Electronic Warfare and Satellites
Challenges in Assuring Space Capabilities

Brian Weeden
Technical Advisor
Secure World Foundation

Takeaways

- Space capabilities play an increasingly important role in national security and military operations
- The reliance on space capabilities makes them a target for adversary counterspace operations
- Electronic warfare and cyber may be the preferred way to attack space capabilities, because they don't have the same long-term consequences as kinetic attacks on satellites (space debris)
- Mitigating EW and cyber attacks against space means learning lessons from other domains

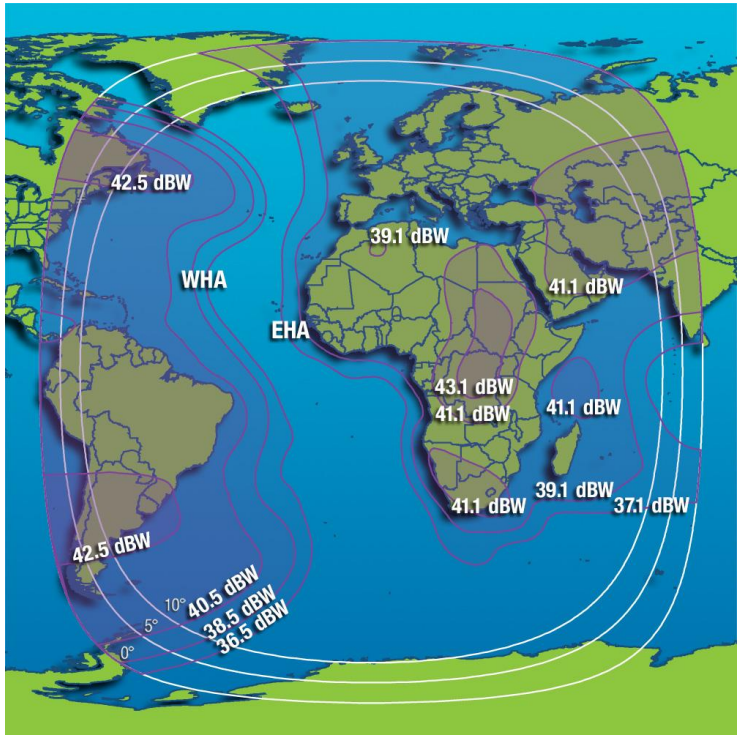
Current satellites on orbit

Total number of operating satellites: 1,419			
United States: 576	Russia: 140	China: 181	Other: 522
LEO: 780	MEO: 96	Elliptical: 37	GEO: 506

Total number of military satellites: 350					
Navigation	Weather	Communications	Missile Warning	Intelligence, Surveillance, & Reconnaissance	Technology Development
101	10	117	10	113	30

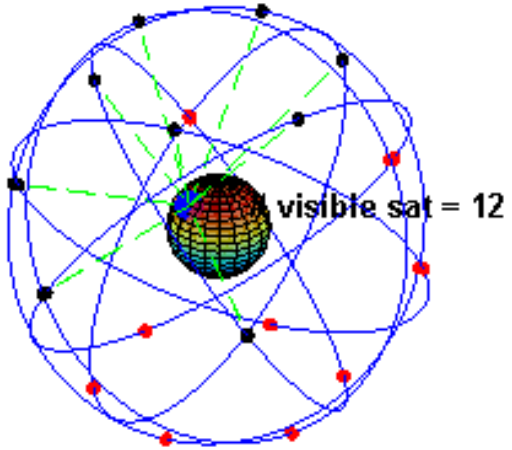
Source: Union of Concerned Scientists Satellite Database
(includes launches through 6/30/16)
http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database

Major military activities in space



Field of view of a single geostationary satellite
Source: Intelsat

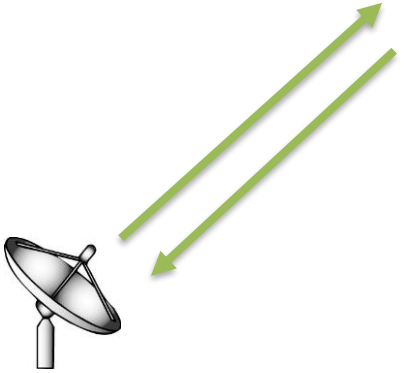
1-Meter Resolution Radar Image of the U.S. Capitol



