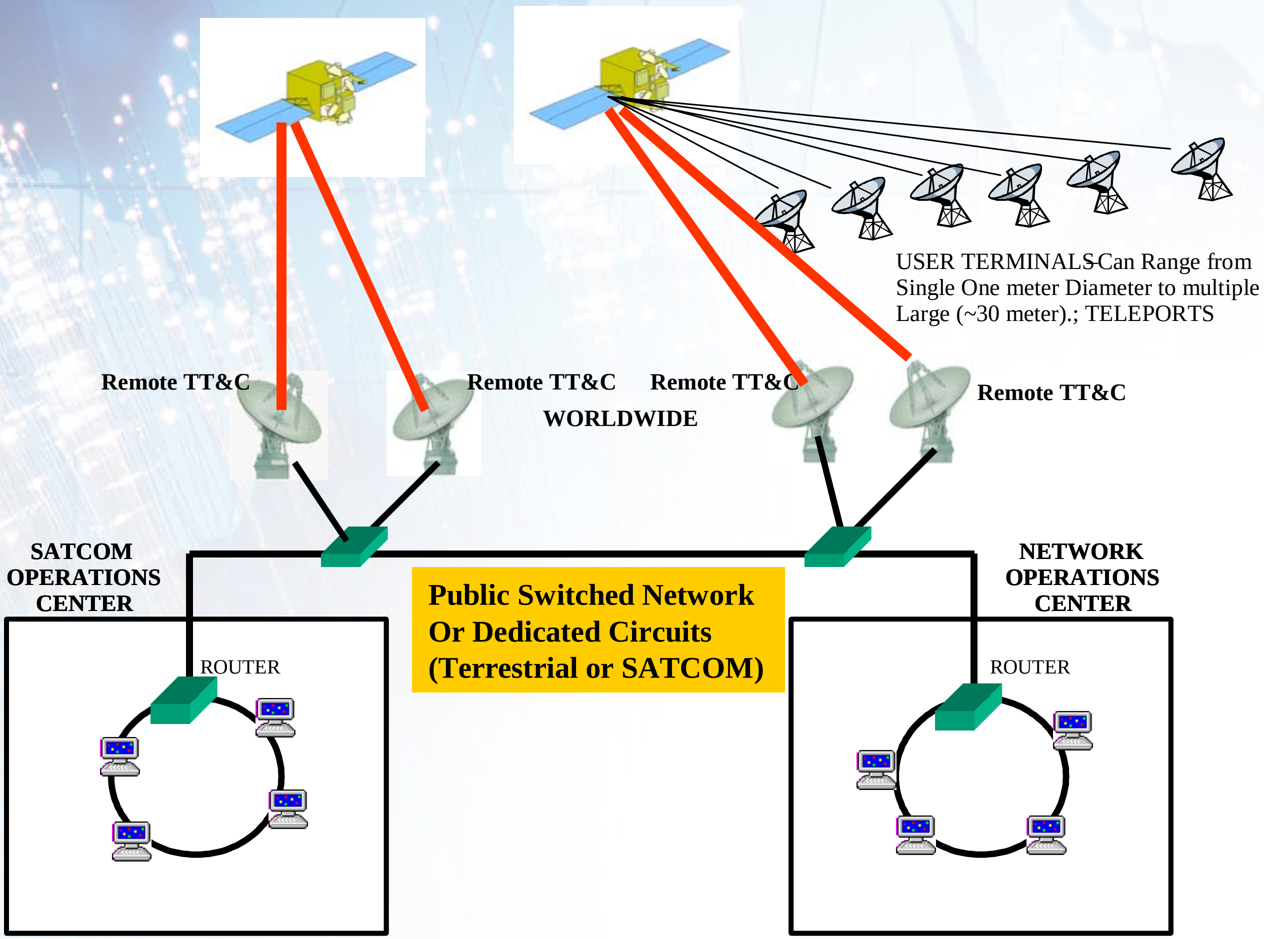
- Assess the vulnerabilities of the commercial satellite infrastructure
- Identify changes to policy to mitigate commercial satellite vulnerabilities
- Coordinate the STF response with representatives from the National Security Council and others
- Report findings and Presidential recommendations

STF Members and Participants

The STF had strong participation from NSTAC member companies, as well as non-NSTAC satellite service providers, a trade association, and Government experts

Task Force Members	Other Industry/Nongovernmental	Government Agencies
Boeing	Hughes Network Systems	Defense Information Systems Agency
Lockheed Martin	The George Washington University	Department of Transportation
Northrop Grumman	Inmarsat	Federal Communications Commission
BellSouth	Intelsat	General Services Administration
MCI	Loral	National Communications System
Motorola	MITRE	National Security Space Architect
Qwest	Mobile Satellite Ventures	Office of Science and Technology Policy
Raytheon	PanAmSat G2 Satellite Solutions	U.S. Strategic Command
Rockwell Collins	Satellite Industry Association (SIA)	
SAIC	SES Americom	
SBC	Spacenet	
	The Aerospace Corporation	
	Verestar	

