A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems

Thesis · December 2022

CITATIONS
0

READS
121

2 authors:

Jordan J. Plotnek
University of South Australia
12 PUBLICATIONS **34** CITATIONS
SEE PROFILE

Jill Slay
University of South Australia
176 PUBLICATIONS **5,509** CITATIONS
SEE PROFILE

A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems

By

Jordan J. Plotnek

Thesis submitted to

The University of South Australia

for the degree of Doctor of Philosophy

December 2022

Primary Supervisor: Professor Jill Slay

Associate Supervisor: Grant Wigley

Declaration

These doctoral studies were conducted under the supervision of Professor Jill Slay. I declare that this thesis does not incorporate, without acknowledgement, any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge it does not contain materials previously published or written by another person, except where due reference is made in the text.

Jordan Plotnek

01 December 2022

Abstract

Space systems provide vital services for many critical industries on Earth, including global communications, geolocation, imagery, and precision timing, as well as non-satellite applications such as space exploration and human habitation and settlement. The space environment is one of the most naturally hostile environments known to humankind, constantly facing threats such as electromagnetic radiation and space debris. In addition, the malicious threat environment is becoming increasingly adverse with an ongoing rise in cyber and electromagnetic attacks against space infrastructure, both terrestrial and deployed. Compounding the issues above, space systems are also known to have extensive and vulnerable international supply chains, with the space segment notably lacking inherent access to redundancy or maintenance options. Adding to the complexities of resilient space systems design, the space environment is becoming increasingly congested and contested with a burgeoning second space race that is seeing the rapid deployment of space systems containing a vast array of new technologies and, hence, vulnerabilities.

The combined effect of an increasingly hostile threat environment with increasingly vulnerable space systems necessitates that space technologies are built to be resilient-by-design. This requires the development of a pragmatic resilience assessment framework that can be utilised by space systems security professionals to assess the resilience of their system to any given adversity and shed light on any weaknesses in the space system design. The research project described in this dissertation details the development of a foundational space systems security ontology to guide future research and development, as well as a space system resilience assessment framework for determining the high-level resilience status of any given space system to any given adversity. This includes the space system's ability to anticipate, react to, survive, recover from, and adapt to adverse events whilst maintaining control and sustaining core operations and services in a degraded state.

This research dissertation presents the space systems resilience assessment framework, which consists of seven individual novel academic contributions to the contemporary field of space systems security and resilience:

1. Comprehensive evaluation of space systems security literature;
2. Space systems security definition;
3. Space systems security knowledge domain;
4. Space systems resilience taxonomy;

5. Space systems resilience definition;
6. Space systems resilience model (including a phasal cycle and temporal chart); and
7. Space system resilience assessment framework.

This thesis outlines a mixed methodology to achieve the above outcomes, utilising both quantitative and qualitative approaches. The research involves conducting a three-phase Delphi study of two dozen space security experts across ten countries using online surveys and an expert focus group. The outcomes of the Delphi study are then experimentally tested using the case study methodology. In the methodology, three cyber-physical case studies are utilised to evaluate the effectiveness of the final framework against real-world space systems, using data collected through interviews with practicing space systems security managers. A cyber-physical terrorist threat model is used alongside the Lockheed Martin Cyber Kill Chain model to generate a theoretical adverse event that exploits the identified vulnerabilities in the real-world systems to finally test the high-level resilience of each space system using the new framework.

The final outcome of this body of research is an experimentally evaluated space system resilience assessment framework for assessing the high-level resilience status of any given space system to any given threat. This includes definitions and taxonomies for space systems security and resilience, a comprehensive space systems security knowledge domain, and a complete phasal and temporal resilience model.

Acknowledgements

Although there are countless people who have assisted, supported, and inspired me along the way, I certainly couldn't have achieved anything without the support and patience of my partners, Sabrina and Lizzie. Thank you both for enduring those years of seemingly endless rants and ravings about things far too specific to make much sense to you. Especially, thanks to Sabrina for keeping me alive by bringing food and drink to my desk throughout the thesis writing stage, even while pregnant. Also, to my newborn son, Léon Jude, whose future world(s) my work seeks to protect.

I owe this entire research project to Professor Jill Slay for her brilliant guidance and continuous inspiration to complete this significant body of work. Despite the challenges of the COVID-19 pandemic and me being stuck abroad for several years throughout the study, you never wavered in your dedication to keeping me motivated and financially supported. My career will forever be shaped by your words of wisdom and pragmatic approach to both academia and life.

