University of
South Australia

Space Systems Security: Frameworks and Standards

Professor Jill Slay

Background

- Space security is well-articulated in political, legal, and social sciences literature
- Engineering, science, and technology space security literature is limited and disjointed
- Traditionally space security has been viewed as a military domain due to the Cold War
- More recently this view has expanded to include three dimensions of space security:
  1. security in space (i.e. protecting space systems)
  2. space for security (i.e. military space operations and satellite imagery)
  3. security from space (i.e. protecting Earth from space-based threats).
- This presentation focuses on the first dimension, herein called ***Space Systems Security***

Research Overview

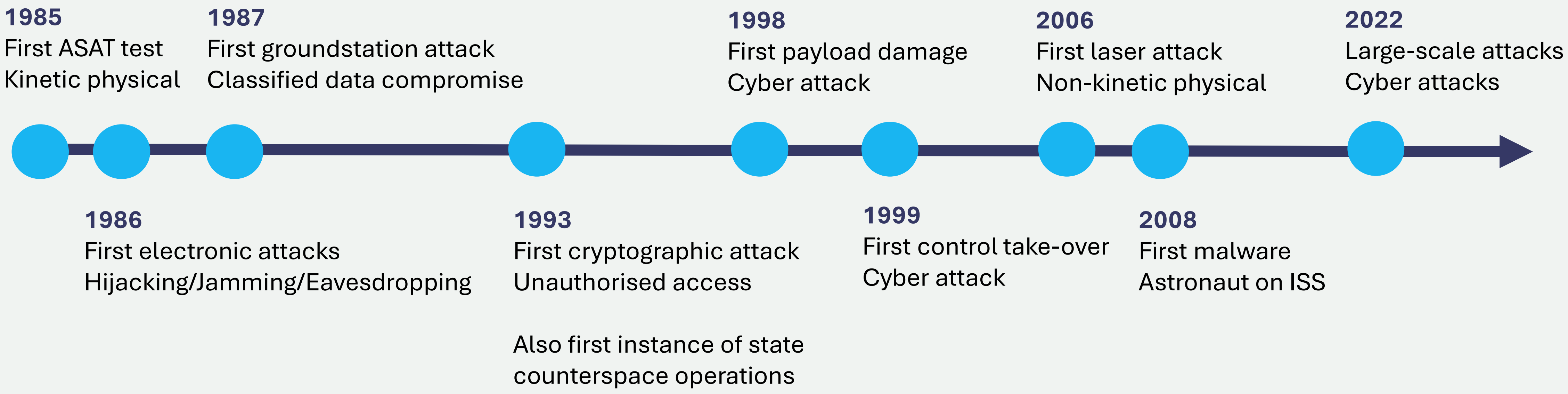
- We wanted to develop a framework for measuring resilience in space systems
- But found the need to come back down to the basics first which was security
- Our research focuses on defining and modelling two key concepts:
    - Space Systems **Security**
    - Space Systems **Resilience**
- We involved two dozen academics and professionals from 7 different countries in Delphi Style research which underpins this presentation
- This presentation focuses on security

Space Context

- Space is the next frontier for human civilisation
- Humans rely on space infrastructure for the advancement of technologies here on earth
- New industries forming, such as extra-terrestrial tourism, space mining, and more
- There are four key trends that make space systems particularly vulnerable to attack:
  1. Increasing technological complexity
  2. Increasing operational capability
  3. Increasingly hostile threat environment
  4. Increasing reliance on space infrastructure.

Notable Past Events

There have been well over 100 significant satellite attacks since the launch of Sputnik.



1985
First ASAT test
Kinetic physical

1986
First electronic attacks
Hijacking/Jamming/Eavesdropping

1987
First groundstation attack
Classified data compromise

1993
First cryptographic attack
Unauthorised access

Also first instance of state
counterspace operations

1998
First payload damage
Cyber attack

1999
First control take-over
Cyber attack

2006
First laser attack
Non-kinetic physical

2008
First malware
Astronaut on ISS

2022
Large-scale attacks
Cyber attacks

Space Infrastructure

Critical Space Infrastructure (CSI) can be broken down into five key categories:

1. Remote Sensing
2. Communications
3. Meteorological
4. Global Navigation Satellite Systems (GNSS)
5. Administrative and Legislative Frameworks.

The technologies covered above are predominantly artificial satellites, but may also include space stations, rovers and vehicles, rockets, space probes, ground stations, and terrestrial communications links.

Georgescu, A., Gheorghe, A.V., Piso, M., Katina, P.F., 2019. Critical Space Infrastructures: Risk, Resilience and Complexity, Topics in Safety, Risk, Reliability and Quality. Springer, Switzerland.