Generic Communications Satellite System



USER TERMINALS-Can Range from
Single One meter Diameter to multiple
Large (~30 meter).; TELEPORTS

Remote TT&C

Remote TT&C

Remote TT&C

Remote TT&C

WORLDWIDE

SATCOM
OPERATIONS
CENTER

ROUTER

Public Switched Network
Or Dedicated Circuits
(Terrestrial or SATCOM)

NETWORK
OPERATIONS
CENTER

ROUTER

SATELLITE HOUSEKEEPING FUNCTIONS
•Station Keeping
•Fuel Management
•Attitude Control

CUSTOMER SERVICE FUNCTIONS
•Transmission Plans PAYLOAD CONTROL
•Circuit & Network Establishment & Teardown
• Carrier Monitoring & Policing

Components of a Satellite System

- The Task Force’s Vulnerabilities Working Group examined and analyzed the following four components of the satellite system
  - Space Segment
  - Terrestrial Segment
    - NOC, SOC, TT&C sites,
  - Cyber Segment
  - RF Links
- The analysis including applying a panoply of threats using different mechanisms to each of the four components

Analysis and Triage

- Next, approaches to mitigate each of the threats were formulated.
- Then, the cost of each threat and the cost of the mitigation were estimated (with rough granularity)
- A triage approach based on cost was used to identify those mitigations that were “reasonable” to apply.
- As a sanity check, some of the mitigations, such as in the Cyber area, were cross checked with the best practices issued by the NRIC and the MSRC
- Also, reports prepared by previous NSTAC Task Forces, such as the report on “Trusted Access”, were used in developing the recommendations.
- As part of the process, a survey was made of the satellite operators to determine the status of what steps they had already taken to mitigate some of the threats.

STF Findings

The STF Report identified 22 findings on vulnerabilities of the commercial SATCOM infrastructure and implications of commercial satellite use for NS/EP operations

Key task force findings include:

- Satellite services are important for NS/EP telecommunications because of their ubiquity and independence from other communications infrastructures
- Current trends and increased government usage raise the likelihood that the U.S. will experience an attack on its space-based services which could have a detrimental impact
- Components (terrestrial, cyber, RF, & space) of commercial satellite systems are susceptible to both intentional and unintentional threats
- The terrestrial and cyber segments are more vulnerable than the RF links and the satellite itself
- RF links are susceptible to electronic interference threats capable of disrupting or denying satellite communications
- There is a need to improve the industry/Government process to escalate the corrective response to a jamming incident
- Ground stations are susceptible to threats of physical attack and sabotage

STF Findings Continued

More key findings from the STF Report

- Satellite carriers are now using many of the cyber security mitigation techniques recommended by the STF and NRIC
- It is cost prohibitive for the commercial SATCOM industry to protect its spacecraft against direct attacks
- There is a need to improve clear lines of responsibility or coordination within the Federal Government for commercial satellite communications
- Civil agencies need additional in-house technical expertise that can integrate SATCOM into the agencies' communications architectures
- Government/Agency procurement processes need to be improved to allow the Government to compete effectively for commercial SATCOM capacity
- The Government needs to pursue a more proactive information assurance policy
- The current regulatory structure evaluating foreign ownership provides a framework that adequately protects NS/EP interests

NSTAC Recommendations

The NSTAC made three recommendations to the President

1. Develop a national policy with respect to the provisioning and management of commercial SATCOM services integral to NS/EP communications, recognizing the vital and unique capabilities commercial satellites provide for global military operations, diplomatic missions, and homeland security contingency support.

   The Executive Office of the President has begun to incorporate some of these recommendations into an update of the National Space Policy

2. Fund the Department of Homeland Security to implement a commercial SATCOM NS/EP program within the National Communications System to procure and manage the non-Department of Defense satellite communications satellite facilities and services necessary to increase the robustness of Government communications.

3. Appoint several members to represent service providers and associations from all sectors of the commercial satellite industry to the NSTAC.

   In September 2004, the White House appointed Mr. Joseph Wright of PanAmSat to the NSTAC membership

Summary

The Federal Government should address satellite vulnerabilities and immediately establish an NS/EP program for commercial SATCOM as real threats exist to vital role satellites play in NS/EP communications

- Satellites can and should complement terrestrial communications networks as a physically separate disaster recovery network
- Increasing dependence of commercial satellite systems by the DoD and DHS will make them an attractive target
- Vulnerabilities in satellites are real and can be/have been targeted from outside the U.S.
- Redundancy and restoral of satellite services is comparable to terrestrial alternatives