There are many people and organisations who have come together at different points over the four years, without whom I would not have been able to produce the high-quality outcomes we achieved in this research. For reasons that are too many to recount, a huge thank you to Harpreet Cheema and Glenn Ashe from Anchoram Consulting; Bernard Lebel, Frederic Audet, and François Couderc from Thales Canada; Mourad Debabbi from Concordia University; everyone that assisted from SmartSat CRC across Australia; and the whole team of university admin and research staff who were consistently helpful, both from the University of South Australia and at La Trobe University in Melbourne where this research project commenced.

Finally, and perhaps most importantly of all, thank you to the dozens of expert participants who responded to the Delphi Study surveys and case study interviews, and who provided invaluable input and feedback throughout the entire research process. Also to the reviewers who spent hours reading the draft dissertation and providing constructive feedback to improve it. I am overjoyed by the outcomes of our collective efforts and am honoured to have gotten to know many of you throughout the study. I hope our findings will help to mature the security and resilience of space systems in operations now and those to be developed for years to come. May space continue to serve humanity in

pursuing peaceful and sustainable outcomes for life on earth, as well as for other planets yet to be colonised.

The research detailed in this dissertation is related to, and funded by, a joint research agreement between the University of South Australia and SmartSat CRC in Adelaide, Australia. All research relating to power systems and the smart grid were funded by Thales Canada and supported by the University of Concordia in Montréal, Québec, Canada.

Publications

The following publications have been produced in the course of work associated with this dissertation:

Plotnek, J.J., 2022. Enhancing Cyber Resilience in Smart Grids. Australian Institute of Energy, Energy News 40, 7–10.

Plotnek, J.J., 2022. Space-Cyber trends and opportunities in Australia. Australia in Space Magazine 18–21.

Plotnek, J.J., Slay, J., 2022. Space Systems Security: A Definition and Knowledge Domain for the Contemporary Context. Journal of Information Warfare 21, 103–119.

Plotnek, J.J., Slay, J., 2022. A New Dawn for Space Security, in: Proceedings of the 17th International Conference on Cyber Warfare and Security 2022. Presented at the 17th International Conference on Cyber Warfare and Security, State University of New York, Albany, USA, pp. 253–261. https://doi.org/10.34190/iccws.17.1.17

Plotnek, J.J., Slay, J., 2021. Satellite Cyber Resilience Whitepaper. SmartSat CRC, Adelaide, Australia.

Plotnek, J.J., Slay, J., 2021. Power systems resilience: Definition and taxonomy with a view towards metrics. International Journal of Critical Infrastructure Protection 33. https://doi.org/10.1016/j.ijcip.2021.100411

Plotnek, J.J., Slay, J., 2021. Cyber terrorism: A homogenized taxonomy and definition. Computers & Security 102, 102–145. https://doi.org/10.1016/j.cose.2020.102145

Plotnek, J.J., Slay, J., 2019. What is Cyber Terrorism: Discussion of Definition and Taxonomy, in: 18th Australian Cyber Warfare Conference 2019. Presented at the Australian Cyber Warfare Conference, Deakin University, Melbourne, Australia, pp. 1–4.

Rahiminejad, A., Plotnek, J.J., Atallah, R., Dubois, M.-A., Malatrait, D., Ghafouri, M., Mohammadi, A., Debbabi, M., 2023. A Resilience-Based Recovery Scheme for Smart

Grid Restoration following Cyberattacks to Substations. International Journal of Electrical Power and Energy Systems 145. https://doi.org/10.1016/j.ijepes.2022.108610

Thangavel, K., Plotnek, J.J., Sabatini, R., 2022. Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity. Presented at the 41st AIAA/IEEE Digital Avionics Systems Conference (DASC), USA.

