United Nations Institute for Disarmament Research
Institut des Nations Unies pour la recherche sur le désarmement

Space Security Conference 2011:
Building on the Past, Stepping Towards the Future

Space Security Capabilities and Trends

Tal Dekel **Ram Levi**

Yuval Ne'eman Workshop for
Science, Technology
and Security
Tel Aviv University

TEL AVIV UNIVERSITY

Space Security

"The secure and sustainable access to, and use of, Space and freedom from Space-based threats".(SSI2010)

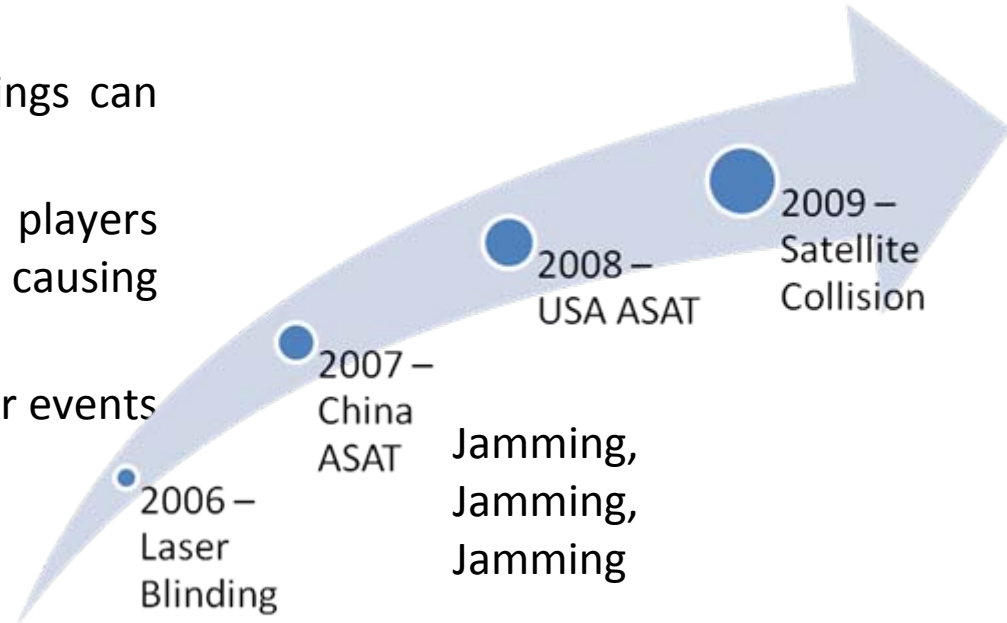
Methodology

Intentions and vision
Straight-forward examination of Space programs, and statements of key players

Actual capabilities
Examining events and R&D programs through the prism of Space security, to understand actual capabilities or vulnerabilities

Space Security – Why Now?

- Superpowers understand that Space is vital to their national security and to their capability to manage continuous military campaigns
- Space is an enabler for information superiority
- Space assets are vulnerable and things can happen…
- The Space Club is growing – more players have access to Space – more players causing damage
- Kessler syndrome – a few more major events could cause a cascading effect



Outline

- Bottom-up analysis
  - Space security events
  - Actual ASAT capabilities
- Top-down analysis
  - Intentions and vision
  - Declared Space capabilities of the main players as seen from outside
- Conclusions

SPACE SECURITY EVENTS

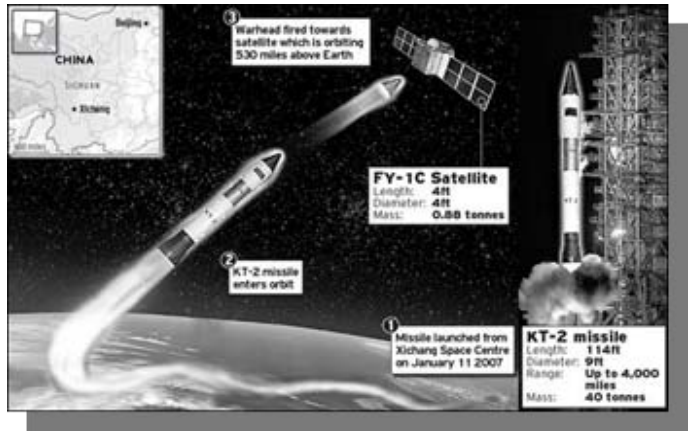
Space security events are events that reduce or deny access to, and use of, Space systems.

Recent Space Security Incidents

ASAT tests	2
Satellite collision	1
Laser blinding	1
Fire in ground station	1
Presumed cyber-attacks	2
Lost and found satellites	>5
Events of jamming	Hundreds

ASAT Tests

- Date: Jan. 11, 2007
- Source: PRC
- Target: PRC Weather Satellite
- Description: SC-19 Ballistic Missile armed with a kinetic kill vehicle hit a 950 Kg. satellite at about 853 Km. in LEO



- Date: Feb. 21, 2008
- Source: US
- Target: US Reconnaissance Satellite
- Description: SM-3 missile fired from a Navy ship hit a 2000 Kg. US satellite ~246 Km. above Earth

Consequences: successful interceptions of more than 20,000 tractable debris, international concern

ROSAT Allegedly Hit by Cyber-Attack

- Event Type: cyber-attack
- Date: Sep. 1998
- Source: unknown
- Target: ROSAT, US-German-UK Satellite
- Description: satellite turned to the sun for no reason
- Consequences: damaged optical sensor resulting in satellite to be useless
- Vulnerability: "The OIG review found that six computer servers associated with information technology (IT) assets that control NASA Spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable"

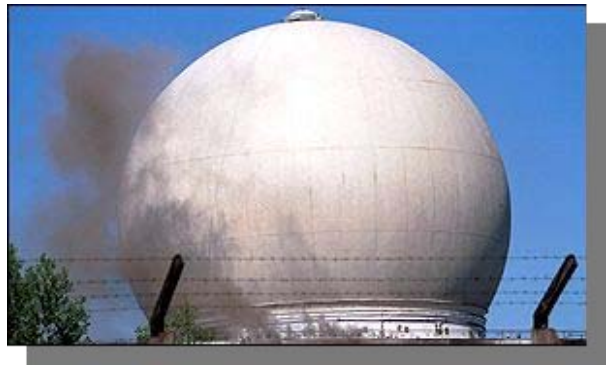
ROSAT Satellite. Source: NSAS

NASA Control room. Source: NASA

Image Source: http://www.mpe.mpg.de/xray/wave/technologies/amcs.php / NASA
Event Source: http://www.schneier.com/blog/archives/2008/12/cyberattacks_ag.html
NASA Source: http://oig.nasa.gov/audits/reports/FY11/IG-11-017.pdf OIG audit report 30 March 2011