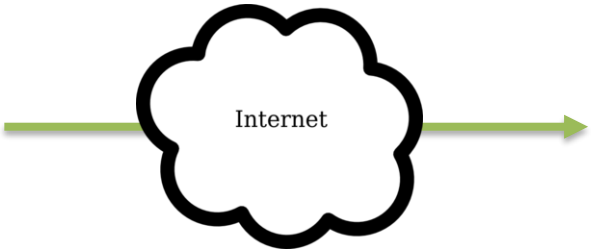
GPS constellation

Elements of a space capability

Space segment

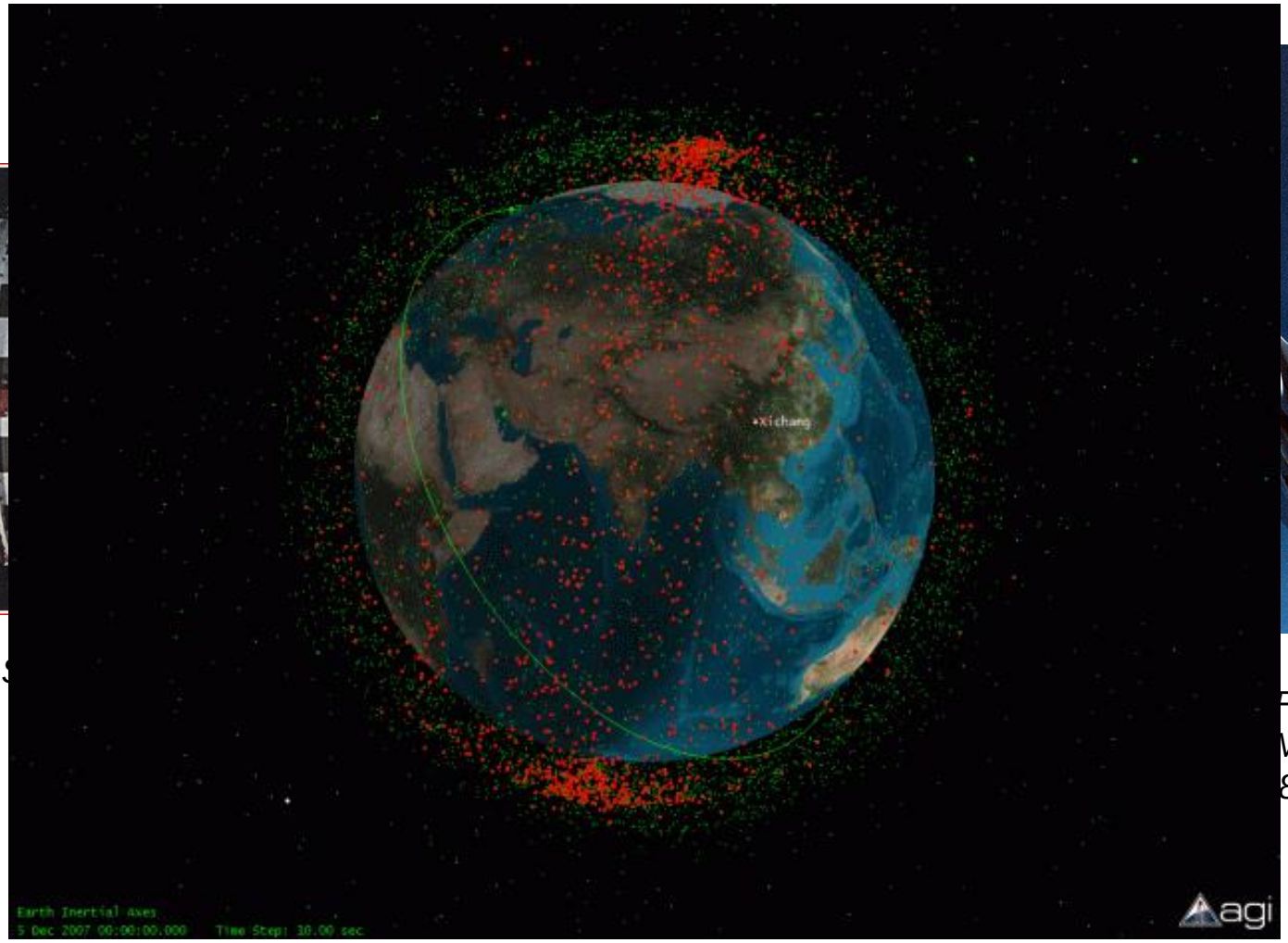


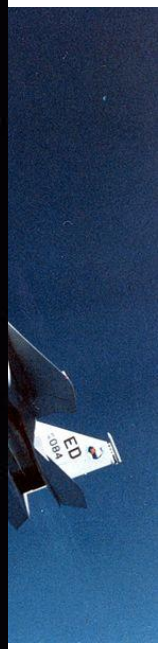
