Online Journal of Space Communication

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

Article 7

June 2021

Satellite Security and Performance in an Era of Dual Use

Joseph N. Pelton

Satellite Security and Performance in an Era of Dual Use

By Dr. Joseph N. Pelton
Director, Space and Advanced Communications Research Institute (SACRI)
The George Washington University

Introduction

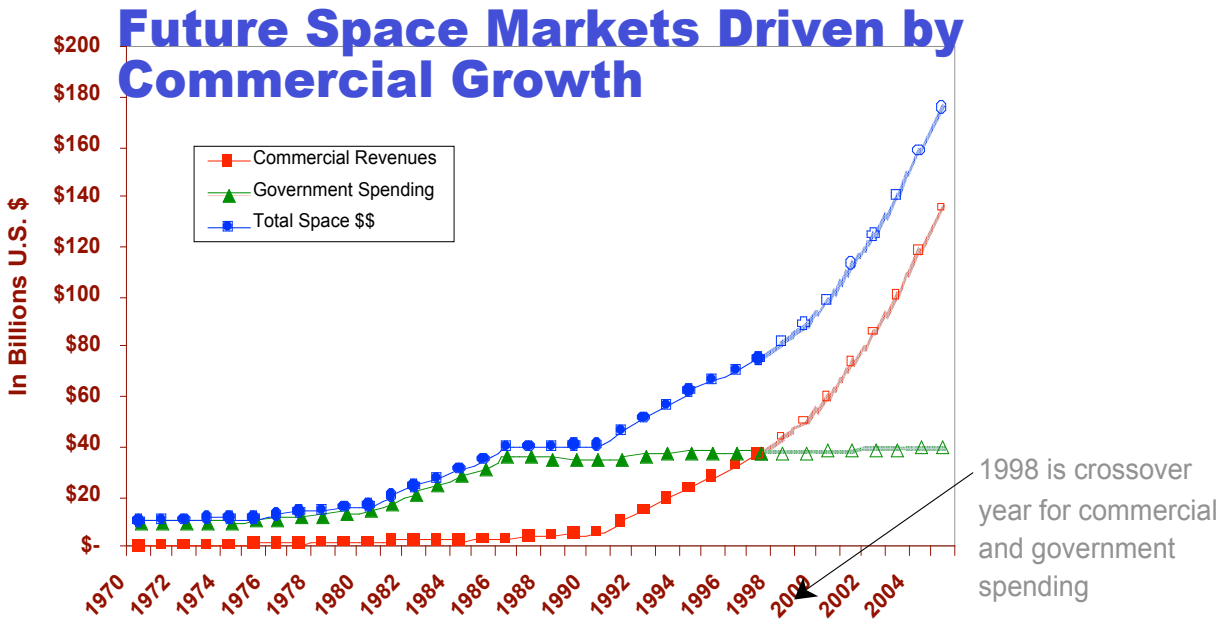
Since the mid-1990s the U.S. Government and military forces have placed more and more reliance on commercial satellite systems for military communications of a non-tactical nature. Requirements such as the U.S. Armed Forces Radio and Television require a great deal of bandwidth but do not require any special security protection. Further there are many other forms of communications involving national security or defense systems where a varying degree of security is required. Many of these applications do not require a very high level of "top secret" protection since these communications do involve tactical, strategic or highly classified messages. For instance, communications services that allow overseas forces to talk to their family and friends can be provided with only a minimum of digital encryption protection.

In the post 9/11 environment there are also now growing requirements for secure messaging involving homeland security. These communications typically do require highly protected fiber or military satellite facilities with 132 bit digital encryption, but still require a reasonably high level of security. In some cases these services can be made available via commercial satellite systems. Beyond the American-based military, governmental and security satellite requirements there are many other military, security, police, fire and peace-keeping telecommunications requirements around the world that

can and will also be met on commercial satellite systems. Such requirements today represent a very high percent of commercial satellite system growth.