CSI #1 Remote Sensing

- Provide passive or active collection of data without making physical contact
  - systems that conduct surveillance
  - scientific monitoring
  - information gathering for terrain mapping and military reconnaissance

- If attacked, could cause sensitive data compromise, corruption, or loss

- Most vulnerable to laser and electronic attacks due to the need for electromagnetic penetration to achieve their primary function

CSI #2 Communications

- Provide global telecommunications coverage
  - Aviation and air traffic control
  - Military coordination
  - Internet and other long-distance connections

- If attacked, could result in grounded aircraft, loss of communications, and data compromise

- Most vulnerable to jamming, spoofing, and eavesdropping attacks

CSI #3 Meteorological

- Transmit photos and meteorological data to Earth
  - Climate and weather monitoring
  - Natural disaster prediction
  - Human activity monitoring
  - Geospatial imagery

- If attacked, could result in unreliable intelligence, compromised data, loss of global visibility

- There is yet to be any published research specific to meteorological satellite vulnerabilities
- Due to their simple anatomy they likely share general vulnerabilities to other satellite systems

CSI #4 GNSS

- Provides navigation, positioning, and timing information
  - Global Positioning System (GPS)
  - High-reliability timing applications (e.g. for critical infrastructure)
  - Relied on by terrestrial technologies such as the electric grid and guided weapons systems

- If attacked, could result in far-reaching and catastrophic consequences, including loss of life

- Most vulnerable to jamming and spoofing attacks

CSI #5 Administrative & Legal

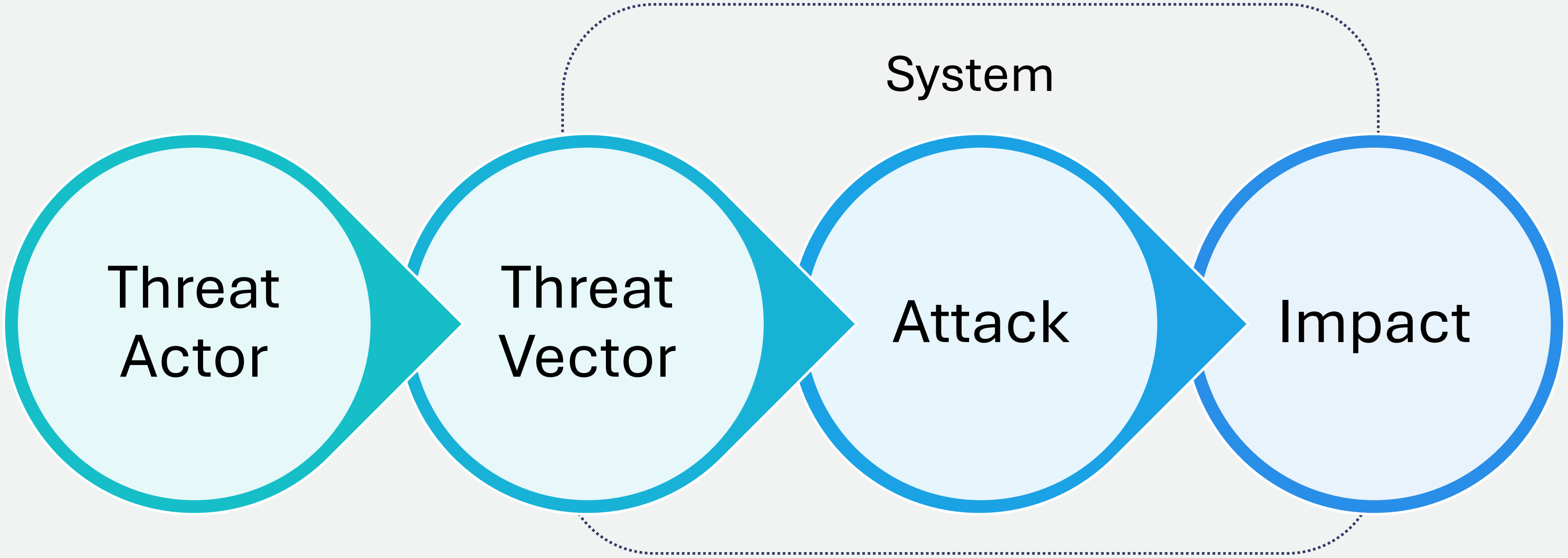
- Supports the security of other CSI by aiding:
  - Pre-emptive security efforts
  - Data collection and retention standards
  - Post-compromise forensics
  - Attribution, prosecution, and retaliation

- Notoriously complex due to international significance and lack of any divisible territory

- Without adequate administrative and legal frameworks CSI remain increasingly vulnerable.
  - Recent changes to the SOCI Act aim to better protect Australian space technologies.
  - The Woomera Manual project articulates international law for military SpaceOps

Threats

- Space systems operate in one of the most naturally hostile environments known to man
- They also face unique challenges that don't commonly apply to terrestrial infrastructure
- Our research focuses on malicious threats



Threat Actors

- A formal threat actor taxonomy is yet to emerge in the literature, but in general includes:

Threat Actor	Capability	Example Intent / Motive
State	High	Space superiority
Terrorist	Low	Intimidate population
Criminal	Moderate	Extort money
Hacktivist	Low	Awareness of cause
Individual	Low	Notoriety

Threat Vectors

- Threat vectors need to be assessed in detail on a case-by-case basis

- In general, there are four common attack surfaces for deployed space systems:
  - inputs (e.g. sensors and RF antennae)
  - outputs (e.g. telemetry transmitters)
  - internal components (e.g. power system)
  - computing (e.g. onboard processing).