Ground segment



User segment

Kinetic attacks on satellites





F-15
M-135
8-1988)

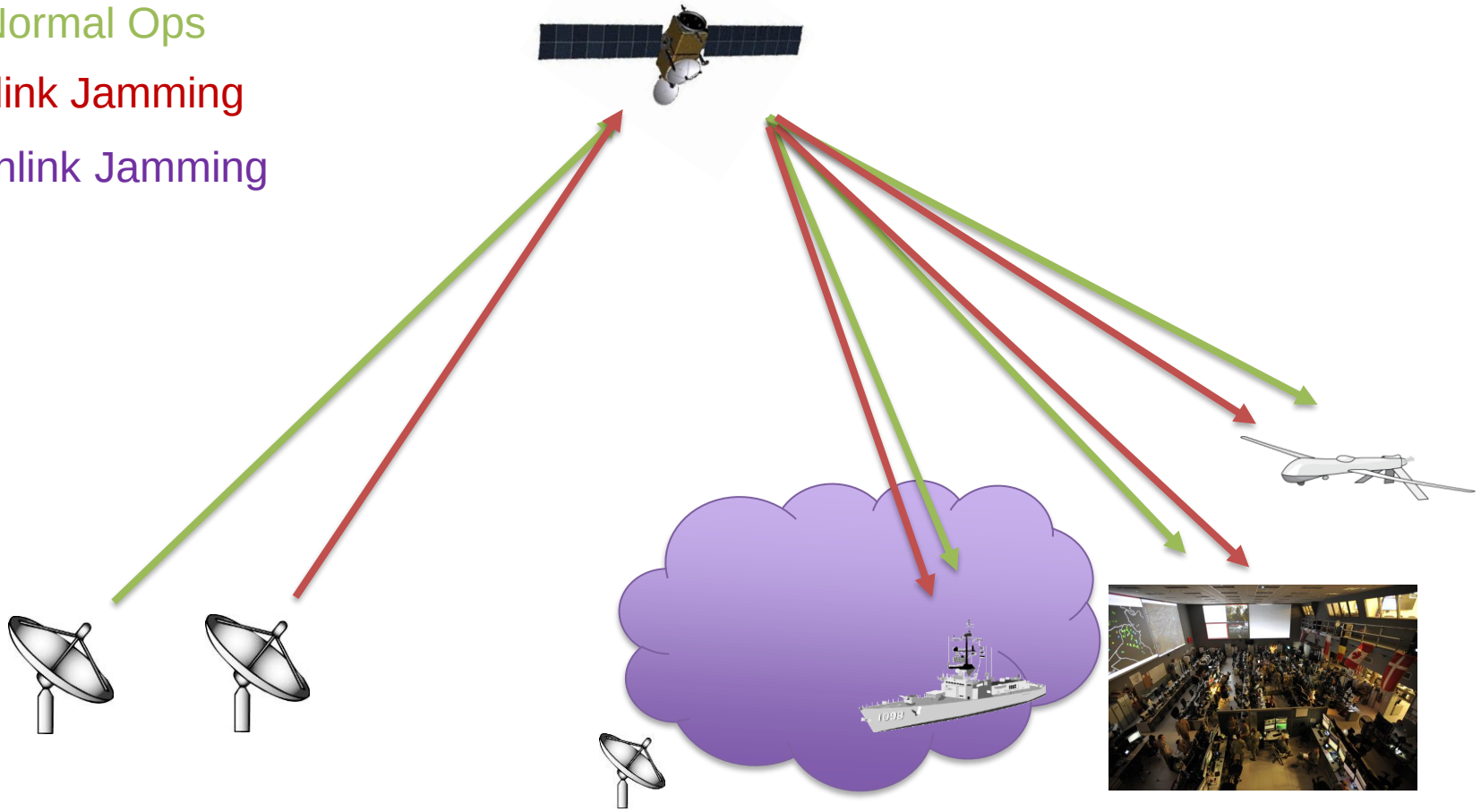
Debris from 2007 Chinese ASAT Test
(Source: Celestrak)