Table of Contents

List of Figures

List of Tables

Acronyms and Abbreviations

3PP	Third-Party Procurement
AI	Artificial Intelligence
APT	Advanced Persistent Threat
ASAT	Anti-Satellite
C3	Communications, Control, Computing
C5ISR	Communications, Control, Computing, Command, Cyber, Intelligence, Surveillance, & Reconnaissance
CCPI	Critical Cyber-Physical Infrastructure
CIRT	Cyber Incident Response Team
CKC	Cyber Kill Chain
CNI	Critical National Infrastructure
COLA	Collision Avoidance
COMSAT	Communications Satellite
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical System
CRC	Cooperative Research Centre
CSI	Critical Space Infrastructure
CSIS	Center for Strategic and International Studies
D4P2	Disaggregation, Diversity, Distribution, Deception, Protection, Proliferation
DDoS	Distributed Denial of Service
DEW	Directed Energy Weapon
DISP	Australian Defence Industry Security Program
DoS	Denial of Service
DRP	Disaster Recovery Plan
DSPF	Australian Defence Policy Framework
E3	Electromagnetic Environment Effects
ECM	Electromagnetic Countermeasures
EMC	Electromagnetic Compatibility
EMP	Electromagnetic Pulse
EMSEC	Emanations Security

EW	Electronic Warfare
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning Satellite
GRC	Governance, Risk, and Compliance
HILF	High Impact Low Frequency
IAM / IDAM	Identity and Access Management
ICS	Industrial Control System
IoT	Internet of Things
IIoT	Industrial Internet of Things
IRAP	Australian Government Industry Registered Assessors Program
ISM	Australian Government Information Security Manual
ISR	Intelligence, Surveillance, & Reconnaissance
IT	Information Technology
ITU	International Telecommunication Union
LEO	Low Earth Orbit
LIHF	Low Impact High Frequency
LPI / LPD	Low Probability of Interception / Detection
MCS	Mission Control System
MFA	Multi Factor Authentication
MIL	Military
NUC	Next Unit of Computing (basic mini-PC)
OS	Operating System
OT	Operational Technology
PC	Personal Computer
PNT	Position, Navigation & Timing
PLC	Programmable Logic Controller
PRO	Primary Research Outcome
PsyOps	Psychological Operations
QoS	Quality of Service
RAT	Remote Access Trojan
RF	Radio Frequency
SATCOM	Satellite Communications
SCADA	Supervisory Control And Data Acquisition

SME	Subject Matter Expert
SOC	Security Operations Centre
SOCI	Australian Security of Critical Infrastructure Act
SRO	Secondary Research Outcome
SV	Space Vehicle
TT&C	Telemetry, Tracking, and Command
TTP	Techniques, Tactics, and Procedures
UCS	Union of Concerned Scientists
UniSA	University of South Australia
V&V	Verification and Validation
WHS	Work Health and Safety

1 Introduction

1.1 Chapter Overview

The Introduction presents an overview of the dissertation, describing in detail the background and historical context of the thesis and the overall research motivations, problems, and goals. The chapter then closes with a synopsis of the research strategy used to solve the stated problems, before outlining the remaining chapters in the dissertation, highlighting the research problems that each chapter addresses, along with the methodology chosen to investigate each problem.

This dissertation is cross-disciplinary and relies on literature across a breadth of subjects and professional communities. The thesis is rooted in several bodies of knowledge and methodologies, including computer science, engineering, and social science, and is intended for academic and professional audiences such as space security researchers, critical infrastructure resilience researchers and consultants, cyber security governance and risk professionals, security architects and managers, and space systems operators and administrators.

1.2 Background

Space infrastructure provides vital services for a number of critical industries, including; defence, transportation, energy, utilities, emergency services, banking, environment, academia, and others. These services range from global communications to remote sensing and geolocation, with many new applications undoubtedly on the horizon, including plans for further exploration and even human settlement. It is therefore essential that space technologies are protected from unwanted interferences – a task that is becoming more challenging by the day. Adding to the already complex space security environment, we are experiencing the beginnings of a second space race that is seeing the rapid deployment of space systems containing a vast array of new technologies, such as the Internet of Things (IoT) and advanced onboard processing. This is subsequently introducing new vulnerabilities to an already aged and vulnerable satellite ecosystem, hence increasing the risk of potentially catastrophic security events. This effect has been demonstrably exacerbated through political instability, such as the 2021 Russian invasion of Ukraine, which was linked to a number of high profile satellite hacks, and recent destructive anti-satellite tests by countries such as China and Russia. Although well-

articulated in political, legal, and international relations literature, the engineering, science, and technology aspects of space security are currently under-studied and disjointed, leading to fragmented research and inconsistent terminology.

