Vör-TechX

GNOSIS - SSA
Data Management
Workshop

Chris Jones

# Space Sector Security Challenges in a Complex World

Critical Infrastructure:

- Space was designated by CPNI as Critical National Infrastructure (CNI) in February 2015.
- This imposes additional requirements for resilience on the sector.

Threats:

- Counterspace operations
- Proliferation
- CoTS, IoT / IoST
- Hacking

Response:

- Regulation
- Countermeasures

# Critical Infrastructure: https://www.cpni.gov.uk/critical-national-infrastructure-0

In the UK, there are 13 national infrastructure sectors:







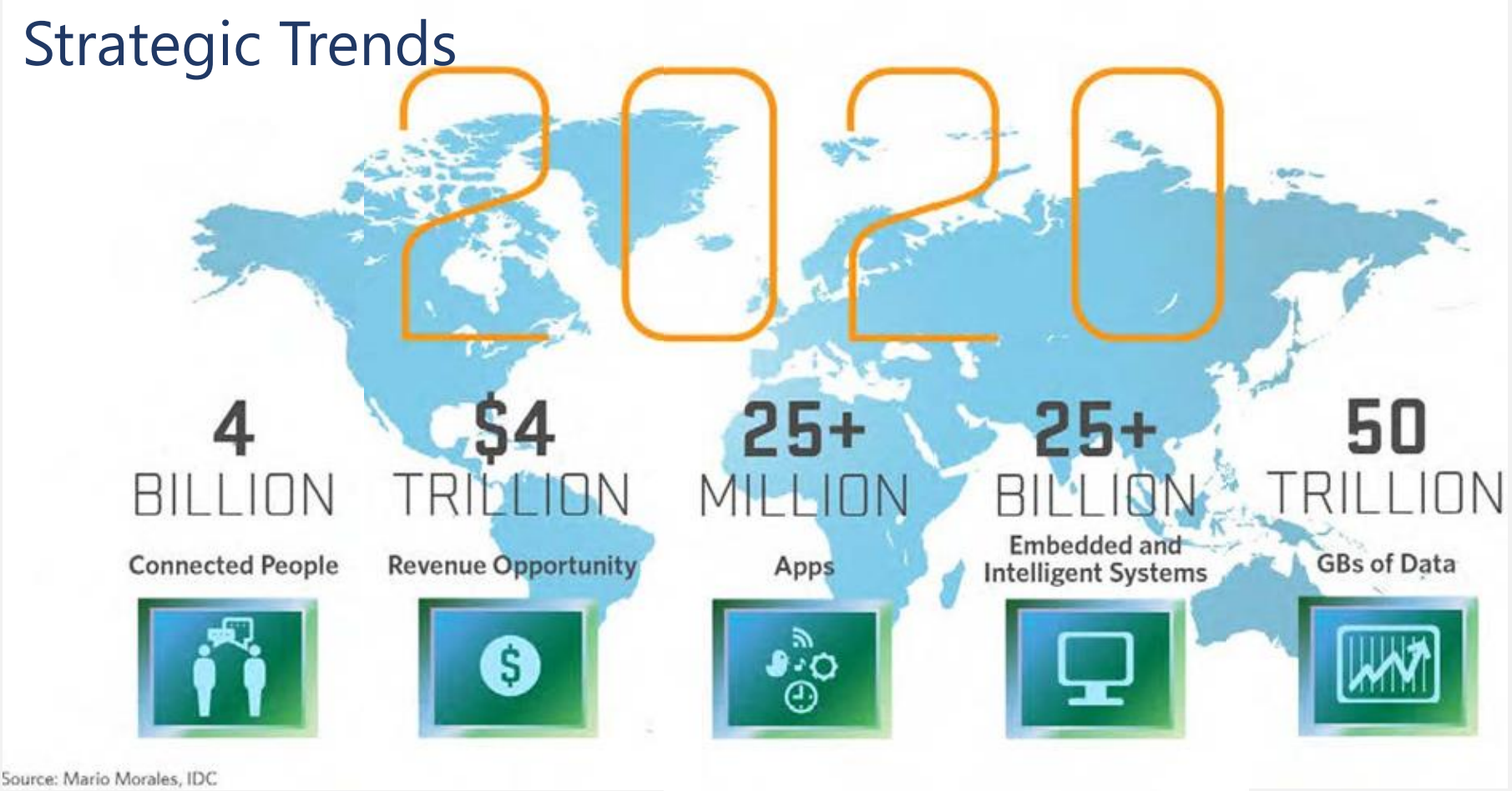



GOV.UK

Vör-TechX

Vör-TechX

# Strategic Trends



# Threats:

Counterspace operations

- Offensive counterspace operations involve the use of lethal or non-lethal means to neutralize an adversary's space systems or the information they provide.