Satellite jamming

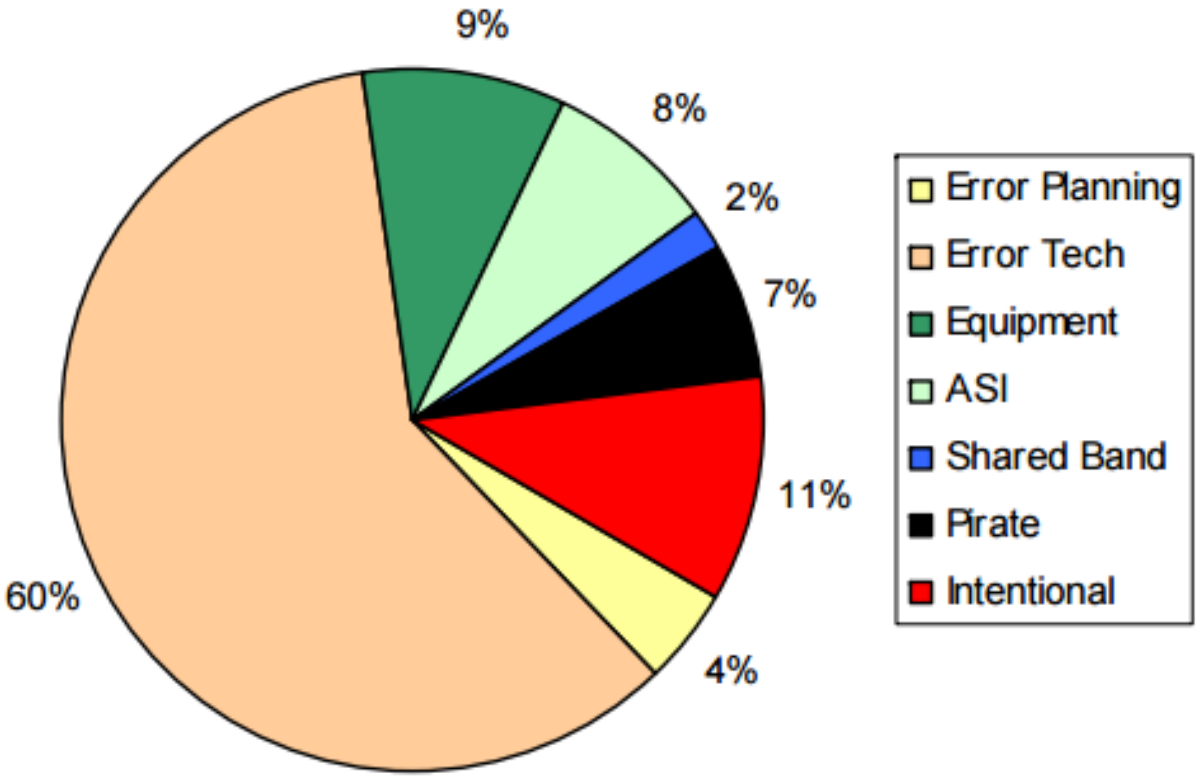
Normal Ops

Uplink Jamming

Downlink Jamming



Sources of interference



Source: Eutelsat briefing to the ITU (2013)

Space EW in Ukraine

At 13.01hrs and again at 13.19hrs the SMM UAV was subjected to serious electronic jamming while flying over "DPR"-controlled Chermalyk (40km NE of Mariupol). Initial analysis of the SMM UAV flight log data indicated that the SMM UAV was subjected to military-grade GPS jamming. The Ukrainian Air Operations Liaison Officer to the "Anti-Terrorism Operation" ("ATO") headquarters in Sector 'M', who was immediately contacted by the SMM UAV Team, told the SMM at 13.24hrs that there was no jamming by the Ukrainian forces. The SMM UAV left the area and landed safely. This is the third serious interference with the movement of the SMM UAV and is an impediment to the fulfilment of the Mission's mandate.