Fire at Russian Ground Control Station

- Event Type: satellites loss due to ground control failure
- Date: May 10, 2001
- Source: Russia
- Target: na
- Description: "A fire at the ground control station damaged the system almost beyond repair. The fire destroyed one of the buildings and cables at the Serpukhov-15 control station, which led to a loss of communication with all four satellites in orbit"
- Consequences: "Three satellites, Cosmos-2340, Cosmos-2342, and Cosmos-2351, remained non-operational (although Cosmos-2342 performed a maneuver in October 2001). These satellites are very unlikely to recover, since they have drifted too far off their stations"
- Vulnerability: ground station lack of safety can cause loss of satellites

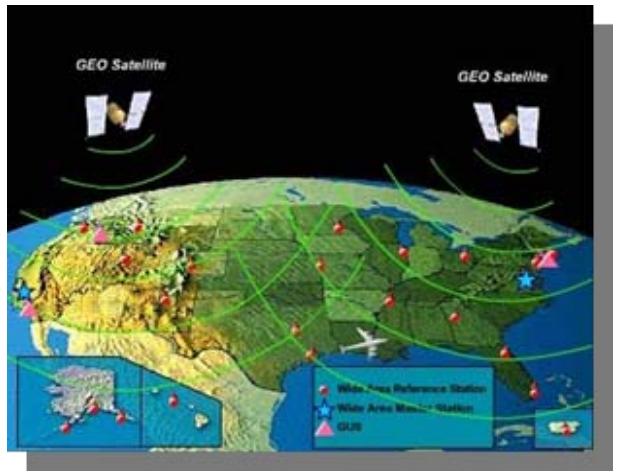


Serpukhov-15. Source: BBC

Source: http://cisac.stanford.edu/publications/history_and_the_current_status_of_the_russian_earlywarning_system/
Image Source: http://news.bbc.co.uk/2/hi/europe/1322700.stm

Zombiesat

- Event Type: unprecedented loss of control
- Date: Apr. 2010 – Jan. 2011
- Source: Intelsat Galaxy 15 GEO satellite
- Target: interference to Neighboring satellites, WAAS
- Description: lost communication with the G15 TC&C module. As a result, the satellite started drifting eastward, threatening interference with other satellites in its path. Jan 2011 control has been re-established
- Consequences: loss of WAAS in Alaska
- Vulnerability: no backup for some of the WAAS coverage, malicious implications of the EW blasting



WAAS architecture. Source: FAA

Galaxy 15. Source: Intelsat

This event "could serve as a war-games-type test for aeroSpace engineering students."

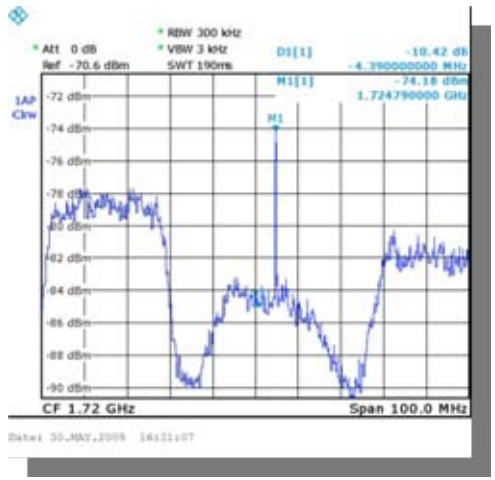
Alan Young, CTO, SES World Skies. Source: Spacenews

Source: http://www.intelsat.com/resources/galaxy-15/operational-status.asp
http://www.Spacenews.com/satellite_telecom/100430-galaxy15-still-adrift-poses-threat.html

Iran Pre-Election Jamming

- Event type: satellite jamming
- Date: spring 2009 (year long event)
- Source: Iran
- Target: Hotbird 6/8, W6, Eurobird 9A/2
- Description: Iran actively jammed Eutelsat satellites broadcasting content opposing the regime (ex. BBC, VOA opposition channels)
- Consequences: formal complaint to ITU, raised cost of jam-potential channels, operator (SAT owners) deterrence

Effect of jamming . Source rnw.nl



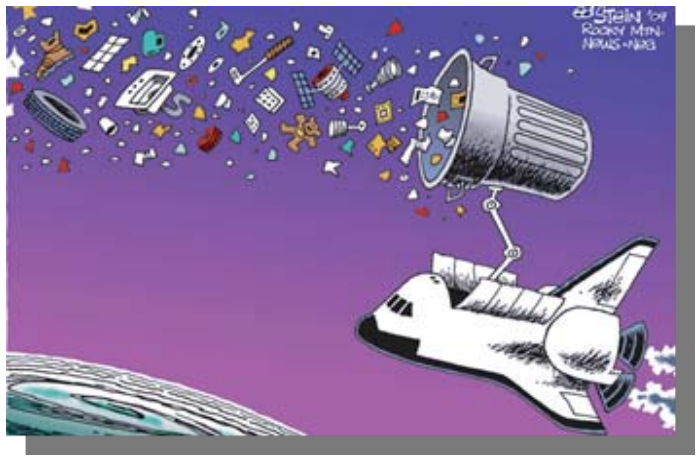
Jammed signal with CW.
Source: Sat Operator

"I felt that someone is giving me on-line instructions. I am shutting off his target and he is turning off the jamming. I bring the channel back, jamming resumes…"

Source: undisclosed satellite operator

POTENTIAL ASAT CAPABILITIES

A capability, developed for peaceful purposes, that can be easily modified to an ASAT capability



”I guess the debris removal system has the potential to be an anti-satellite [system] if you don’t ask the owner if he wants the Spacecraft to be removed”

Heiner Klinkrad, ESA

Source: http://www.militarynewsnetwork.com/magazine/orbital3.jpg

X-37B Orbital Test Vehicle

- Manufacturer / Developer: Boeing / USAF
- First orbital mission: USA-212 launched on Apr. 22, 2010 (1st prototype)
- Current operational mission: USA-226 launched on Mar. 5, 2011 (2nd prototype)
- Capabilities:
  - Reusable return vehicle, max. mission duration 270 days
  - On orbit autonomous maneuvering and re-entry
  - Specific mission payload
- ASAT Capabilities:
  - Directed energy payload against satellites in orbit
  - Host for secret satellites with ASAT capabilities
  - Close proximity maneuver