Critical infrastructures, and industrial systems in general, are both particularly vulnerable and specifically targeted by such adversarial groups and state actors (Kaspersky Lab 2019), and space systems are by no means immune to this exponentially increasing threat. In fact, as detailed in the following sections, space systems face an even greater range of threats and have even further reaching consequences than those combatted by terrestrial critical infrastructures (Bradbury et al. 2020), and considering the level of military dependence on space infrastructure and the volatile state of global affairs today (Donnelly 2021), there has never been a more urgent need for resilient space systems as there is now.

1.3 Historic Context

In 1957 the Soviet Union launched Sputnik-1, the first manmade object to enter earth's orbit, triggering a two-decade long space race and forever changing the course of human history. Today we are on the cusp of a second space race, this time with over 5000 artificial satellites already in operation (Union of Concerned Scientists 2022), and countless more space debris littered in perpetual orbit.

As the battle for space superiority ramps up for a second time, we are forced to acknowledge the wildly different technological landscape compared to that which our scientific colleagues faced back in 1957. We now live in a world run by computers, where code has infiltrated every aspect of our lives. From communication to transportation to work, banking, recreation, and even things as mundane as washing machines, fridges, toothbrushes, and toasters — these days everything is interconnected. With this technological revolution comes great opportunity for criminals and other malicious actors who seek to manipulate these technologies in pursuit of power, influence, wealth, and chaos.

Unfortunately, secrecy clouds public access to information about incidents to critical infrastructure, leaving the idea of space systems security largely to the imagination of Hollywood. The lack of academic research in the field only exacerbates the fallacy that space security is purely a political tool or a hypothetical need. However, both past and current events provide concrete evidence of the exponentially growing need for space systems security.

Pavur and Martinovic (2020) conducted a comprehensive study of historical satellite hacking incidents and identified 116 significant events since Sputnik, with the first occurring in 1986. This number includes attacks across three of the four categories of targeted attack (i.e., non-kinetic physical, electronic, and cyber), with kinetic physical attacks being excluded from the study. According to this paper, the first few years of space attacks saw a heavy focus on piracy and spoofing, with satellite imagery data being eavesdropped to avoid subscription fees and television streams being hijacked to broadcast unsolicited messages. A noteworthy example is the 1987 hack conducted by an employee of the American Christian Broadcasting Network who transmitted unauthorised biblical messages over the Playboy Channel's planned broadcast (Knittel 2013). The 1990s saw a move towards signal jamming, with commercially available satellite jammers being produced and state actors such as the US, Iran, Indonesia, and Russia carrying out various jamming operations. This decade also witnessed one of the first suspected attacks targeting OT infrastructure, with a 1998 cyber attack against the NASA Goddard Space Flight Centre causing a US-German satellite, ROSAT, to reposition its solar panels towards the sun and render the sensors and satellite inoperable (Falco et al. 2021).

The turn of the century brought with it a significantly increased interest in malicious operations targeting space infrastructure, including the use of commercial and state-sponsored jamming, signal hijacking, laser attacks, malware, eavesdropping, and other increasingly sophisticated attacks. In 2007 China compromised two NASA satellites via the ground station, taking complete control over their flight signalling (Bardin 2013). That same year China also demonstrated a kinetic ASAT weapon against one of their own satellites, producing hundreds of pieces of dangerous space debris along with it and playing a role in the onset of the second space race that we are witnessing today (Zissis 2010). In November 2021 Russia conducted a similar kinetic ASAT test on their own satellite, known as Cosmos 1408, creating a field of at least 1500 trackable debris (Bugos 2021). A few months later, on the same day Russia invaded Ukraine in February 2022, largescale cyber attacks against the European commercial satellite communications provider, Viasat, affected internet access for tens of thousands of people across Europe and Ukraine (Cyber Peace Institute 2022, Boschetti et al. 2022). In a Press Statement released by the United States Secretary of State, it was assessed that Russia launched the cyber attacks to disrupt Ukrainian command and control during the invasion, with spill over impacts into other European countries (Blinken 2022).

In response to this increase in threat activity targeted towards satellite systems, many countries have recently updated their policies and legislative frameworks to recognise space systems as critical infrastructure and invest in their national space security capability. Some examples of this include Australia's amendment to the Security of Critical Infrastructure (SOCI) Act to designate Space Technology as critical infrastructure and mandate a minimum level of security governance, and the United States' Space Policy Directive 5 that outlines cyber security principles for space systems. Additionally, both the US and China have established independent space forces, including the United States Space Force and the People's Liberation Army Strategic Support Force. Russia has established and disbanded the Russian Space Forces as an independent branch of their military several times (operational between 1992-1997 and 2001-2011), with their current space force being managed under the Russian Aerospace Forces branch. Many other countries have made moves to incorporate space security into their existing military or governmental structures, such as the French Air and Space Force, Iranian Islamic Revolutionary Guard Corps Aerospace Force, the Indian Defence Space Agency, and the Australian Defence Space Command.