- Each of these components can be accessed via a myriad of different threat vectors, such as through ground segments, supply chains, unsecured communications links, and countless other avenues.

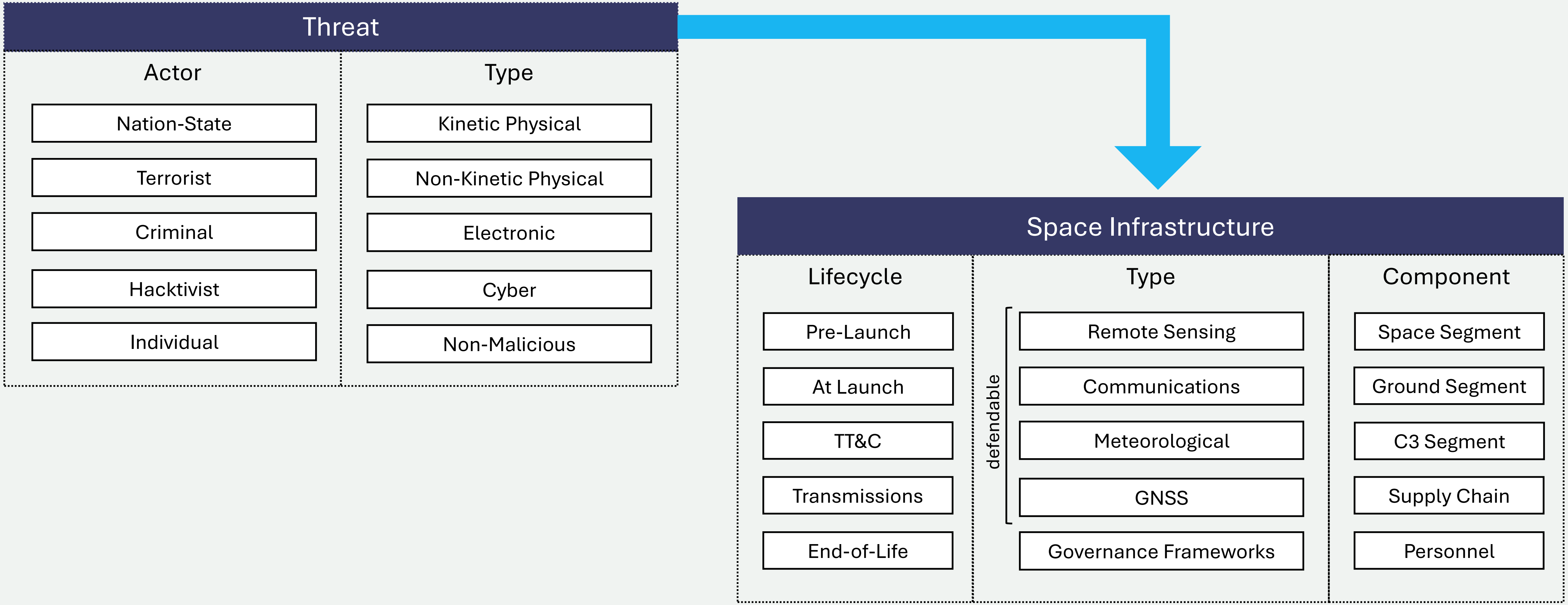
Attack Types

C = Confidentiality
I = Integrity
A = Availability

Targeted attacks to space infrastructure include:

Kinetic Physical Tangible physical threats **Aim**: Permanently impact A **Example**: ASAT missiles	**Non-Kinetic Physical** Intangible physical threats **Aim**: Permanently impact A **Example**: lasers, EMP weapons
Electronic RF-based threats **Aim**: Temporarily impact C, I, or A **Example**: RF jamming or spoofing	**Cyber** Code-based threats **Aim**: Temporarily or permanently impact C, I, or A **Example**: ransomware, code injection

Piecing it all together



Threat

Actor	Type
Nation-State	Kinetic Physical
Terrorist	Non-Kinetic Physical
Criminal	Electronic
Hacktivist	Cyber
Individual	Non-Malicious

Space Infrastructure

Lifecycle	Type	Component
Pre-Launch	Remote Sensing	Space Segment
At Launch	Communications	Ground Segment
TT&C	Meteorological	C3 Segment
Transmissions	GNSS	Supply Chain
End-of-Life	Governance Frameworks	Personnel

Space Systems **Security** is...

> “the assurance of the **confidentiality**, **integrity**, and **availability** of a space system throughout its lifecycle, including all ground, communications, and space segments as well as the data, processes, and supply chains that support it.”

Outcome 2 – Space Systems Security Domain

We commenced the Delphi study with a preliminary knowledge domain mapping shown below:

VECTOR	Ground Segment					Space Platforms				
THREAT	Ground Station	Launchpad	Simulators / Emulators	Supply Chain	Personnel	Payload	Radio Link & Telemetry	Computing	Internal Comms	Onboard Sensors
Non-Malicious (e.g. solar flare)	Teleport Engineering / IT Security	Launchpad Engineering	Software Engineering	Business Continuity Planning	Occupational Health & Safety	Space Engineering	Telecomm. Engineering	Computer Engineering	Telecomm. / Materials Engineering	Electronics Engineering
Cyber (e.g. malware)	Cyber Operations	OT Security	Cyber Security / OT Security	Cyber 3PP / Supply Chain Security	Cyber IAM	OT Security	Cyber Operations	Cyber Engineering	Cyber Engineering	OT / IoT Security
Kinetic Physical (e.g. ASAT)	Building / Perimeter Security	Perimeter Security	Building Security	Business Continuity Planning	Protective Security	Military SpaceOps	Military SpaceOps	Military SpaceOps	Military SpaceOps	Military SpaceOps
Non-Kinetic Physical (e.g. EMP)	ECM	ECM	Emanations Security	Business Continuity	Security Training & Awareness	Space Engineering	Telecomm. Engineering	Materials Engineering	RF/Materials Engineering	RF/Electronics Engineering
Electronic (e.g. RF jamming)	Facility Emanations Security	Perimeter Emanations Security	Building Emanations Security	Business Continuity	Building Emanations Security	Telecomm / Materials Engineering	Telecomm / Materials Engineering	Telecomm / Materials Engineering	Telecomm / Materials Engineering	Telecomm / Materials Engineering

COSMOS^2 – Space Systems Security Domain

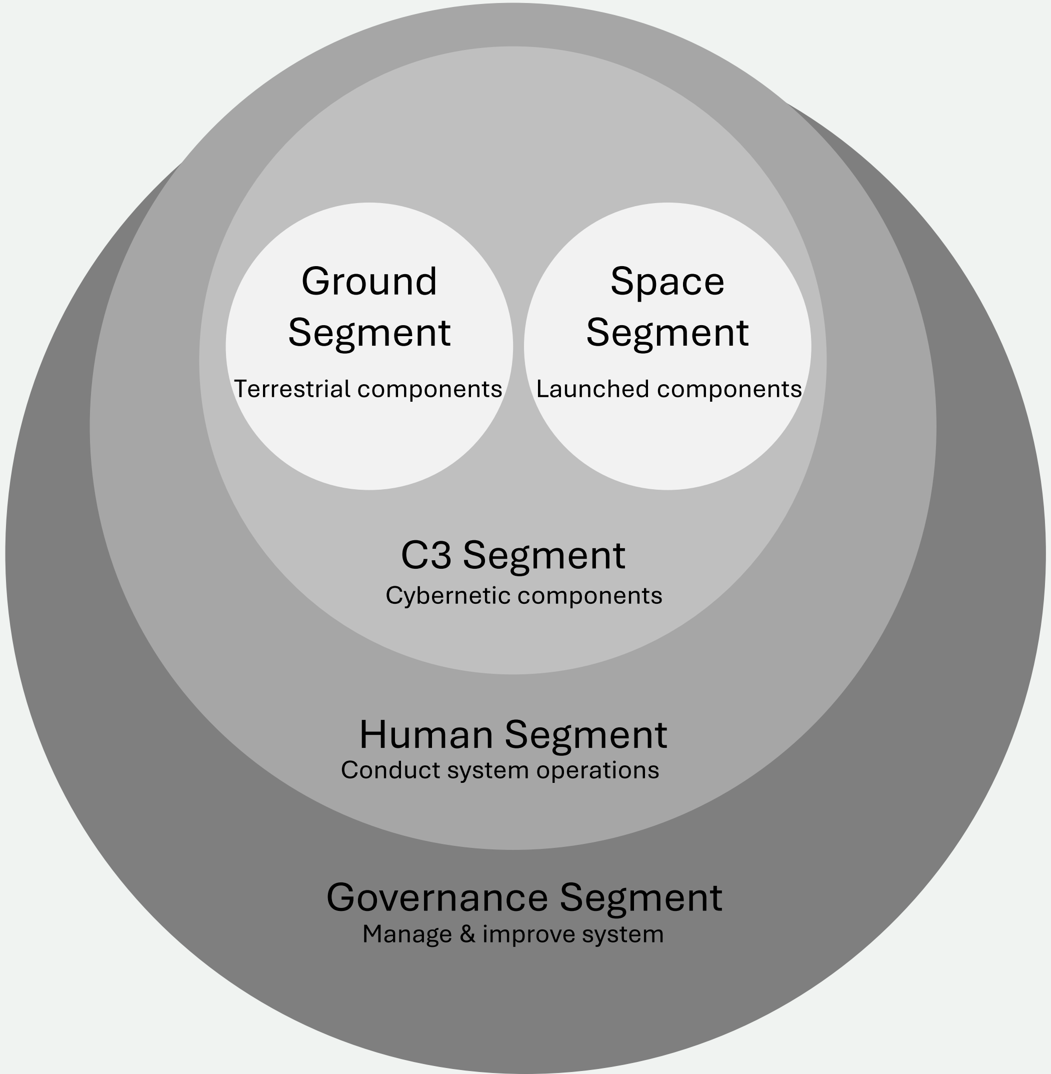
	Governance Segment	Human Segment	Ground Segment	Space Segment	C3 Segment
Non-Malicious	**Governance to assure against non-malicious adversities** through Business Continuity and Disaster Recovery Planning, Legal / Regulatory Compliance, V&V, Quality / Product Assurance	**Assurance of users and personnel against non-malicious adversities** through Security Training & Awareness, Legal / Regulatory Compliance, WHS, Human Factors Engineering, Safety Engineering, Security Culture	**Assurance of ground components against non-malicious adversities** through Debris / Celestial Monitoring and Reliability Engineering (Telecomm, Software, Aerospace, ICT)	**Assurance of space components against non-malicious adversities** through Human Factors, Safety, Materials and Reliability Engineering (Elec., Aero., Mech., Software, Electronics, Robotics)	**Assurance of C3 components against non-malicious adversities** through Data Management, Redundancy / Reliability Engineering (Telecomm., Software, ICT)
Cyber	**Governance to assure against cyber adversities** through Cyber GRC, Cyber Assurance/Testing, Supply Chain Security, Threat Intel., Cyber Law/Regulation	**Assurance of users and personnel against cyber adversities** through Cyber Training & Awareness, Identity and Access Management, Personnel Vetting, Security Monitoring, Data Classification	**Assurance of ground components against cyber adversities** through IT / OT/ IoT Security Engineering, Security Monitoring (e.g. SOC), and Cyber Incident Response	**Assurance of space components against cyber adversities** through OT/ IoT Security Engineering, Security Monitoring (e.g. IDS/IPS), Resilience Engineering (e.g. D4P2), Offensive Defence, Honeypot/Trap	**Assurance of C3 components against cyber adversities** through IT / OT / IoT Security, Secure Coding, Cryptography, Security Monitoring (e.g. IDS/IPS), Anti Malware, Redundancy Engineering, Integrity Checks, Data Classification
Electro-magnetic	**Governance to assure against electromagnetic adversities** through Electronic Assurance Testing, Threat Intelligence, and EW Law/Reg., Spectrum Regulation (e.g. ITU)	**Assurance of users and personnel against electromagnetic adversities** through Physical Security (e.g. perimeter, surveillance), Facility Compartmentalisation, Bug Sweeping, Cell Phone Lockers	**Assurance of ground components against electromagnetic adversities** through EMSEC / TEMPEST, ECM / EW, Physical Security (e.g. perimeter, surveillance)	**Assurance of space components against electromagnetic adversities** through EMSEC / TEMPEST, ECM, EW Counterspace Operations, Resilience Engineering (e.g. D4P2)	**Assurance of C3 components against electromagnetic adversities** through Redundancy Engineering, Integrity Checks, ECM / EW Protection, LPI/LPD waveforms, advanced signals processing, signature management
Kinetic	**Governance to assure against kinetic adversities** through Surveillance / Threat Intelligence, International Space Law / LOAC, Facility Compartmentalisation, Protective Security.	**Assurance of users and personnel against kinetic adversities** through Physical Security (e.g. safes / locks, building, perimeter, surveillance), Social Engineering Awareness Training	**Assurance of ground components against kinetic adversities** through Physical Security (e.g. safes / locks, building, perimeter, surveillance)	**Assurance of space components against kinetic adversities** through Counterspace Operations, Weapons, Space Monitoring, Resilience / Redundancy Engineering, Internal Scanning, Manoeuvrability, Spacecraft Hardening	**Assurance of C3 components against kinetic adversities** through Counterspace Operations, Monitoring, Resilience / Redundancy Engineering, Physical Hardening.

Governance Segment	R&D, Procurement & Supply Chain, Legal, Ethical & Compliance
Human Segment	Personnel, Users, Astronauts/Cosmonauts, Safety, Human Factors
Ground Segment	Teleport & Terminals, Space Traffic Management, Launch Facility / Vehicle, Simulators / Emulators, Manufacturing Facilities, Mission Control
Space Segment	Power System & Wiring, Propulsion System, Weapon System, Life Support Systems, Space Vehicles & Rovers
Communications, Control & Computing (C3) Segment	Sensors, Data (scientific, technical, positional, etc), Control Signalling, Radio Link & Telemetry, Computing, Software, Onboard Processing

Non-Malicious Adversities	Accidental, Environmental (space debris, radiation, interference, solar flares, scintillation).
Cyber Adversities	Code / Data Manipulation, Malware, Denial of Service, Hijacking, Spoofing, Eavesdropping, Cyber Warfare
Electromagnetic Adversities	Jamming, Lasers, Spoofing, Eavesdropping, EMP Weapons, Electronic Warfare, Directed Energy Weapons, Dazzling/Blinding
Kinetic Adversities	Physical Attacks (tampering, theft, etc), Missiles / ASATs, Deliberate Space Junk / Debris Fields, Orbital Threats, Nuclear Detonation

COSMOS^2

The segments in the table on the previous page can be understood to interact at a high-level as per below:



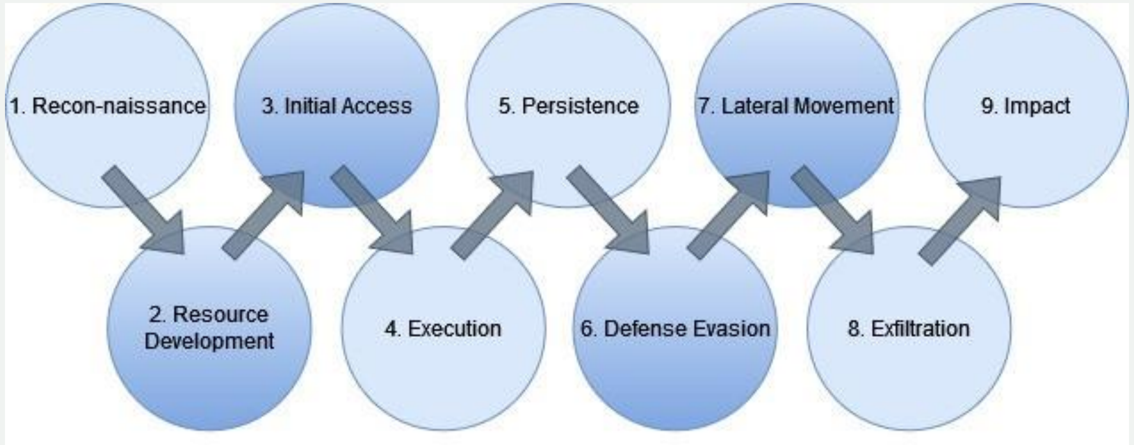
Why is this important now?

- New Space is shifting the focus from government to commercial interests
- Literature does not provide us with an adequate research agenda
- Each technological advancement introduces new vulnerabilities and impacts
    - system-on-a-chip avionics
    - self-optimizing autonomous systems
    - complex on-board satellite processing
    - autonomous satellite-to-satellite (S2S) communications
    - Increasingly complex payloads
- Cyber and electronic weapons are becoming more effective and accessible
- Increased reliance on space infrastructure
- Increased militarisation of space
- **These concepts help to assure critical space services in a high threat environment**

Other Frameworks - SPARTA

SPARTA was adapted from the MITRE ATT&CK framework. The latter provides a matrix of tactics and techniques for the security of enterprise systems .

The SPARTA framework consists of nine tactics as depicted below. The tactics define the typical steps of a malicious actor during the attack lifecycle on a space system. Each tactic consists of techniques which are the procedures for realizing the tactic.



It is recognised that the SPARTA framework needs much experience from the user before it can be applied across both space and cyber domains

https://sparta.aerospace.org/.

Other Frameworks - SPARTA

- *Reconnaissance* involves a malicious actor gathering information about the target system to aid in executing their attack. -- gathering spacecraft design information, spacecraft descriptors as well as gathering launch information, and eavesdropping communication between the spacecraft and the ground station

- *Resource Development*, malicious actors can acquire their resources (tools) by developing, purchasing, or renting them. Alternatively, they can use malware to compromise space systems

- During *Initial Access*, the malicious actor gains entry to the space system. Some of the techniques used by malicious actors to access a space system are compromising either the supply chain, payloads, or the ground system.

- When a malicious actor gains access to a space system, the next step is performing the actual attack which is the *Execution*.

- Through *Persistence*, threat actors strive to maintain their access to the space system to continue exploiting the space system. Techniques include identifying or injecting backdoors and using compromised valid credentials (i.e., user accounts) to maintain access.

- With *Defense Evasion* the malicious actor finds ways to elude security mechanisms (i.e., intrusion detection and/or intrusion prevention systems). The malicious actor may attempt disabling or modifying security software or interfering with downlink communication to prevent a satellite from sending data to the ground station or they can masquerade as a legitimate user.

- The malicious actor subsequently resorts to *Lateral Movement* where they attempt to move to different sub-systems and control the space system. They can use the payload on the satellite to access other sub-systems that communicate with the payload. Additionally, they can try to instruct a satellite through a crosslink with another satellite in order to compromise the satellite.

- The next tactic is *Exfiltration* which consists of techniques that a threat actor may use to steal data from the space system. They can replay the commands or payload data being sent to the ground station to compromise the space system. The malicious actor can eavesdrop on the communication between the satellite and the ground.

- The *Impact* caused by the malicious actors could temporarily disrupt the functionality of the space system or inhibit a satellite from communicating with the ground station. Alternatively, they could steal the data or information on the mission of a space system.

Standards – NIST Space Cyber Standards

https://www.nccoe.nist.gov/cybersecurity-space-domain

- NISTIR 8270: Introduction to Cybersecurity for Commercial Satellite Operations
- NISTIR 8323 Rev. 1: Foundational PNT Profile (Final)
- NISTIR 8401: Satellite Ground Segment (Final)

All refer to Space Policy Directive 5

- SPD-5 establishes key cybersecurity principles to guide and serve as the foundation for America’s approach to the cyber protection of space systems. Best practice and norms

Standards – NIST Space Cyber Standards

https://www.nccoe.nist.gov/cybersecurity-space-domain

- NISTIR 8270: Introduction to Cybersecurity for Commercial Satellite Operations
- NISTIR 8323 Rev. 1: Foundational PNT Profile (Final)
- NISTIR 8401: Satellite Ground Segment (Final)

All refer to Space Policy Directive 5

- SPD-5 establishes key cybersecurity principles to guide and serve as the foundation for America’s approach to the cyber protection of space systems. Best practice and norms

Standards – Paper led to IEEE and ISO standard

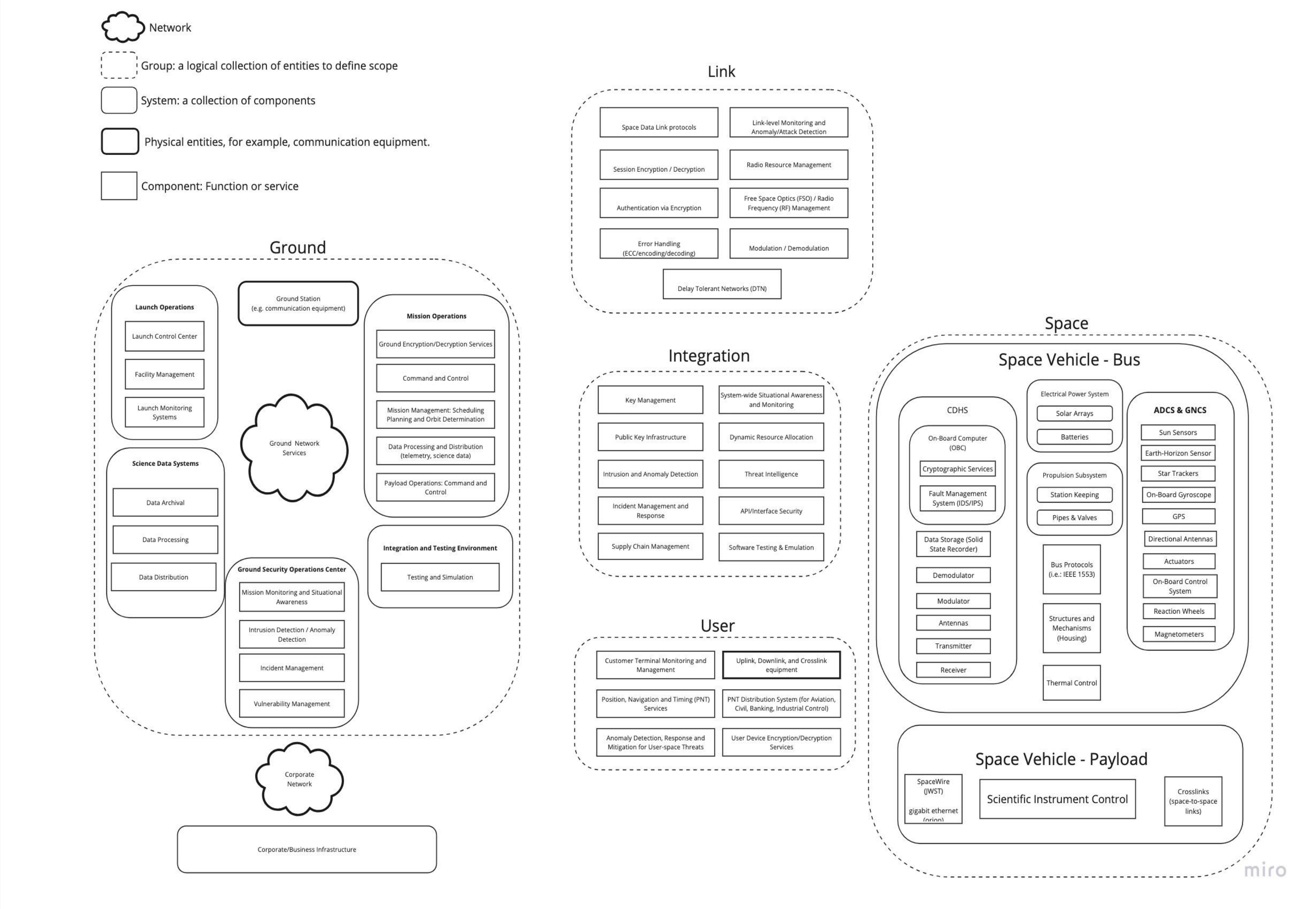
An International Technical Standard for Commercial Space System Cybersecurity - A Call to Action
https://doi.org/10.2514/6.2022-4302
34 international authors .