Source: Organization for Security and Cooperation in Europe

Russian R-330ZH Zhitel

Source: Ukrainian journalist Yaroslav Krechko

Satellite hacking

Malicious Cyber Activities Directed Against U.S. Satellites—*Continued*

Notably, at least two U.S. government satellites have each experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems: *

- On October 20, 2007, Landsat-7, a U.S. earth observation satellite jointly managed by the National Aeronautics and Space Administration and the U.S. Geological Survey, experienced 12 or more minutes of interference. This interference was only discovered following a similar event in July 2008 (see below).†
- On June 20, 2008, Terra EOS [earth observation system] AM–1, a National Aeronautics and Space Administration-managed program for earth observation, experienced two or more minutes of interference.‡ The responsible party achieved all steps required to command the satellite but did not issue commands.
- On July 23, 2008, Landsat-7 experienced 12 or more minutes of interference. The responsible party did not achieve all steps required to command the satellite.
- On October 22, 2008, Terra EOS AM–1 experienced nine or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands.

The National Aeronautics and Space Administration confirmed two suspicious events related to the Terra EOS satellite in 2008 and the U.S. Geological Survey confirmed two anomalous events related to the Landsat-7 satellite in 2007 and 2008.§

Source: US-China Economic and Security Review Commission (2011)

Chinese hack U.S. weather systems, satellite network

Hackers from China breached the federal weather network recently, forcing cybersecurity teams to seal off data vital to disaster planning, aviation, shipping and scores of other crucial uses, officials said.

Source: The Washington Post (2014)

Non-state actors and EW

$2,500 Phase-Coherent GPS Signal Synthesizer

Used to perform cyber attacks on GPS receivers using manipulated civil signals

Source: Nighswander, Ledvina, Diamond, Brumley, and Brumley (2012)

$85 million White Rose of Drachs

Successfully steered off course by UT grad students using homemade GPS spoofer

Source: UT Austin School of Engineering (2016)

Hackers discover satellites

Spread Spectrum Satcom Hacking

Attacking the Globalstar Simplex Data Service

Source: Black Hat USA (2015)

A Wake-up Call for SATCOM Security

Satellite Communications (SATCOM) play a vital role in the global telecommunications system. IOActive evaluated the security posture of the most widely deployed Inmarsat and Iridium SATCOM terminals.

IOActive found that malicious actors could abuse all of the devices within the scope of this study. The vulnerabilities included what would appear to be backdoors, hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. In addition to design flaws, IOActive also uncovered a number of features in the devices that clearly pose security risks.

The findings of IOActive's research should serve as an initial wake-up call for both the vendors and users of the current generation of SATCOM technology.

Source: IOActive (2014)

"The problem," Sec explained, "isn't that Iridium has poor security. It's that it has no security." – *Motherboard, Aug 2015*

Mitigation steps (1)

- Change mindset
  - Satellites and space capabilities are basically computers in space
  - Assume they will have all the challenges computers would (and more)

- Imbed security into the system architecture
  - Software QA and code reviews
  - Authentication, encryption, and validation of C2 and priority traffic
  - Secure update mechanism

- Leverage (don't reject) the hacker mentality
  - Responsible disclosure policies
  - Bug bounty programs
  - Public response campaign

Mitigation steps (2)

- Increase communication between space and cyber security experts
  - Break down silos of excellence
- Increase space situational awareness
  - Will help deter attacks and identify sources of anomaly and malfunctions
- Clarify international law and military rules of engagement
  - At what point does an EW/cyber attack on a satellite become an armed attack?
  - What is a proportional response to an attack on a satellite?
  - McGill MILAMOS Project

Thank You!
Questions?

bweeden@swfound.org