Turning our attention from the past to the future we are greeted with hundreds of optimistic narratives and exciting endeavours. From colonies on Mars to space hotels and deep-space exploration, there is no shortage of ideas to keep humanity driving forward in this domain. The first space race cemented space systems as critical infrastructure for progressing life on earth. The second space race is shifting the focus from government to commercial interests, with significant headway already being made to establish space as a viable human arena in its own right. However, as the Russo-Ukraine war has demonstrated, whether or not a state recognises space as critical infrastructure, both commercial and government space systems are highly attractive targets with the innate ability to generate largescale impacts to society.

1.4 Research Motivation

Space is the next frontier for human civilisation. Humans have long relied on space infrastructure for the advancement of technologies here on earth, with such dependencies becoming more and more critical. We are now on the path toward developments such as extra-terrestrial colonisation, the commercialisation of space, space mining, and other feats that would have been unimaginable a mere two or three generations ago.

Of course, with opportunity comes risk and the risks involved in modern space systems development are considerable. According to Livingstone and Lewis's future space trends predictions (Livingstone and Lewis 2016), the next decade or so could bring about space technologies such as system-on-a-chip avionics, self-optimizing autonomous systems, complex on-board satellite processing, autonomous satellite-to-satellite (S2S) communications, plus a number of complex software additions and improvements; each and all of which will introduce new vulnerabilities that can be exploited to produce unseen effects. For example, consider a futuristic piece of worm-like malware that corrupts a satellite connected via an autonomous S2S system – the entire fleet could be compromised and potentially rendered unserviceable.

Alongside this resurgence in the rapid development of space systems, all kinds of new threats are emerging. Talk of cyber warfare, cyber terrorism, and cyber crime are increasing and so are the capabilities of motivated threat actors (Plotnek and Slay 2021b). Both cyber and electronic weapons are becoming more effective and accessible by the day, with at least 120 different countries already invested in cyber warfare capabilities (McAfee 2005).

Mass-scale environmental and political events may also impact humankind's reliance on CSI, which could cause unforeseeable impacts. For example, hazardous asteroids heading for earth (O'Neill and Handal 2021) or the growing threat of climate change, both of which are tracked and assessed using space infrastructure – a reliance that may evolve and become more critical as time goes on. Another example might be a third eruption of world warfare. Military equipment has become increasingly reliant on satellite technology and such a situation may over-burden aging infrastructure and cause denials of service in critical moments. On a similar tangent, the United States has officially approved the establishment of a Space Force (Farley 2020) and many other countries are likely to follow suit, events that will undoubtedly impact the space security domain.

With an understanding of the criticality of space infrastructure, its deepening vulnerability issues, and the unpredictable threat environment within which it is situated, it is easy to see the importance of space security. Unfortunately, up until now there has been little recognition or structure afforded to the complex domain of space security. In fact, there even exists some hostility towards security research within the space industry (CSRIC 2015), a culture that could impede the advancement of space development altogether.

The second space race has sparked a period of rapid development and deployment, which presents significant complications without a unified understanding of the domain's research problems for efficient prioritisation and collaboration. The current lack of direction and common purpose has led to a massive double-up in the limited research available, with each contributing discipline evidently taking a siloed approach to space security terminology and taxonomy. Additionally, unlike most other critical infrastructures space has direct military applications, meaning that efficient research and development is crucial for national security objectives such as effective threat deterrence and space dominance.

An academic baseline is required to enable space resilience research, and thus adequately and efficiently protect society from the impacts of targeted cyber-physical space threats. This dissertation aims to contribute a body of work to help establish such a baseline for assessing space systems resilience to cyber-physical threats.

1.5 Research Questions

This research sets out to answer the following research questions;

Research Question 1

Is there research in the space security domain that includes cyber-physical threats to space systems as critical infrastructure?

Research Question 2

What is space systems resilience, and can a taxonomy for space systems resilience to cyber-physical threats be developed?

Research Question 3

Can a valid interdisciplinary (engineering, international security, and the social and computer sciences) framework be developed to establish space systems security as a professional domain?