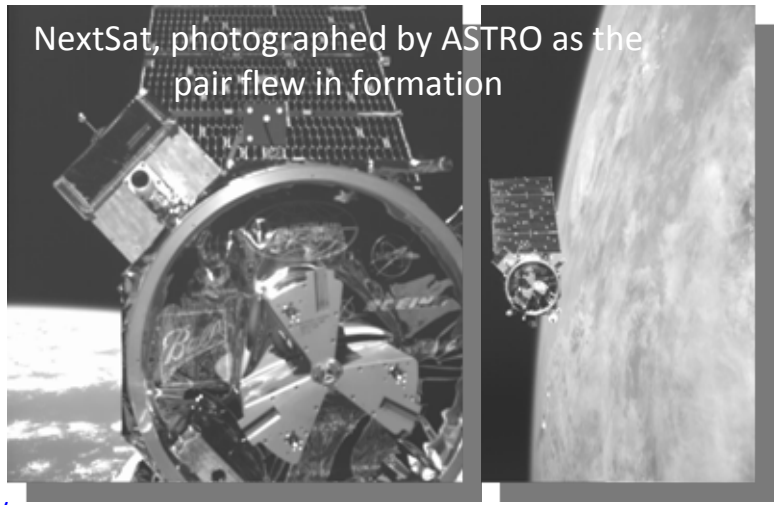
X-37B launch source: Space.com

Source: http://www.popsci.com/technology/article/2011-02/russia-building-its-own-military-Space-plane-match-mysterious-x-37b

Orbital Express Space Infrastructure Servicing ("SIS")

- Manufacturers: Boeing / MDA Corp. & Intelsat
- First proof of concept (LEO): Aster-Nextsat 2007
- Expected Deployment (GEO): 2015
- Capabilities:
  - Servicing of on-orbit satellites via a near Space-based service vehicle
  - Fuel, re-positioning or other maintenance using sophisticated robotics and docking systems
- ASAT capabilities:
  - Rendez-vous , dock , tow and ruin satellites

SIS Architecture. Source: Spacenews



Orbital Express. Source: NASA

Source: http://science.nasa.gov/science-news/science-at-nasa/2007/06jul_astroandnextsat/
Source: http://www.mdacorporation.com/corporate/news/pr/pr2011031501.cfm

Source: Space.com

Lasers in Space

- Developer: ESA
- First deployment: 2005
- Capabilities: up to 100 mJ pulsed laser for 50 Km. range and substance detection LIDAR and DIAL
- ASAT capabilities: blinding or permanent damage to electro-optical payloads

LIDAR Satellite. Source: Roland Meynart, ESA

Source: Roland Meynart, ESA

Source: http://apod.nasa.gov/apod/image/0611/vladish_bobbett.jpg

Cyber-threats

- The cyber-threat is a real threat on satellites and satellite systems
- Ground stations, links, and supporting communications networks are all vulnerable to cyber attacks. Malicious software can be: (GAO 2002)
  - Implanted into computer systems during development or operations.
  - Used to manipulate, corrupt, modify, or compromise data
  - Used to attack processor-controlled transmission equipment, control systems, or the information being passed
- Unverified:
  - Stuxnet worm hit India's INSAT-4B Satellite - not according to ISRO.
  - ROSAT hit by cyber-attack

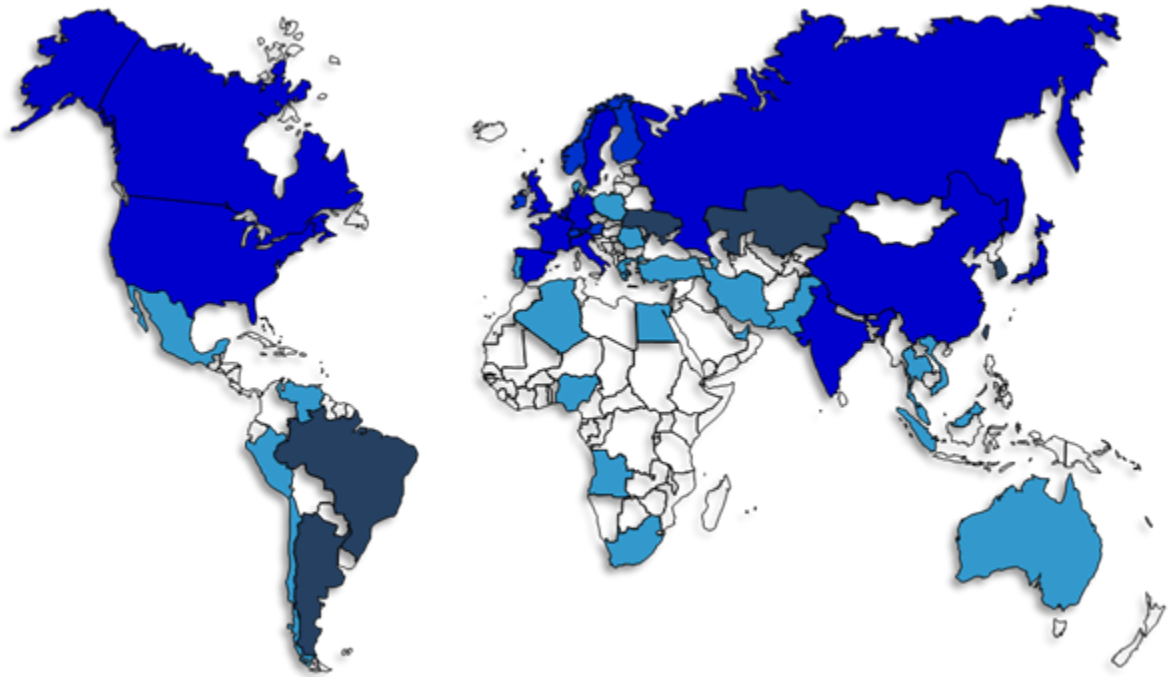
"… Even more troubling is that the threats appear to evolve along with new technologies and range from low-end hacking to complex attacks aimed at some of NASA's most sensitive data"

(NASA 2007)

" We identified a situation that could severely degrade or cripple NASA's operations"

(OIG on NASA IT 2011)