Back in 1997, a Futron study as shown as Figure 1 below projected that new commercial traffic to support commercial business enterprise networks, scientific networks and entertainment would dominate growth while government and military service requirements would represent very limited growth. The cross over did occur in the 1ate 1990s. Since then commercial market growth on satellites has stagnated while military and related security growth has continued to be quite strong and is significantly fueled by "dual use" of commercial satellite systems.

Figure 1



Source: Futron Corporation, Satellite Industry Statistics Survey 1997 (conducted for Satellite Industry Association by Futron Corporation), with thanks to *Aerospace America* 's annual series of reports on national expenditures on space activities

The result has been that governmental and military services requirements for satellites continue to represent a very substantial portion of all commercial satellite services and satellite systems have had to adapt to this situation in terms of capacity availability, flexibility of geographic capability, and certain types of encryption and security requirements. Digital Video Broadcast (DVB) services that have represented a substantial share of satellite system growth in the past three years have been deployed to meet military requirements.

Overall non-strategic communications requirements for governmental operations, research, security and military systems now form the largest single user group on commercial satellite systems. Current rapid growth patterns suggest this will be even truer tomorrow. This demand is sufficiently strong that the new X-TAR commercial venture, involving U.S. and Spanish interests, now plans to build and launch at least two satellites to operate in the X-band that will carry exclusive military communications to support U.S. and European needs. The bulk of the $18.7 billion appropriated for the US Defense Department Transformational Communications Program will apparently be applied to dual use applications, despite the $8.7 billion earmarked for Milstar.

This concept of "dual use" is certainly not new. The Intelsat system has been carrying “non-tactic military traffic for the U.S. Armed Forces Radio and Television network to U.S. military basis for over thirty years. What is new is that the volume of traffic is growing exponentially and the type of requirements is expanding. These burgeoning requirements impact fixed satellite systems, mobile satellite systems, broadcast satellite systems, store and forward satellite systems, space navigation systems, radio determination satellite systems.

Dual Use Commercial Satellite Systems in the Post 2000 Time Period

In light of the new types of dual use requirements that have been identified in the last two commercial satellite systems have responded in a varied of ways. One clear way is that the Intelsat, Panamsat and SES Global Satellite systems have created new and more independent divisions to provide the particular needs of military and governmental security agencies. This means being able to handle the procurement, security and service flexibility required of such customers.

Today's commercial satellite systems must be able to respond to diverse requirements in terms of security networks, widely separated geographic locations, sudden peaks of traffic, and increasingly effective delivery of TCP/IP based traffic. Further dual use increasingly will come to mean the use of commercial satellite systems to meet not only non-tactical military communications but also homeland security based traffic as well. Finally commercial systems will need to be more protected and increasingly "secure" so that satellite networks cannot be used to initiate terrorists attacks against national infrastructure.

Figure 2 below outlines some of the security protections that exist in commercial satellite systems and the much more extensive (and expensive) forms of security protection that one finds on protected military communications satellite facilities such as Milstar, DSCS, etc. Despite the adaptations made by commercial satellite systems military satellites are very different and much more costly to build. Because of the special features and the unique design features that makes military satellites highly customized in their engineering and manufacture they can cost as much as three times as much as commercial satellite on a per circuit cost basis. It should be clearly understood that

commercial satellite systems are designed and built to meet commercial requirements and to be as cost effective and reliable as possible within the constraints of business efficiency. Thus there are limits to how effectively commercial satellite systems can meet military requirements. The X-TAR project may create a new paradigm that allows a totally new approach to dual use systems.