1.6 Research Goals

The below goals represent the core objectives of this dissertation;

Research Goal 1

> An experimental evaluation of the research related to space systems security to determine the scope of the domain and theories on the space-cyber threat environment.

Research Goal 2

> An ontological discovery and taxonomical catalogue of space systems resilience for the purposes of resilience assessment by space systems security practitioners.

Research Goal 3

> A space systems resilience framework, based on the outcomes of the ontological discovery exercise, for determining the high-level resilience status of a given space system to a malicious cyber-physical threat.

1.7 Research Strategy

The research described in this dissertation was conducted in distinct stages. This section outlines the approach taken to conduct the research.

The first stage of the research involved a literature review to identify gaps that are required to be filled in pursuit of defining a space systems resilience framework. This stage identified the distinct lack of available literature to construct a space-centric resilience framework. The bulk of available resilience literature was primarily targeted towards the electricity sector and complex cyber-physical systems in general. Available space systems or space security literature was not found to be tangential to the desired outcomes of this research dissertation, and hence a significant gap in space systems security or resilience literature was identified. The findings of this literature review are detailed in Section 2.

Documented inside this same section, Section 2, are the efforts to fill some of the more foundational literature gaps that were required to achieve the desired outcomes of this research. This included establishing the following:

- Power systems resilience definition

- Power systems resilience taxonomy
- Power systems resilience model
- Cyber terrorism definition
- Cyber terrorism taxonomy.

The definition of resilience has long been contested across several domains, from human psychology to complex systems. As mentioned earlier, space systems have very limited literature available and offered no comprehensive framework for understanding resilience in a space context. Some aspects relating to space systems resilience have been published, such as risk and threat taxonomies, however these are not sufficient to address the stated research problem without supporting material from a broader discipline. Treating space systems as critical infrastructure is well-accepted internationally so the logical place to commence the literature search was to search for critical infrastructure resilience frameworks and models that could be adapted to the space context.

After exploring several avenues within critical infrastructure resilience literature, power systems were selected as the prime candidate to model space systems resilience off. Power systems, such as smart grids, have similar and comparable characteristics to satellite constellations, the most prevalent space system at the time of writing, and so the adaptation process would be more natural. The decision to base the space systems resilience model from power systems resilience models was one that was made noting the following observations made at the time of writing:

- Power systems resilience has the most mature literature available out of the various critical infrastructure domains
- Both power systems and space systems are remotely managed due to inaccessibility to end devices and sensors
- Both electric grids and satellite constellations deliver vital services across a geographically expansive user base
- Network segmentation is a vital consideration for both power systems and space systems
- Adverse impacts may immediately affect the end users of the system's critical services
- Both space and power services can have geopolitical impacts if interfered with

- Both space and power services offer military strategic advantage and provide necessary vital services during wartime
- Smart grid literature often references the modernisation of the grid, and hence the new technologies introduced into an aging infrastructure, which is comparable to those being rapidly deployed as part of the second space race (e.g. IoT, AI, advanced computing, and sensor technology).

Although power systems resilience literature offered the most advanced and comparable research for this study, there was yet a lack of consensus surrounding the exact definition, taxonomy, and model to provide a comprehensive power systems resilience framework. Given the bounty of available power systems resilience literature, a meta-analysis was conducted to provide the required resilience framework, including a definition, taxonomy, and lifecycle; as detailed in Section 2.2.2. This was then able to be adapted to the space systems context The findings of this preliminary framework were then modified and validated through expert participants in the Delphi Study, as described in Section 3.3. Finally, the outcomes of the Delphi Study were verified through a case study on real-world operational space systems, as detailed in Section 4.2.

The Delphi Study involved three individual rounds of survey questions, provided over an anonymous online platform, to over two dozen recognised experts with at least 7 years of experience operating in a domain related to space security. Over the three rounds, the preliminary framework produced above was presented and iteratively modified until complete consensus was achieved on the following outcomes:

- Space systems security definition
- Space systems security knowledge domain
- Space systems resilience definition
- Space systems resilience taxonomy
- Space systems resilience model.

The case study in Section 4.2 verified the proposed space systems security and resilience framework by taking real-world security processes and testing the system's resilience against the proposed framework. The case study utilises a theoretical worst-case threat scenario to highlight any gaps identified through applying the proposed resilience framework. The worst-

case threat scenario specifically involves a cyber-physical attack conducted by a motivated and capable terrorist threat actor. