RAAKS 2017

New Risks, Unknowns and opportunities

Denis Bensoussan
2 March 2017

beazley

- **Space becoming Earth-like:** *Congested, Contested and Competed*
- New playground for the **information war and power games**
- Emerging risks environment is growing **more diverse and threatening**
- **New, mutating risks** confronting satellites
  - ✓ Disruptions of traditional space paradigms / business models
  - ✓ Space cyber risks
  - ✓ Space environment threats: space weather, space traffic, weaponisation…

- **Technologies and technical solutions while progressing appears insufficient** to deal with and mitigate alone the entire range of current and future threats
- **Sudden / high frequency technology introduction** could be a problem

Horizon 2020: New launch vehicles everywhere

- Current lineup

Vehicle	Ariane 5	Atlas V	Delta IV Medium	Dnepr M	Falcon 9	Proton M	Rockot	Soyuz 2	Zenit 3SL
Country	Europe	USA	USA	Russia	USA	Russia	Russia	Russia	Multinational
LEO kg (lbs)	17,250 (37,950)	9,800-29,400 (21,600-64,820)	8,120 (17,885)	4,100 (9,030)	10,450 (22,990)	21,000 (46,305)	1,850 (4,075)	7,800 (17,100)	15,246 (33.611)
GTO kg (lbs)	10,500 (23,127)	4,750-13,000 (10,470-28,660)	4,210 (9,273)	--	4,680 (10,296)	5,500 (12,125)	--	1,700 (3,800)	6,100 (13,448)

Active Commercial Launch Vehicles

Federal Aviation Administration

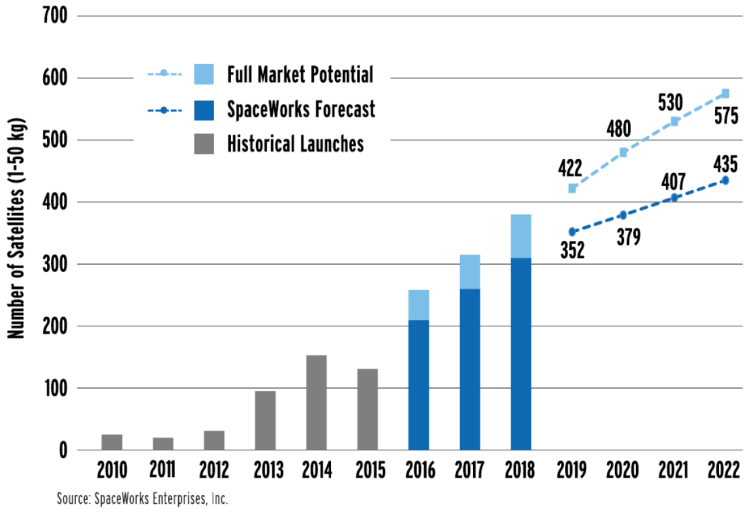
- New lineup

Launch vehicles reliability / availability an “industry hazard”?

Smallsats and Constellations – Old Space and New Space

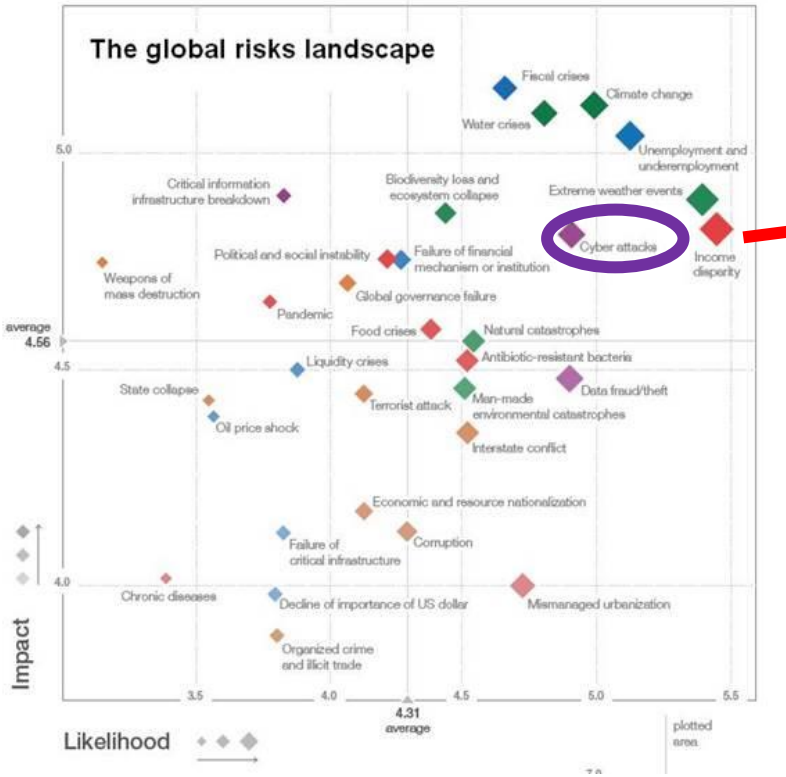
Nano/microsatellite launch history and forecast

