University of
South Australia

Space Systems Security and Resilience – Impact on Curriculum

Professor Jill Slay (draws on Jordan Plotnek PhD work)

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

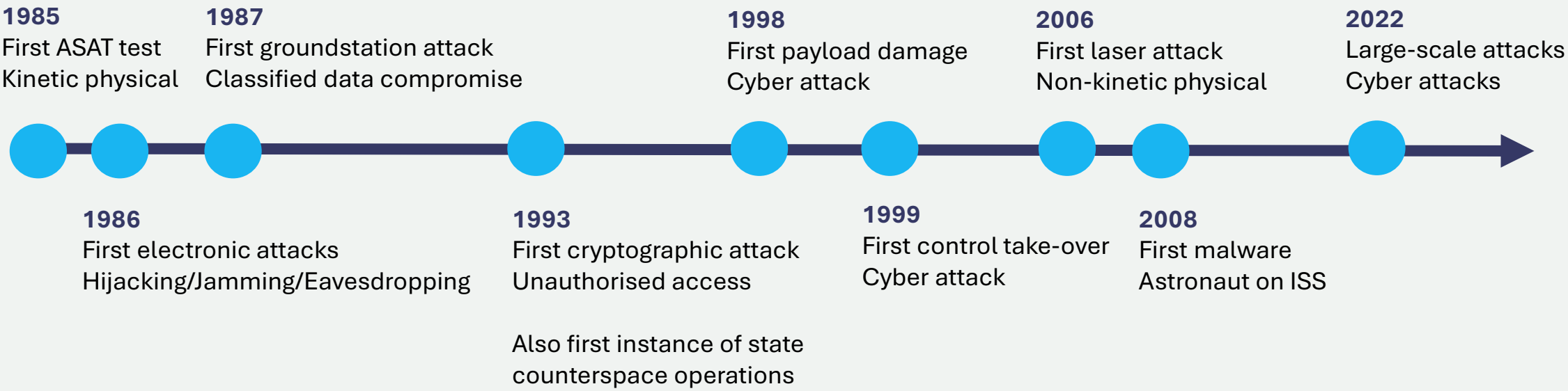
- We wanted to develop a framework for measuring resilience in space systems
- But found the need to come back down to the basics first
- Our research focuses on defining and modelling two key concepts:
  - Space Systems **Security**
  - Space Systems **Resilience**
- We involved two dozen academics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

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.



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

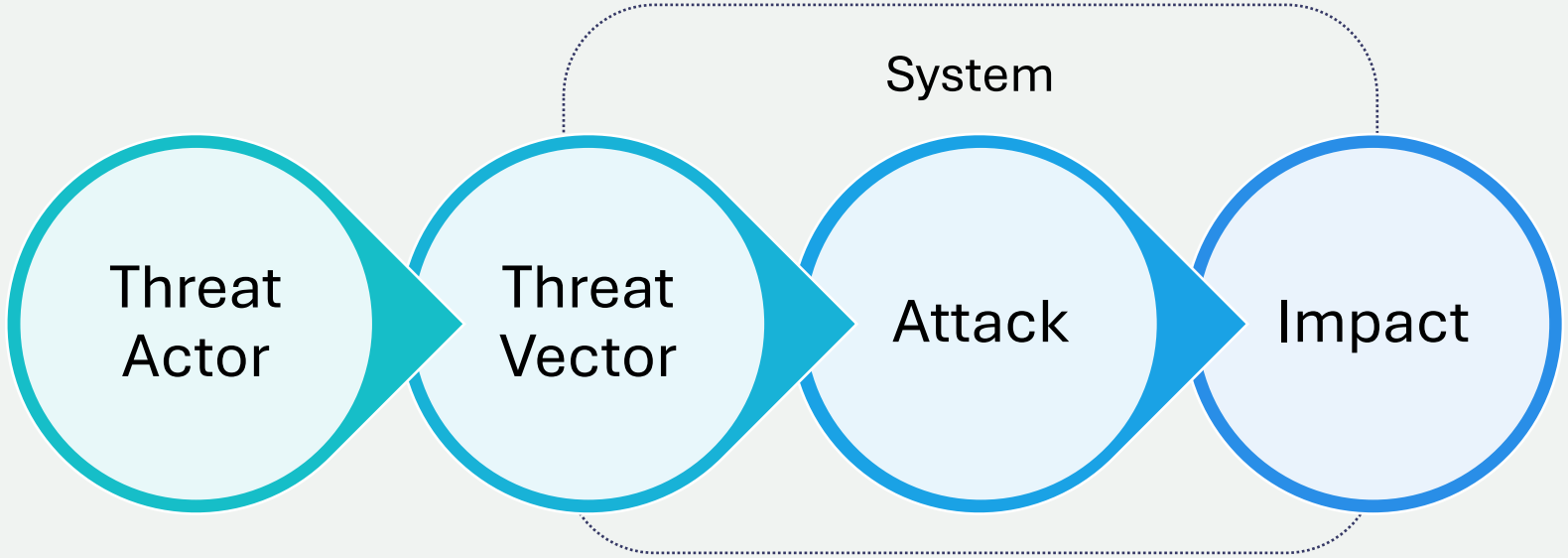
- Supports the security of other CSI by aiding:
  - Pre-emptive security efforts
  - Data collection and retention standards
  - Post-compromise forensics
  - Attribution, prosecution, and retaliation

- 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.

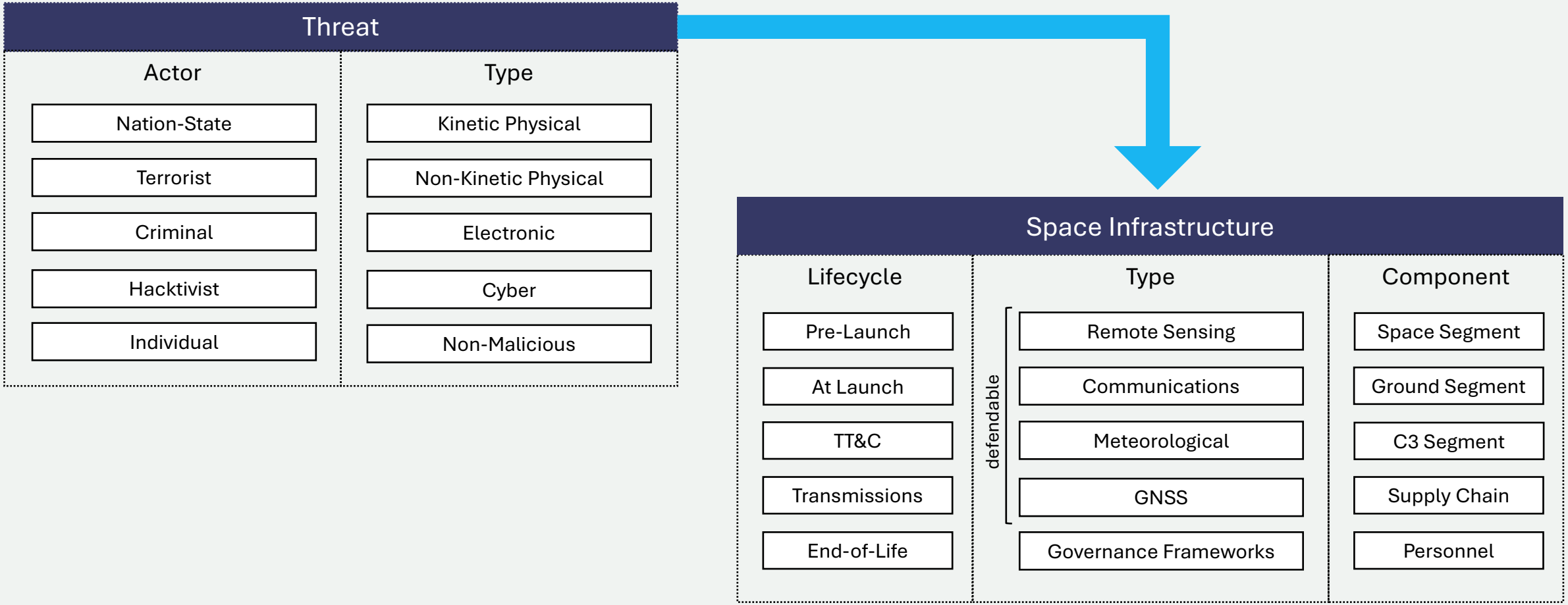
Attack Types

Targeted attacks to space infrastructure include:

C = Confidentiality
I = Integrity
A = Availability

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



Outcome 2 – Space Systems Security Domain

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

VECTOR / THREAT	Ground Segment					Space Platforms				
	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

Outcome 2 – Space Systems Security Domain

The new proposed knowledge domain based on expert collective input is:

	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.

Curriculum content space security

Governance Segment	R&D, Procurement & Supply Chain, Legal, Ethical & Compliance
Human Segment	Personnel, Users, Astronauts/Cosmonauts, Safety, Human Factors
Ground Segment	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

Masters Telecomms and Cyber Curriculum Content

In your first year you'll study the fundamentals of telecommunication systems,

Specialist courses covering topics such as

- big data concepts,
- systems engineering,
- critical infrastructure and control system security,
- cryptography and data protection, and
- digital communications.

In second year you'll take further specialist cyber engineering and telecommunications courses including

- telecommunications and device security,
- statistical programming for data science,
- information theory and coding and
- mobile communications and wireless access.

Also key to this degree is the development and application of research methods and skills. These will be invaluable when you begin work on your minor thesis.

Program Outcomes

1. Develop and implement encryption methodologies into secure system solutions.
2. Examine and assess the role policy plays in engineering secure systems, technology for policy implementation and the role of policy in driving the composition of cybersecurity solutions.
3. Apply the foundational elements of cybersecurity and engineering principles in architecting, developing and fielding secure network solutions against advanced persistent threats.
4. Explore the role assurance plays in security, particularly in the development and deployment of software products, and how one must account for this in security planning.
5. Design and evaluate trusted systems and implement designs into secure systems.
6. Perform system assessments using knowledge of network forensics, technical knowledge that incorporates incident response and continuity planning, as well as knowledge of various types of penetrations an adversary might attempt on an information system.

What next?

- Cyber Engineering from EA
- Review of Cyber Security from ACS
- AustCyber Australian Cyber Security Professionalisation project
- Incorporation in 2023 – 2030 Cyber Strategy