NATIONAL PROGRAMS



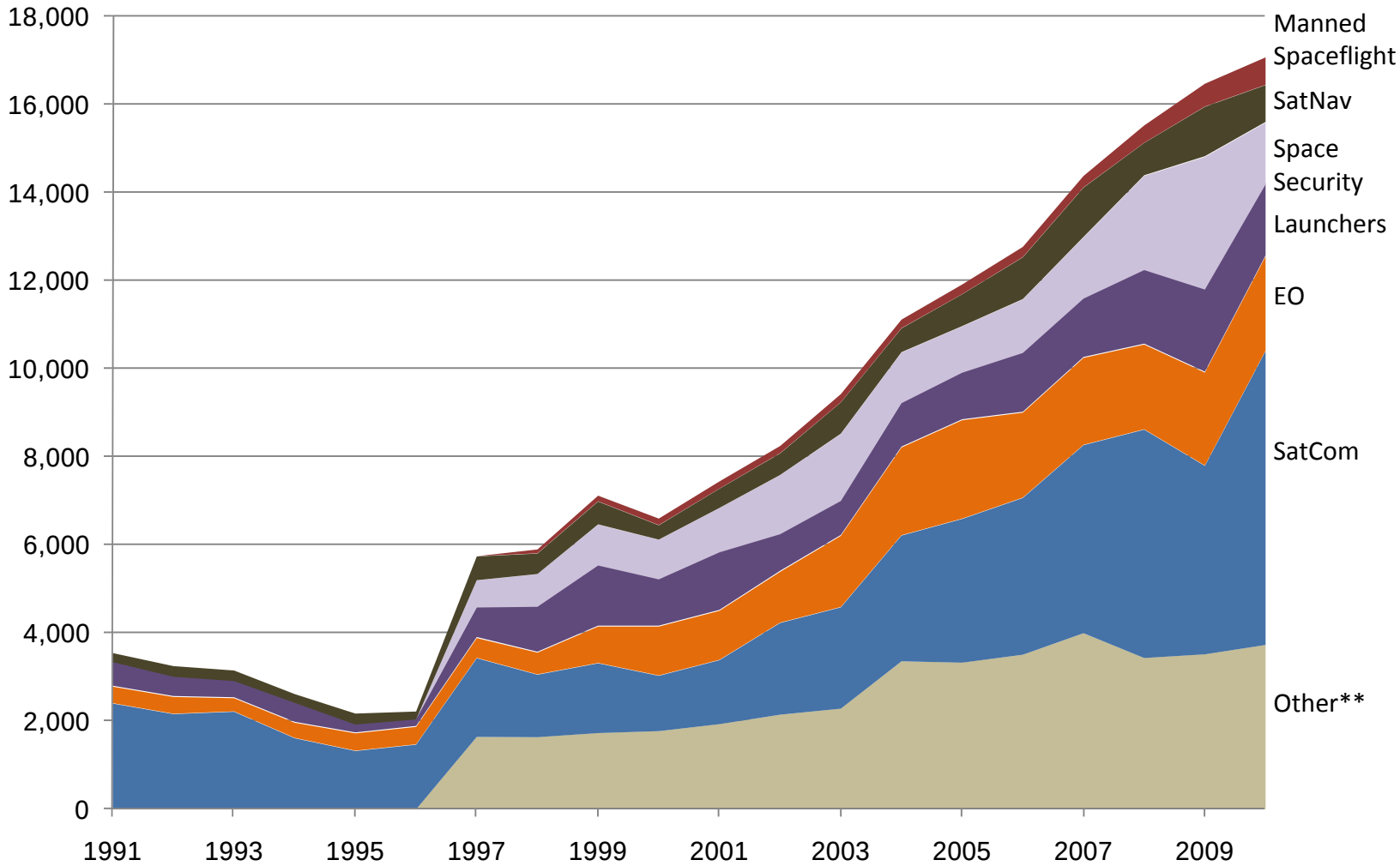
Source: Euroconsult

Key Capabilities

- All major actors have proven ASAT capabilities
- “Dual-use” capabilities: lasers, debris removal, broadcast
- Jamming capabilities are a common commodity – a threat that can cause escalations
- Nations are building cyber-attack capabilities that impose a real threat on Space systems

World Government Defense Expenditures by Application* (1991 – 2010)

US Dollars in millions



* Unclassified expenditures only

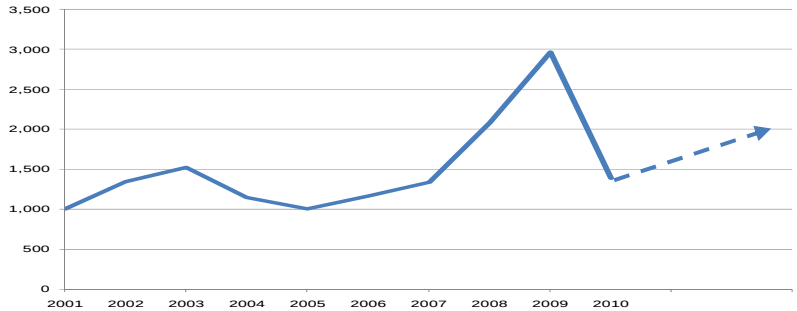
** Other includes technology, general budget and other expenditures

Source: Euroconsult

World Leading National Government Space Security Expenditures

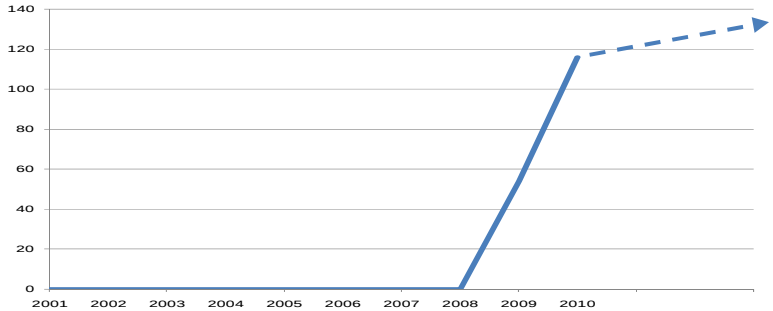
Dollars in millions

USA



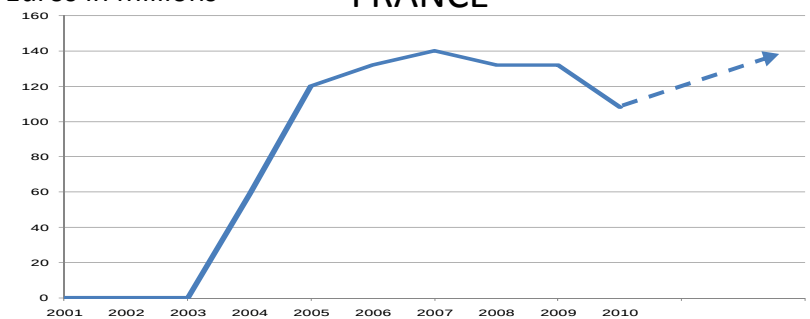
Euros in millions

EUROPEAN COMMISSION



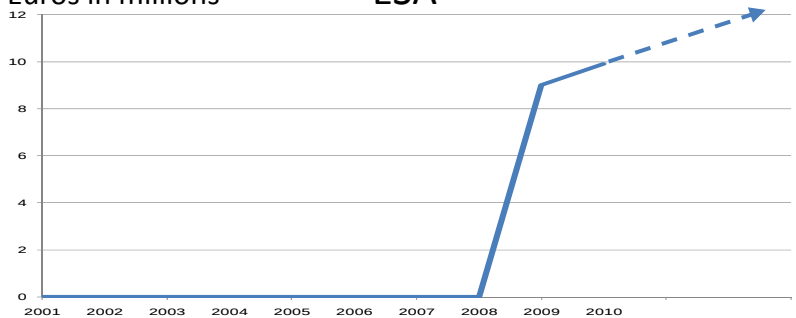
Euros in millions

FRANCE



Euros in millions

ESA



Source: Euroconsult

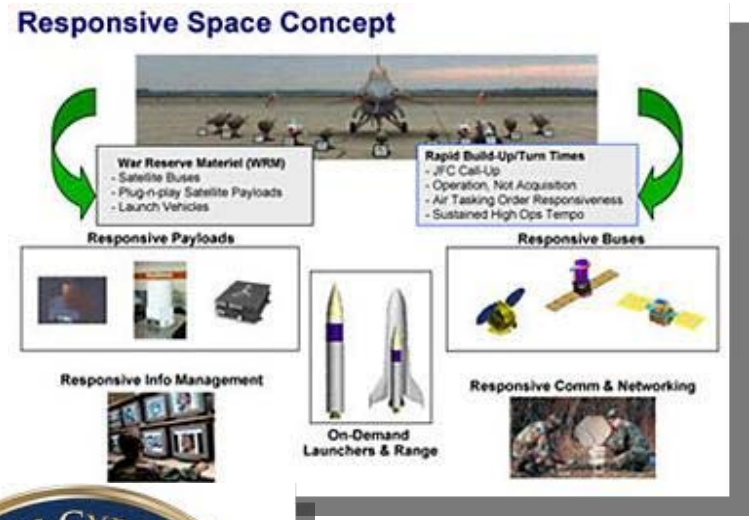
United States

- Sees freedom of action in Space is as important to the US as air power and sea power
- Heavily reliant on integrated (vulnerable) Space capabilities
  - R&D to keep the capability (not necessarily the asset) – ORS, SBIRS, SBSS, F6
  - R&D to deny capabilities of those willing to deny the freedom of Space for the X-37B, ABL
  - A leader in collision prevention – joint NASA & DoD R&D efforts to mitigate and remove Space debris
  - Seeking code of conduct for Space-faring nations
  - Seeking cost-effective and innovative system concepts for the removal of orbital debris

> "Freedom of action in Space is as important to the United States as air power and sea power."
>
> *US National Space Policy, 2006*

Capabilities

- Space Situational Awareness:
  - Space Surveillance Network
  - Space-Based Surveillance Network
- Operationally Responsive Space, F6, X-37B
- Early warning (Space Based Infrared System)
- Airborne Laser and Space-based lasers
- Fueling and servicing – Orbital Express
- Joint NASA/DARAP Space debris removal capabilities
- Cyber-capabilities and EW



EU / ESA

- EU is an emerging player in Space security
- Three Wiseman reports – Europe's security perception is incomplete without a component regarding Space security
- EC calling in 2004-5 for a Space security roadmap
- According to the Von Wogau report adopted by the European parliament, Europe should not contribute to the militarization and "weaponization" of Space
- EU policy emphasizes European independence in access to Space

"We send soldiers and civilian personnel into dangerous operations and we have to ensure that they get reliable and complete information and adequate equipment. To this end, the EU needs for the efficiency of its ESDP a full range of Space-based systems which will enable itself [EU] to watch, listen, communicate and navigate accurately."

Capabilities

- SSA – Europe developing autonomous SSA based on civilian (ESA) and military (EDA) requirements
- European responsive Space-based architecture for crisis management linking navigation, satellite communications and Earth observation, among others, into one coherent and user-driven system
- Necessity of secure satellite-supported communication for ESDP operations
- Galileo for autonomous ESDP operations

France

- France opposes the transformation of Space into a new battlefield
- France declared no intentions to deploy weapons in Space
- France invests in various satellite applications: communication, EO, SIGINT, ELINT, and Space debris

"France will make a major effort in the field of Space applications, in line with our national security strategy."

The French White Paper on defence and national security

Source: The French White Paper on defence and national security

Capabilities

- Major Player with ballistic capabilities (part of the NPT)
- Space situational awareness partnership with the US (2011)
- Emphasis towards SIGINT and ELINT capabilities (Essaim demonstrator) – for the analysis of the electro-magnetic environment of Earth's surface
- SPIRAEL early warning micro-satellite demonstrator
- Grave – Space security radar system by 2014

Russia

- Long legacy and activity in all Space disciplines
- Sees US development in Space as an evidence for the growing military gap
- Sees Space as a potential for precision strike capabilities for strategic advantage
- Pursues Space debris mitigation
- Cyber-attack capabilities (Estonia, Georgia)

Capabilities

- R&D for Space debris mitigation – announced special orbital pod (2010) and Space interceptor
- Baikal reusable launch vehicle (minimizes debris)
- LEO surveillance system based on radars installed in Russia and neighboring countries
- GEO surveillance (early warning) with Okno system deployed in 1999
- Proven kinetic ASAT capabilities
- Ground laser for distance measurement for SSN

China

- Weaponization of Space is an inevitable development
- PLA recognizes the importance of Space for achieving information dominance
- PLA maintains a strong R&D focus on counter-Space

"Competition between military forces is developing towards the sky and Space […] This development is a historical inevitability and cannot be undone […] The militarization of the sky and Space is a challenge to the peace of mankind […] Only if you have strong power can you protect and safeguard peace […] [we] must forge a sword and a shield capable of winning peace."

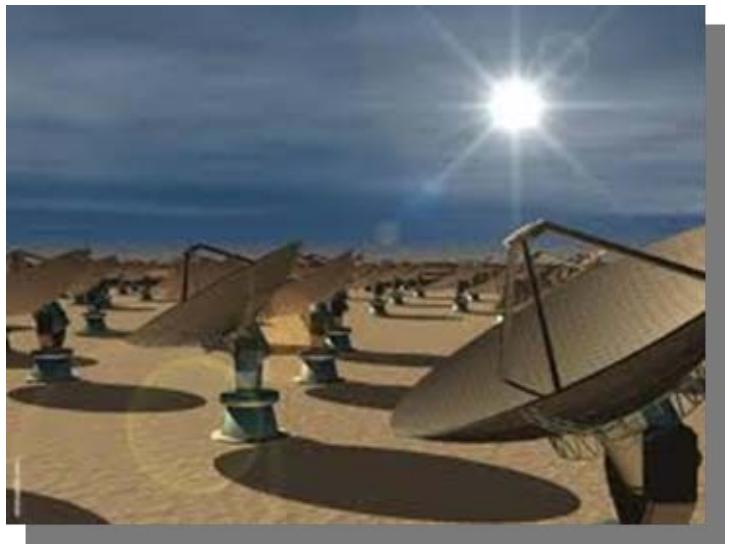
China's airforce chief General Xu Qiliang, 2009

Capabilities

- Among the most dominant China's ASAT capabilities are:
  - Kinetic weapons
  - Directed energy weapons such as lasers, HPM, EMP under development
  - Involvement in Space security shown through laser blinding in 2006 and ASAT test in 2007
- Increasingly sophisticated jamming systems and anti-satellite (ASAT) weapons:
  - Coordinated use of CNO, electronic warfare (EW), and kinetic strikes
  - Jam-proof satellite (sinsosat 2)
  - Dedicated computer network attack and exploitation units
- Proven Laser blinding capabilities (2006)
- Proven kinetic ASAT capabilities (2007)

Iran

- Desire to be Middle-East's Space power by 2020
- First satellite launched in 2009 (26 Kg.)
- Limited launch vehicle (LEO) capabilities (Safir 2)
- A "leader" in satellite TV jamming (policy):
  - Long jamming history (1997-2011)
  - UL Arrays – indications for a coordinated array of UL jammers jamming anti-regime broadcasts (VOA, BBC, opposition TV)
  - DL "smart Jamming" - indications of unprecedented deployment of 300 DL jammers
  - Recently, Iran set up a cyber pre-emptive action unit



Conclusions

- All major actors have ASAT capabilities
- **Nations are** concerned and thus **developing debris removal capabilities**
  - **All Space debris removal capabilities are potential ASAT**
  - **Jamming** and unintentional interferences are **a major threat**
  - Barriers to entry are low, hard to detect therefore hard to deter
  - If not addressed, might cause financial /operational damages
- **The cyber-threat is real**
  - Cyber-attacks are likely to be the new ASAT threat to old systems
  - Easier to attack ground Space systems than assets in Space

United Nations Institute for Disarmament Research
Institut des Nations Unies pour la recherche sur le désarmement

Thank you!

Contact us at:

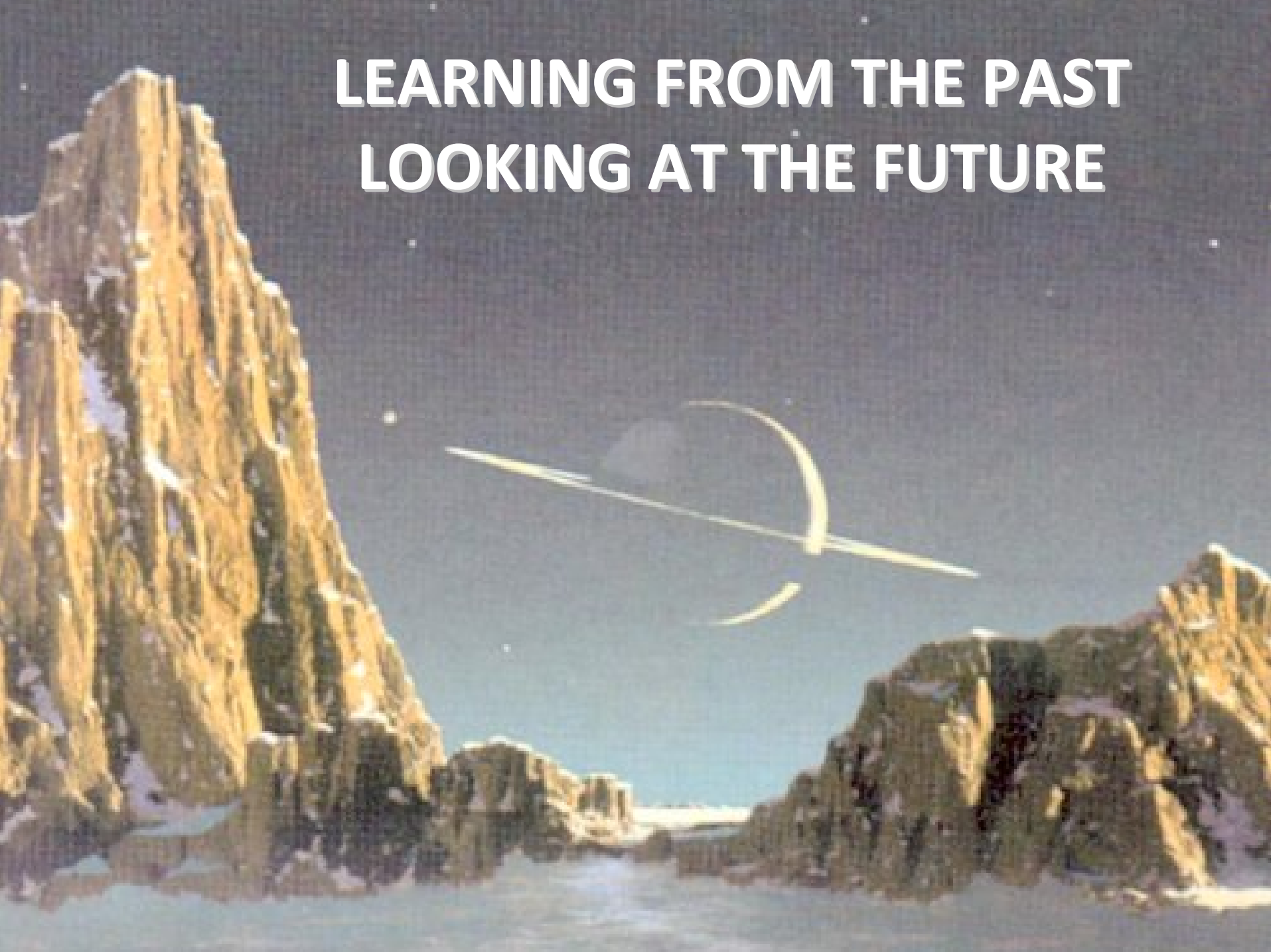
Tal Dekel: Tal@TalDekel.com

Ram Levi: RamLevi@tau.ac.il

http://www.sectech.tau.ac.il

Yuval Ne'eman Workshop for
Science, Technology
and Security
Tel Aviv University

TEL AVIV UNIVERSITY


LEARNING FROM THE PAST
LOOKING AT THE FUTURE

Source: http://www.Spacenews.com/images/032111IntelsatMDA02.jpg

NextSat, photographed by ASTRO as the pair flew in formation on May 5, 2007

Source : NASA,

Interference Report Sent to Iran

Annex 1 – Summary of the interference reports sent to the Islamic Republic of Iran or to the Radiocommunications Bureau

Annex	Date of occurrence of the interference	Date of sending the interference report	Reference[1]	Orbital position	Interfered-with satellite	Affected transponder	Satellite network	Sent to
3	27 May 2009	28 May 2009	09-0449/FV	13°E	HOT BIRD™ 8	#153	EUTELSAT 3-13E	Iran
4	30 May 2009	12 June 2009	09-0469/FV	13°E	HOT BIRD™ 8	#14	EUTELSAT EXB-13E	Iran
5	12 June 2009	17 June 2009	09-0486/AV	13°E	HOT BIRD™ 6	#130	EUTELSAT 3-13E	Iran
					HOT BIRD™ 8	#50	EUTELSAT B-13E	
6	27 July 2009	30 July 2009	09-0659/AV	13°E	HOT BIRD™ 8	#80	EUTELSAT B-13E	Via the Bureau
7	7 December 2009	9 December 2009	09-1091/AV	13°E	HOT BIRD™ 8	#155	EUTELSAT 3-13E	Iran
8	20 December 2009	22 December 2009	09-1143/AV	13°E	HOT BIRD™ 6	#130	EUTELSAT 3-13E	Via the Bureau
9	23 December 2009	30 December 2009	09-1154/AV	13°E	HOT BIRD™ 6	#131	EUTELSAT 3-13E	Via the Bureau
10	29 and 30 December 2009	6 January 2010	10-0014/AV	13°E	HOT BIRD™ 8	#76	EUTELSAT B-13E	Via the Bureau
11	18 January 2009	1 February 2010	10-0180/AV	13°E	HOT BIRD™ 8	#153	EUTELSAT 3-13E	Via the Bureau
12	19 January 2009	2 February 2010	10-0189/AV	13°E	HOT BIRD™ 8	#76	EUTELSAT B-13E	Via the Bureau
13	3 February 2010	8 February 2010	10-0211/AV	9°E	EUROBIRD™ 9A	#56	EUTELSAT B-9E	Via the Bureau
14	8 February 2010	10 February 2010	10-0231/AV	25.5°E	EUROBIRD™ 2	#158	EUTELSAT 3-25.5E	Via the Bureau
15 and 15bis	9 et 10 February 2010	18 February 2010	10-0260/AV	9°E	EUROBIRD™ 9A	#56	EUTELSAT B-9E	Via the Bureau
	10 et 11 February 2010			13°E	HOT BIRD™ 8	#75	EUTELSAT B-13E	
						#155	EUTELSAT 3-13E	
	9 February 2010			25.5°E	EUROBIRD™ 2	#158	EUTELSAT 3-25.5E	
16 and 16bis	12 February 2010	18 February 2010	10-0261/AV	13°E	HOT BIRD™ 8	#155	EUTELSAT 3-13E	Via the Bureau
	16 February 2010			21.5°E	W6	B4	EUTELSAT 3-21.5E	

Source: ITU

Recent Space Security Incidents

2 ASAT tests

1 collision

1 laser blinding

1 fire in Ground Station

1 presumable cyber-attack

Some lost and found satellites

Hundreds events of jamming

Potential ASAT capabilities

A capability, developed for peaceful purposes, that can be easily modified to an ASAT capability

Space Plane (X-37B)