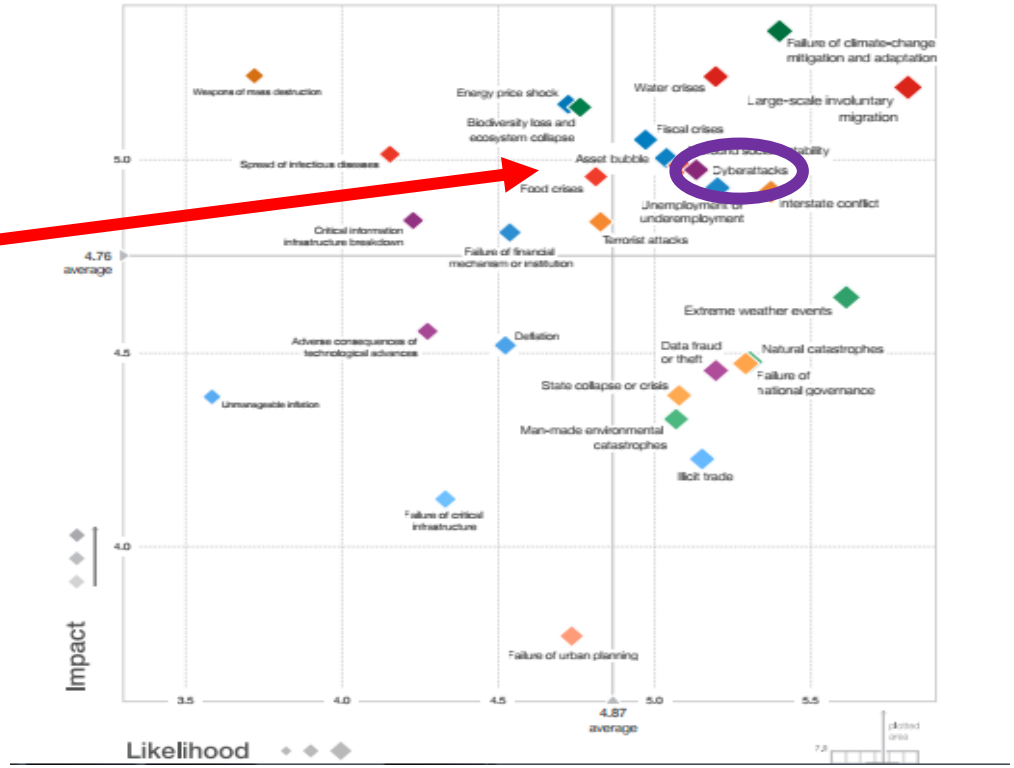
Projections based on announced and future plans of developers and programs indicate as many as 3,000 nano/microsatellites will require a launch from 2016 through 2022.



Source: SpaceWorks Enterprises, Inc.

- Among current and future threats, **cyber risks has increasingly captured a prominent role**
- Cyber attack risk now considered **more severe and more likely**





beazley

- **Satellite global, systemic risk nature** due to society's **ever increasing reliance** on satellite technologies make them part of the **critical digital infrastructure** and as such vulnerable to **ever increasing cyber attack opportunities**
- Paradox:
  - ✓ Frequency of cyber attack on satellites increasing?

