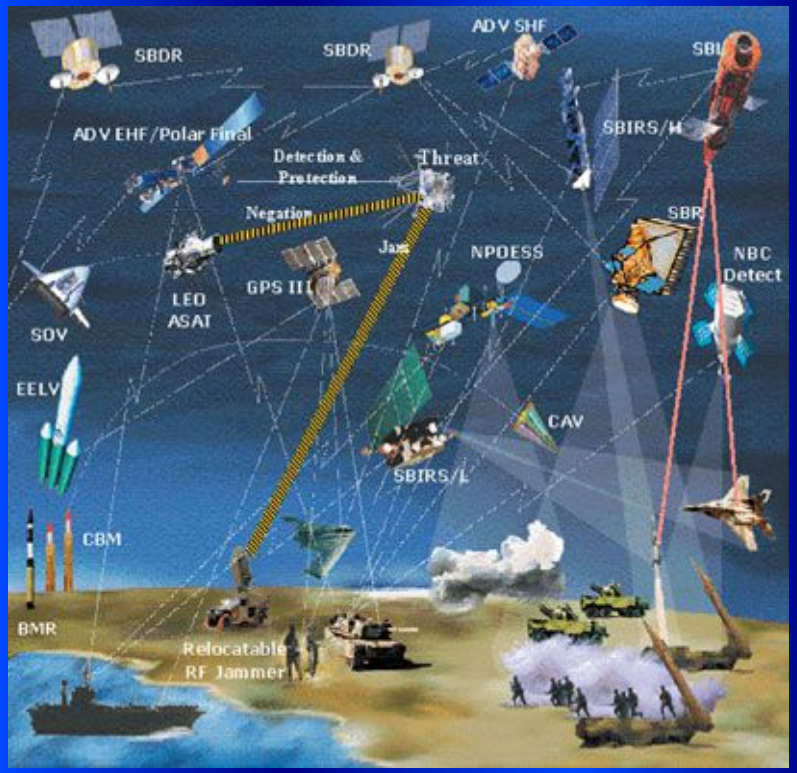
CRITICAL SPACE SYSTEMS AND INFRASTRUCTURE PROTECTION

STUDY CASE: THE SATELLITE SYSTEMS

I. VULNERABILITIES (1)

- THE VULNERABILITIES OF SATELLITE SYSTEMS ARE INTRODUCED BY THEIR INTRINSIC ATTRIBUTES:
  - MOVE IN ORBIT AT HIGH SPEEDS;
  - RENDERING COLLISIONS WITH EVEN SMALL SPACE DEBRIS ARE DISASTROUS;
  - NEARLY IMPOSSIBLE TO HIDE - JUST AS SATELLITES CAN VIEW LARGE SWATHS OF THE EARTH, THEY ARE ALSO VISIBLE TO OBSERVERS OVER LARGE SWATHS OF THE EARTH.



I. VULNERABILITIES (2)

- ONCE IN ORBIT, A SATELLITE'S MOTION IS PREDICTABLE;
- CHANGING THE ORBIT TAKES SIGNIFICANT EFFORT;
- DIFFICULT TO PROTECT: LAUNCH MASS IS AT A PREMIUM, SO ARMOR AND DEFENSIVE MEASURES COME AT SOME PRICE;
- THE SENSITIVITY OF COMMUNICATIONS SATELLITES, EASILY ACCESSED BY USERS ACROSS THE GLOBE, CAN BE EXPLOITED TO HARM THEM OR INTERFERE WITH THEIR OPERATION;
- ESSENTIALLY, NO SATELLITE CAN NOW BE REPAIRED ONCE DAMAGED.

II. SATELLITE SYSTEMS COMPONENTS

some of which make better targets than others

- THE SATELLITE ITSELF;
- THE GROUND STATIONS USED TO OPERATE AND CONTROL THEM;
- THE LINKS BETWEEN THEM.

III. SATELLITES BASIC ELEMENTS

- A STRUCTURAL SUBSYSTEM OR BUS.
- A THERMAL REGULATION SUBSYSTEM,
- A POWER SOURCE, OFTEN THE SOLAR PANELS

III. SATELLITES BASIC ELEMENTS (2)

- AN **ON-BOARD COMPUTER CONTROL SYSTEM**
  CIP: MAY INCORPORATE SOPHISTICATED ANTI-JAMMING HARDWARE
  - ❖ IF SOMEONE GAINED CONTROL OF THE SATELLITE'S COMPUTER, **THE SATELLITE COULD BE MADE USELESS BY ITS LEGAL OWNERS**;
  - ❖ COMPUTER SYSTEMS **MAY SHUT DOWN OR REBOOT** DURING SOLAR STORMS OR IF BARRAGED BY HIGH LEVELS OF ELECTROMAGNETIC RADIATION.