- Analysis of international and national standards
- Examines various component
  - Ground Segment
  - Space Segment
  - Link Segment
  - User Segment
  - System-of-System Integration Layer

This paper led to:

- **P3349 - Space System Cybersecurity Working Group**
- **https://sagroups.ieee.org/3349/**

P3349 - Space System Cybersecurity Working Group



Network

Group: a logical collection of entities to define scope

System: a collection of components

Physical entities, for example, communication equipment.

Component: Function or service

Ground

Launch Operations
- Launch Control Center
- Facility Management
- Launch Monitoring Systems

Ground Station (e.g. communication equipment)

Mission Operations
- Ground Encryption/Decryption Services
- Command and Control
- Mission Management: Scheduling Planning and Orbit Determination
- Data Processing and Distribution (telemetry, science data)
- Payload Operations: Command and Control

Ground Network Services

Science Data Systems
- Data Archival
- Data Processing
- Data Distribution

Integration and Testing Environment
- Testing and Simulation

Ground Security Operations Center
- Mission Monitoring and Situational Awareness
- Intrusion Detection / Anomaly Detection
- Incident Management
- Vulnerability Management

Corporate Network

Corporate/Business Infrastructure

Link

- Space Data Link protocols
- Link-level Monitoring and Anomaly/Attack Detection
- Session Encryption / Decryption
- Radio Resource Management
- Authentication via Encryption
- Free Space Optics (FSO) / Radio Frequency (RF) Management
- Error Handling (ECC/encoding/decoding)
- Modulation / Demodulation
- Delay Tolerant Networks (DTN)

Integration

- Key Management
- System-wide Situational Awareness and Monitoring
- Public Key Infrastructure
- Dynamic Resource Allocation
- Intrusion and Anomaly Detection
- Threat Intelligence
- Incident Management and Response
- API/Interface Security
- Supply Chain Management
- Software Testing & Emulation

User

- Customer Terminal Monitoring and Management
- Uplink, Downlink, and Crosslink equipment
- Position, Navigation and Timing (PNT) Services
- PNT Distribution System (for Aviation, Civil, Banking, Industrial Control)
- Anomaly Detection, Response and Mitigation for User-space Threats
- User Device Encryption/Decryption Services

Space

Space Vehicle - Bus

CDHS
- On-Board Computer (OBC)
  - Cryptographic Services
  - Fault Management System (IDS/IPS)
- Data Storage (Solid State Recorder)
- Demodulator
- Modulator
- Antennas
- Transmitter
- Receiver

Electrical Power System
- Solar Arrays
- Batteries

Propulsion Subsystem
- Station Keeping
- Pipes & Valves

Bus Protocols (i.e.: IEEE 1553)

Structures and Mechanisms (Housing)

Thermal Control

ADCS & GNCS
- Sun Sensors
- Earth-Horizon Sensor
- Star Trackers
- On-Board Gyroscope
- GPS
- Directional Antennas
- Actuators
- On-Board Control System
- Reaction Wheels
- Magnetometers

Space Vehicle - Payload

SpaceWire (JWST)

gigabit ethernet (orion)

Scientific Instrument Control

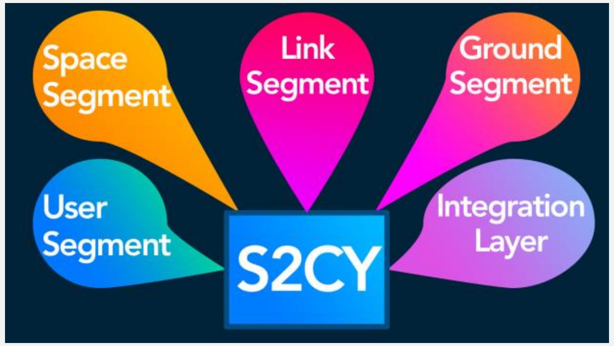
Crosslinks (space-to-space links)

P3349 - Space System Cybersecurity Working Group

The first step in this process will be defining common terms and vocabulary to ensure a consistent understanding of technical concepts across all parties involved in developing the standard.

The following step will be a gap analysis to identify areas where current standards and practices fall short in addressing the cybersecurity challenges specific to space systems. This analysis will help to determine the cybersecurity requirements and guide the development of adequate cybersecurity controls and countermeasures.

To leverage existing knowledge and avoid reinventing the wheel, a study of existing standards that could be useful and relevant to the current situation will be conducted. Similarly, existing best practices will be linked to the gap analysis to identify potential solutions that can be implemented in the new standard.



- New members welcome
- 120 people now involved.