Figure 2

Comparing Commercial and Military Satellite Systems

Commercial Systems Security	Military and Gov't Systems
• TTC&M protection and security	• Radiation Hardening
• Digital encryption	• Anti-Jamming
• Data base protection	• 132 bit encryption or better
• Hardware & traffic redundancy + sparing + ISLs	• Enhanced TTC&M security
• PKI-GPS-Billing Authentication	• Use of special frequencies and laser com
• IP "Spoofing" Accelerators	• IP Sec
• 99.98% system availability	• Orbits-supersynchronous-ISL
	• Hardware redundancy System protection-secure tails

Commerical Satellites: How to Provide IP Security and Still Maintain Transmission Efficiency

One of the key challenges for commercial satellite systems that are providing dual use capability is to provide reliability, high efficiency and secure IP based services on which the entire world, including military forces increasingly rely. Here are the key steps that can be undertaken to make broadband IP transmission on satellite networks to work effectively:

- Break the TCP/IP end-to-end connection into three parts: the part before the satellite link, the satellite link, and the part after the satellite link.
- Put a TCP accelerator at each network node that uses the satellite link (This could be products such as the Mentat's SkyX product or the Via Sat Linkway product).
- Use a block protocol with appropriate forward error correction. These protocols include a go back and retry mechanisms for the satellite link where there is a "perception of congestion" due to latency rather than cycling through a "slow restart" process that would be normally associated with system congestion. This requires the ability to perform protocol translation in the TCP accelerator boxes at either end of the satellite link.
- For end-to-end secure communications, this requires the choice of security schemes that are compatible with above steps.

Such accelerator systems that are compatible with military security systems are operational on a number of commercial systems carrying "dual use" traffic.

Future Considerations

There are many complexities that arise from dual use of satellites and many who believe that use of commercial civilian telecommunications satellites to support military objectives, even those that are clearly non-conflict oriented such as television and radio entertainment programming, should not be allowed. M. Cervino, S. Corradini and S. S. Davolio, "Is the 'Peaceful Use' of Outer Space Being Ruled Out", Space Policy, (November 2003) Vol. 19, No.4 pp. 231-237 have quite recently argued that mixing commercial and military roles in space makes the ultimate military use and "weaponization" of space just that much more easy. They state

: "Even if the 'weaponization' of outer space is still (just) taboo, the development of dual-use systems (that is space systems with both civilian and military uses) is starting to be widely implemented by European and national communities in reply to what is already happened in the USA. Dual-use, seemingly a 'mild' form of military activity, may be the Trojan horse that opens the way to other military uses aimed at confrontation and military superiority on Earth."

The market, technical and operational forces that support dual-use in commercial civilian satellite systems around the world are today very strong. There can certainly be no doubt that blurring the lines between military, security and strictly civilian applications has it dangers for the satellite industry. Time will tell the extent to which these dangers become real or remain only theoretical.

Comparing Commercial and Military Satellite Systems

Commercial Systems Security

- **TTC&M protections**
- **Digital encryption**
- **Data base protection**
- **Hardware & traffic redundancy + sparing+ISLs**
- **PKI-GPS-Billing Authentication**
- **IP Sec +Accelerators**
- **99.98% system availability**

Military and Gov't Systems

- **Radiation Hardening**
- **Anti-Jamming**
- **132 bit encryption or better**
- **Enhanced TTC&M security**
- **Use of special frequencies and laser com**
- **IP Sec**
- **Orbits-supersynchronous-ISL**
- **Hardware redundancy**

  System protection-secure terrestrial tails

* NOTE: The addition of increased security to military and commercial systems has been an ongoing phenomena for many years as security technology has become more sophisticated and as security threats in both the business world and the world of military operations have also increased. Today the U.S. military systems relies very heavily on fiber optic networks for a good deal of its telecommunications requirements. Nevertheless it still uses an estimated 4.2 Gbps of satellite capacity on an overall basis and that amount has been estimated to increase by a factor of 10 over the next five years. Meanwhile the demand for broadband wireless and satellite business requirements is also now growing rapidly and the demand for security protection also has escalated as the demand to protect intellectual property and commercial business information has also increased. In short the commercial satellite world must be able to protect information and maintain its cost efficiency and throughput efficiency to respond to both commercial and dual use market demand.