- Deception--manipulate, distort or falsify information
- Disruption--temporary impairment of utility
- Denial--temporary elimination of utility
- Degradation--permanent impairment of utility
- Destruction--permanent elimination of utility

# Threats:

Proliferation

- With the proliferation of satellite warning data, denial and deception has become a highly effective means of attack.
- Proliferation in the use of micro/nanosatellites continues to expand the attack surface
- The increasing number of manufacturers involved in building the various components increase system vulnerabilities as hackers have multiple opportunities to infiltrate the system.
- The proliferation of ballistic missile and space technology has made it easier to develop direct ascent antisatellite weapons

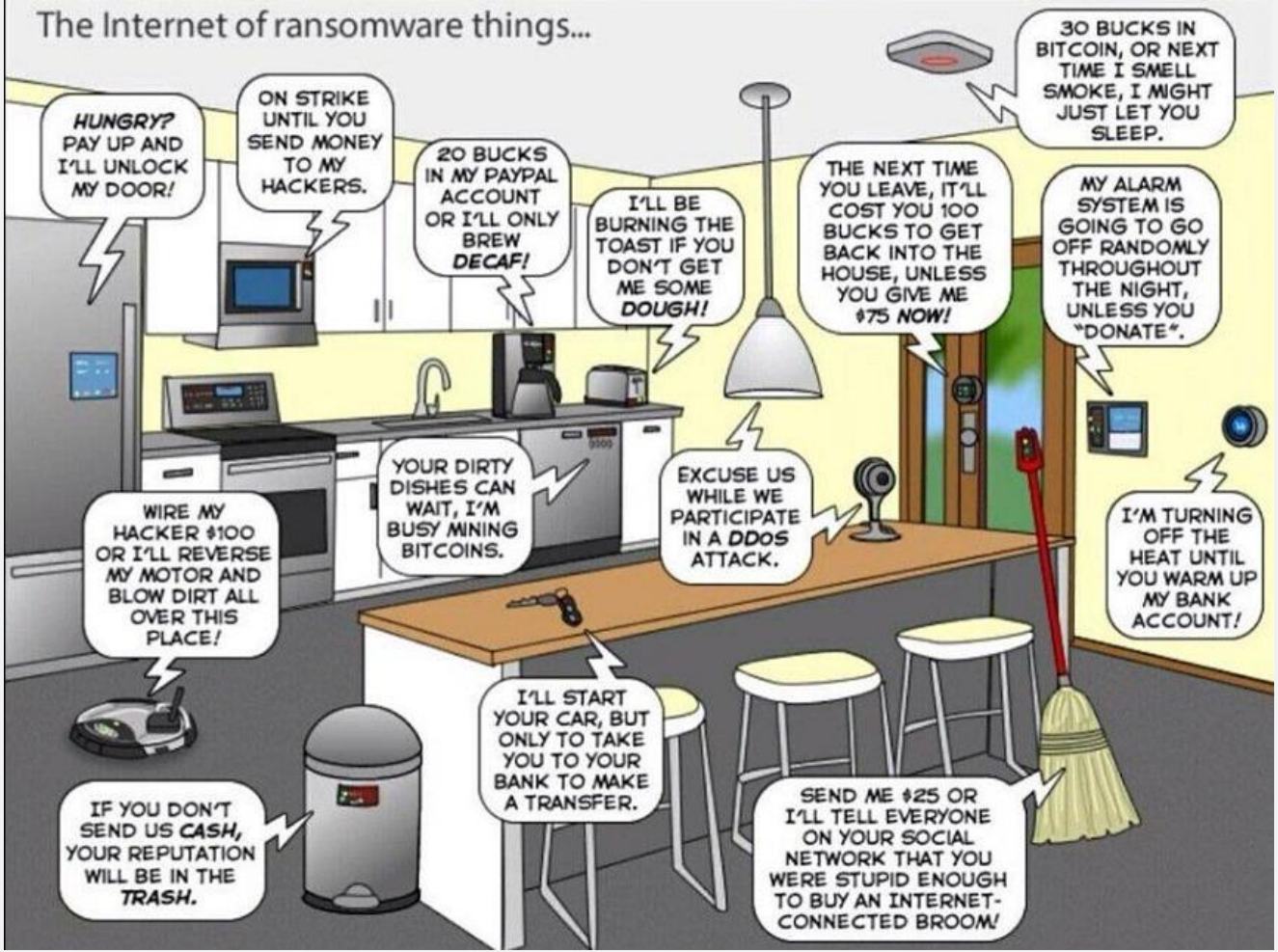
# Threats:

CotS, IoT/IoST

- As more CubeSat constellations are deployed, we get closer to an Internet of Space Things
- An increasing number of satellites, particularly CubeSats, use Commercial off-the-shelf technology to keep costs low, speed up development simplify production.
- This makes it tempting for companies to ignore cybersecurity.
- Many of the CotS components have ‘known’ vulnerabilities.
- Many of the CotS components draw on open-source technology.
- Open-source technology is frequently vulnerable to ‘back-door’ hacks.

# Threats:

IoT / IoST



# Threats:

Hacking

- Satellites, like so much critical infrastructure, have many vectors of vulnerability. The most obvious is the simple ‘Man-in-the-middle’ attack.
- Hacking even sophisticated satellites can potentially be achieved by simply sending a cyber attack using relatively cheap antennas whilst the satellite is overhead.
- Ground stations are as vulnerable as any other business to cyber attacks; Phishing, MitM, Ransom ware, DDoS etc…
- There is a long history of cyber attacks against space assets so non of this is exactly new.

- Fast forward to the Space Security Challenge August 2020: Hack-A-Sat
- Governments are now taking the threat of cyber warfare more seriously, but…

# Response:

## Regulation

Complex and extended supply chains with multiple parties at each stage inevitably means identifying who bears responsibility and liability for cyber breaches is near impossible.

We need legislation that requires satellites manufacturers to develop a common cybersecurity architecture including:

- Enforcing new foreign Cyber laws
- Voicing an interest in small satellite manufacturers
- Exploring controls to prevent known attack vectors

# Response:

## Advanced Threat Intelligence

We are seeing the growth of Heuristic analysis, AI and machine learning to help over burdened IT departments.
This brings an understanding of entity behaviours while also automatically adjusting to known and approved changes within an environment.
There is a slow increase in the use of encrypted data streams, but the legacy issues remain.
All this is starting to provide relevant recommendations and a significant reduction in false positive fatigue.

# Going forward

- What are the takeaways?
  - All these are an issue right now.
  - They are the tip of the iceberg.
- We live and work in a rapidly evolving world of threat and counter measures. The enemy doesn't stand still and neither must we.
- The space sector needs to consider new thinking and innovative approaches to security to keep pace and prosper in the digital world.
- We need a joined up security stance is a comprehensive but also designed with the future in mind.

# Thank you for your time.


- Chis Jones
- chris.jones@vor-techx.co.uk
- 07940876955