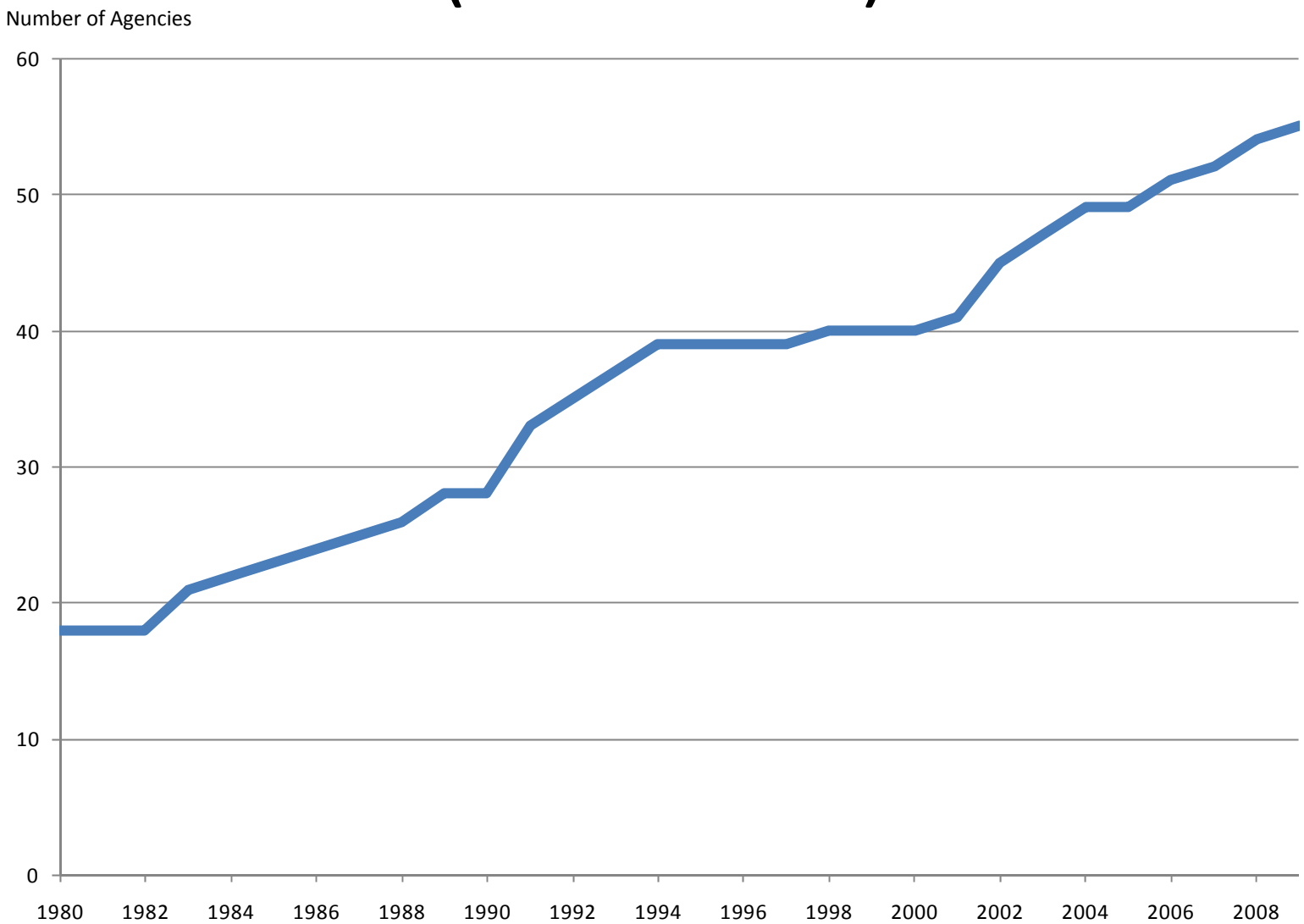
Satellite servicing

Jamming

Lasers

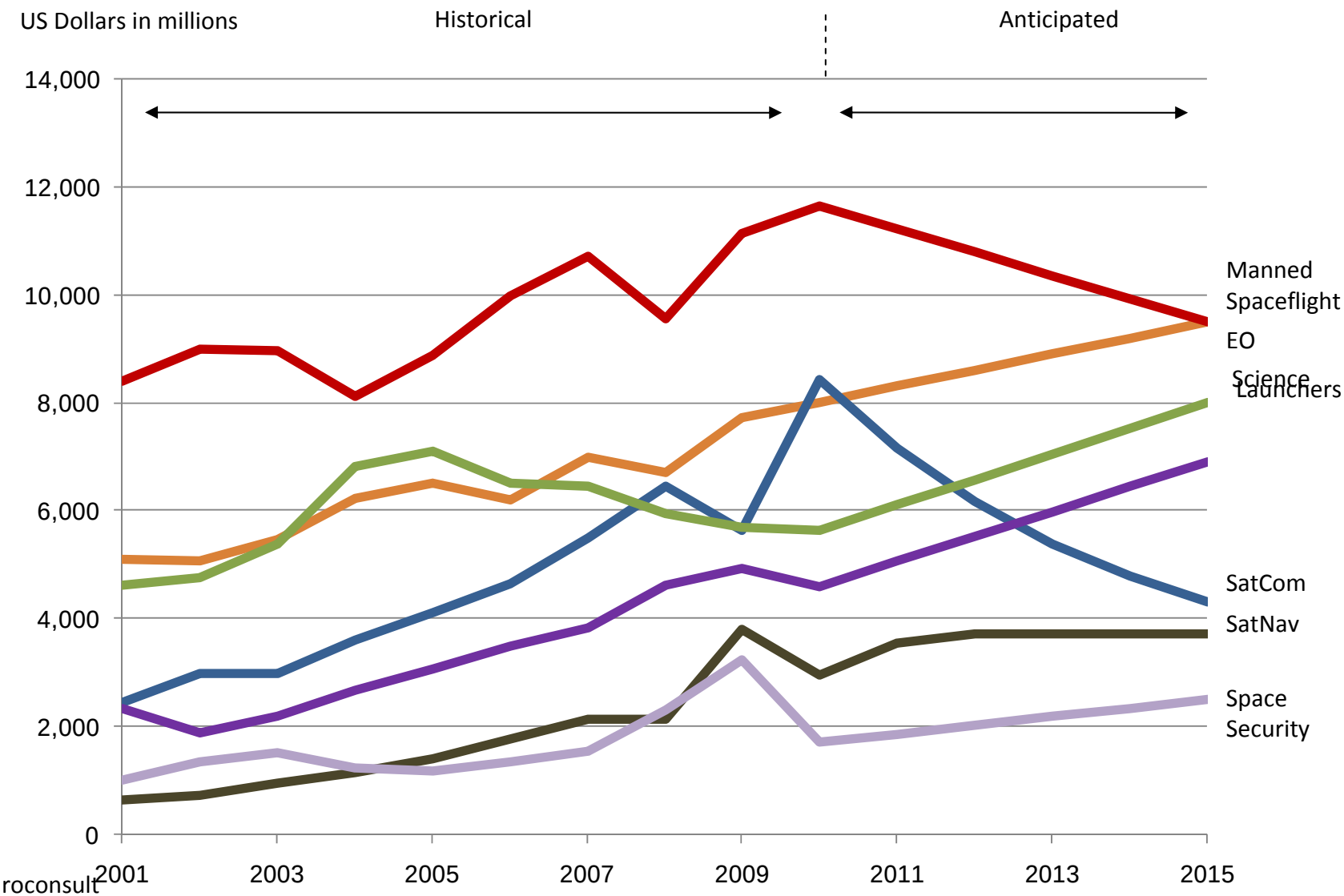
Cyber threats

Number of Space agencies worldwide (1980-2009)



Source: Euroconsult

World Government Expenditures Evolution by Application (2001-2020)



Source: Euroconsult