- A **COMMUNICATIONS SYSTEM**
  - ❖ SATELLITE TO/FROM ITS GROUND STATIONS;
  - ❖ SATELLITE TO/FROM OTHER SATELLITES.

IV. THE COMMUNICATION SYSTEM

- THE COMMUNICATION SYSTEM GENERALLY CONSISTS OF:
  - ❖ A RECEIVER;
  - ❖ A TRANSMITTER;
  - ❖ ONE OR MORE RADIO ANTENNAE.

- **CIP:** THE RADIO LINKS SATELLITE TO/FROM GROUND STATIONS ARE ONE OF THE MOST CRITICAL AND MOST VULNERABLE PARTS OF A SATELLITE SYSTEM.
- ALL SATELLITES REQUIRE A LINK TO AND FROM THE GROUND TO PERFORM "TELEMETRY, TRACKING, AND COMMAND" (TT&C) FUNCTIONS:
  - ❖ OPERATES THE SATELLITE;
  - ❖ EVALUATES THE HEALTH OF OTHER SATELLITE SYSTEMS

MAJOR THREATS AGAINST SATELLITES COMMUNICATION SYSTEM

1. JAMMING: RECEIVERS ON THE SATELLITE AND ON THE GROUND OVERWHELMED BY AN INTRUDING SIGNAL.

- ❖ THE JAMMING ATTACK IS MOUNTED FROM THE BROADCAST AND RECEPTION AREA OF THE TT&C COMMUNICATIONS CHANNEL;

CIP MEASURE: RESTRICTING THE SIZE OF THIS AREA BY INCREASING THE ANTENNA'S DIRECTIONALITY PROTECT THESE CHANNELS FROM ATTACK BY REDUCING THE REGION FROM WHICH THE JAMMING COULD TAKE PLACE;

- IS NOT A VIABLE SOLUTION FOR SATELLITES THAT NEED TO SUPPORT USERS FROM A BROAD GEOGRAPHIC AREA;
- THE TT&C CHANNELS ARE USUALLY WELL PROTECTED WITH ENCRYPTION AND ENCODING, AVOIDING A GREAT DEAL OF DAMAGE GENERATED BY INTERFERING;
- THE MORE VULNERABLE PIECE OF THE COMMUNICATIONS IS THAT USED FOR MISSION - SPECIFIC COMMUNICATIONS.

2. SPOOFING: INFORMATION CONFUSED BY FALSE SIGNALS

II. (cont.) DEDICATED SATELLITES CAN CARRY WEAPONS SYSTEMS FOR ATTACKING OTHER SATELLITES OR TARGETS ON THE GROUND OR IN THE ATMOSPHERE:

- ❖ A LASER SYSTEM;
- ❖ FUEL AND MIRRORS NEEDED TO USE THE LASER;
- ❖ EXPLOSIVE CHARGE INTENDED TO DESTROY ANOTHER SATELLITE.

III. GROUND STATIONS FOR SATELLITES MONITORING AND CONTROL.

- GENERALLY NOT HIGHLY PROTECTED FROM PHYSICAL ATTACK.
- COMPUTERS AT CONTROL CENTERS MAY BE VULNERABLE ESPECIALLY IF THEY ARE CONNECTED TO THE INTERNET.

IV. JAMMING OR SPOOFING THE LINKS (I)

1. **JAMMING THE DOWNLINK:** ATTACKER PREVENTS A GROUND STATION FROM RECEIVING A USABLE SIGNAL FROM THE SATELLITE
   - A DOWNLINK JAMMER COULD BE PLACED IN LEO TO JAM TRANSMISSIONS FROM SATELLITES IN HIGH ORBIT. SINCE SUCH A JAMMER WOULD BE 50 TO 100 TIMES CLOSER TO THE RECEIVER THAN A SATELLITE IN GEO OR SEMI-SYNCHRONOUS ORBIT
   - COULD GENERATE SIGNIFICANTLY LARGER SIGNALS AT THE RECEIVER.
   - IF A JAMMER CAN BE LOCATED, IT CAN BE ATTACKED DIRECTLY - WHICH IS LIKELY TO BE SEEN AS A LEGITIMATE ACTION DURING A MILITARY CRISIS.

IV. JAMMING OR SPOOFING THE LINKS (II)

- THE ANTI-JAMMING SYSTEMS MAY JUMP BETWEEN FREQUENCY BANDS USING A PATTERN KNOWN ONLY TO THE LEGITIMATE USER;
- TO COUNTER - SPOOFING, THE SIGNAL FROM THE SATELLITE CAN BE ENCRYPTED AND SCRAMBLED BEFORE IT IS SENT AND UNSCRAMBLED AFTER RECEIPT. BECAUSE SOPHISTICATED TECHNIQUES SUCH AS ENCODING AND ENCRYPTION ADD COMPLEXITY AND REDUCE THE AMOUNT OF DATA THE SATELLITE CAN HANDLE, COMMERCIAL SATELLITE OPERATORS ARE UNLIKELY TO FIND A FINANCIAL CASE FOR ADOPTING SUCH TECHNIQUES UNLESS

JAMMING OR SPOOFING THE LINKS (III)

2. JAMMING THE UPLINK:

- JAMMING UPLINKS TO SATELLITES OTHER THAN COMMUNICATIONS AND BROADCAST SATELLITES IN GEO IS TECHNICALLY MORE DEMANDING, SINCE THE ATTACKER NEEDS TO LOCATE AND PERHAPS TRACK THE SATELLITE. THIS WOULD BE THE CASE FOR ANY COMMUNICATIONS NETWORKS BASED IN LEO (AS THE IRIDIUM SYSTEM) AND FOR ANY SATELLITE NOT IN GEO.
- COMMERCIAL COMMUNICATIONS AND BROADCAST SATELLITES MAY BE PARTICULARLY VULNERABLE TO UPLINK JAMMING AND SPOOFING BECAUSE THEY ARE DESIGNED TO RECEIVE SIGNALS FROM USERS OVER BROAD GROUND AREAS, AND THUS THERE WILL BE A LARGE AREA FROM WHICH IT WILL BE POSSIBLE TO JAM OR SPOOF THE UPLINK.

IV. OTHER THREATS:

1. LASER ATTACKS ON SATELLITE SENSORS

- LASERS ARE ESPECIALLY USEFUL FOR DIRECTED ENERGY ATTACKS BECAUSE THEY CAN EMIT A LARGE AMOUNT OF ENERGY IN A NARROW BEAM AND A NARROW BAND OF FREQUENCIES.
- ALLOW THE ATTACKER TO EFFICIENTLY DIRECT ENERGY TO THE RIGHT SPOT ON A SATELLITE WITH THE PROPER FREQUENCY TO INFLICT DAMAGE;
- NEED TO CHOOSE A FREQUENCY THAT PENETRATES THE ATMOSPHERE IN THE CASE OF A GROUND-BASED LASER.
- A LASER ASAT SYSTEM ALSO REQUIRES A TRACKING AND POINTING SYSTEM. A MOVABLE MIRROR CAN BE USED BOTH TO DIRECT THE LASER BEAM TOWARD THE SATELLITE AND TO FOCUS THE BEAM.
- ASAT LASER SYSTEMS CAN BE BASED ON THE GROUND, AT SEA, IN THE AIR, OR IN SPACE. GROUND AND AIR-BASED LASER ASAT SYSTEMS WOULD OPERATE AT VISIBLE AND INFRARED WAVELENGTHS—THAT CAN PROPAGATE THROUGH THE ATMOSPHERE.

IV. OTHER THREATS:

- **DAZZLING:** USING THE LASERS FOR TEMPORARILY INTERFERING WITH THE SENSOR OF A A SATELLITE THAT TAKE IMAGES OF OBJECTS ON THE GROUND.
- **PARTIAL BLINDING:** AT SUFFICIENTLY HIGH INTENSITIES, LASER LIGHT CAN PERMANENTLY DAMAGE THE SENSORS OF IMAGING SATELLITES. SUCH DAMAGE IS KNOWN AS PARTIAL BLINDING, SINCE SUCH AN ATTACK WILL DAMAGE ONLY A PORTION OF THE SENSOR.
- **HIGH POWER LASER ATTACKS ON SATELLITES:** HEATING AND STRUCTURAL DAMAGE
  - ❑ THE DEFENSIVE MEASURES A SATELLITE COULD TAKE:
    - ❖ HARDENING EXPOSED SURFACES;
    - ❖ BUILDING IN REDUNDANCY;
    - ❖ DEPLOYING A PROTECTIVE SHIELD AGAINST THE LASER LIGHT
-

IV. OTHER THREATS:

- HIGH-POWERED MICROWAVE ATTACKS
- KINETIC ENERGY ATTACKS
- SPACE MINES
- ELECTROMAGNETIC PULSE FROM A HIGH-ALTITUDE NUCLEAR EXPLOSION

"Sample Nuclear Launch While Under Cyber Attack"

[yes, this is a doctored photo, used here just to lighten a serious moment]
Source: http://www.armscontrolwonk.com/1955/missile-palooza

BIBLIOGRAPHY (I)

1. Report of the Commission to Assess United States National Security, Space Management and Organization, January 11, 2001, http://www.fas.org/spp/military/commission/report.htm
2. Michael J. Muolo et al.: Space Handbook, Volume 1: A War Fighter's Guide to Space, (Maxwell Air Force Base, AL: Air University Press, December 1993), http://www.au.af.mil/au/awc/awcgate/au- 18/au180001.htm
3. Michael J. Muolo et al.: Space Handbook, Volume 2 - An Analyst's Guide, (Maxwell Air Force Base, AL: Air University Press, December 1993); Office of Technology Assessment, Anti-Satellite Weapons, Countermeasures, and Arms Control (Washington, DC: Government Printing Office, 1985);
4. Philip E. Nielsen, Effects of Directed Energy Weapons, (National Defense University, 1994), http://www.ndu.edu/ctnsp/directed_ energy.htm.
5. Bob Preston et al., Space Weapons Earth Wars (Arlington, VA: RAND Project Air Force, 2002) http://www.rand.org/publications/MR/ MR1209/.
6. Report of the American Physical Society Study Group on Boost-Phase Intercept Systems for National Missile Defense, July 2003, http://www.aps.org/public_ affairs/popa/reports/nmd03.html.

BIBLIOGRAPHY (II)

7. Report of the American Physical Society Study Group on Boost-Phase Intercept Systems for National Missile Defense, July 2003, http://www.aps.org/public_affairs/popa/reports/nmd03.html.
8. Air University Space Primer, August 2003, http://space.au.af.mil/primer.
9. Federation of American Scientists' Panel on Weapons in Space, Ensuring America's Space Security, September 2004, http://www.fas.org/main/content.jsp?formAction=297&contentId=311
10. Bruce M. DeBlois et al., "Space Weapons: Crossing the U.S. Rubicon," International Security (Fall 2004): 1–34.
11. Orbital Sciences Corporation, "Pegasus Mission History," http://www.orbital.com/Space_Launch/Pegasus/pegasus_history.htm
12. William Scott: "Fighters as Spacelift," Aviation Week & Space Technology, April 7, 2003.
13. Robert Wall, "Hot Rod to Space," Aviation Week and Space Technology, September 22, 2003, 48.
14. American Physical Society (APS), Report of the American Physical Society Study Group on Boost-Phase Intercept Systems for National Missile Defense, July 2003, 127, http://www.aps.org/public_affairs/popa/reports/nmd03.html

BIBLIOGRAPHY (III)

15. Peter Taylor, "Why Are Launch Costs So High?" September 2004, http://www.ghg.net/redflame/launch.htm, accessed January 21, 2005.
16. William Scott, "Rapid Response," Aviation Week and Space Technology example, Peter Taylor, "Why Are Launch Costs So High?" September 2004, http://www.ghg.net/redflame/launch.htm, accessed January 21, 2005.
17. William Scott, "Rapid Response," Aviation Week and Space Technology, April 7, 2003.
18. Matt Bille and Robyn Kane, "Practical Microsat Launch Systems: Economics and Technology," Paper SSCO3-III-3, AIAA/USU Conference on Small Satellites, August 2003, http://www.mitre.org/work/tech_papers/tech_papers_03/kane_mls/kane_mls.pdf.
25. David Wright, Laura Grego, and Lisbeth Gronlund: "The Physics of Space Security - A Reference Manual", ISBN#: 0-87724-047-7, American Academy of Arts and Sciences
20. Leonard David, "Military Space: Securing the High Ground," Space.com, April 2, 2003, http://www.space.com/businesstechnology/technology/higher_ground_030402.html
21. Matt Bille and Robyn Kane, "Practical Microsat Launch Systems: Economics and Technology," Paper SSCO3-III-3, AIAA/USU Conference on Small Satellites, August 2003, http://www.mitre.org/work/tech_papers/tech_papers_03/kane_mls/kane_mls.pdf.
22. Leonard David, "Military Space: Securing the High Ground," Space.com, April 2, 2003, http://www.space.com/businesstechnology/technology/higher_ground_030402.html.
23. Kamran Ahmed, "Tutorial Satellite Communications", http://www.slideshare.net/kamranahmed7186/satellite-communication-a-tutorial-28226854

THANK YOU FOR YOUR KIND ATTENTION !

General** (Ret.) Prof. MARIUS – EUGEN OPRAN
ROSA / EESC / INFLPR / IFIN-HH