List of reported events satellite hacks / excluding jamming

Year	Satellite	Application	Type of attack	Damage
1998	ROSAT	Science - Deep space radar observation	TT&C - Imager oriented toward Sun	Total loss
1999	SKYNET	Military communication	TT&C - Communication/ransom	Service interruption
2003	Unknown	NASA AMES Center Supercomputing	Downtime	unknown
2005	INTELSAT	Communication	Pirated use of satellite	Service corruption/interruption
2007	LANDSAT 7	NASA Earth optical observation	TT&C	12mins of interference
2008	TERRA EOS AM-1	NASA Earth optical observation	TT&C	2mins of interference
2008	LANDSAT 7	NASA Earth optical observation	TT&C	12mins of interference
2008	TERRA EOS AM-1	NASA Earth optical observation	TT&C	9mins of interference
2014-2015	Unknown	NOAA	Data breach / theft - 10 security inci	Service interruption

- But lack of documented events seems to lead to a **false sense of security**: *little seems to be happening, little is likely to happen…*

Satellite TT&C hack

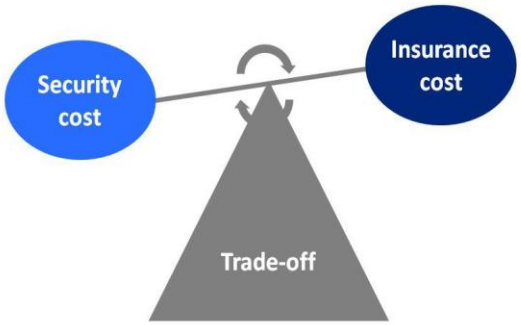
- Aim is **temporary or permanent physical control and/or destruction** of satellite
- **High technical challenges but far from impossible** (VSAT, VPN, ground stations, SCADA vulnerabilities)
- Few reported / documented events
- **Probability low / severity potentially catastrophic**
- Attacks probably not driven by commercial intention, greed…but **political in nature with the direct or implicit support of States**

Data breach attacks

- Obtain confidential information, competitive advantage, create disruption, incur financial damages
- Skills and knowledge more accessible
- Frequency and scope increasing
- Probability increasing / severity variable depending of type of attacks
- Attacks more likely to be driven by direct or indirect financial gain…but could also be political in nature

Cyber risks for Satellites – Challenges and Opportunities

Security vs Insurance



- Maximum Probable Loss
- Contractual Exposure
- Risk Appetite
- Budget
- Insurable risks
- Market limitations
- Peer Purchasing
- Regulatory Compliance

- Finding the **correct balance depends on technological and risk assessment / management as technical solutions alone are insufficient:** quantify the true exposure (knowns / unknowns risks) and uncover the areas where unknown risks could have the largest impact
- Insurance professionals shall contribute and provide the **necessary back-up and gap-filler solutions** by enabling **relevant, comprehensive and affordable transfer of risks to insurance**

  1. Clarification of **space damage insurance policies** and exclusion regime

  2. Development of **space cyber first party and third party liability comprehensive coverages** including systematic business interruption

  3. **Loss of revenues** and **Space War / Terrorism** cyber damage and liability coverages

- Insurers shall **encourage and incentivize security-conscious operators** applying best security practices

beazley

Space 3Cs Challenge - Congested, Contested, Competitive

- Safety, security and long term sustainability of space systems.

  ✓In terms of security, States need **to protect space assets from interference and prevent the escalation of hostilities in space**.

  ✓In terms of sustainability, we need to ensure that both **orbits and radiofrequency spectrum are managed effectively**, avoiding harmful interference between systems, thereby avoiding the threat to the long term viability of space based systems.

- Technologically disruptive systems: Operators of new systems need to demonstrate they are **good neighbours**, providing appropriate levels of transparency and reassurance to those that share their investment in the space domain

beazley

CONCLUSION

- The primary deterrents to enhanced satellite security are **denial of vulnerabilities, fear of increased costs and/or decreased productivity**
- Costs of cybersecurity are indeed high and rising but so are the consequences to overlook the risks
- If the industry is not able to meet these costs, **vulnerabilities will only increase further**
- **Security vs costs is not a safe, sustainable trade-off**
- Finally **development of a versatile, flexible and cooperative space security ecosystem** through information / knowledge sharing within a community of willing and competent space industry stakeholders is **highly required**

Thank you.

Denis Bensoussan
Head of Space Risks – Beazley

Mr Bensoussan joined Beazley in March 2014 from Hiscox, where, as senior underwriter for space risks, he managed the global satellite risks account.

Prior to joining Hiscox in 2006, Mr Bensoussan worked in the aerospace department of Marsh Aviation as well as aerospace-related positions at the European Space Agency, the United Nations and the European Commission. With more than 16 years' experience in the aerospace industry, Mr Bensoussan possesses deep knowledge of the risk exposures satellite and launch vehicle operators and manufacturers confront.

Mr Bensoussan obtained a space systems engineering training from Southampton University and Supaero Paris and holds a post-graduate degree in Air & Space Law along with degrees in International Law.

beazley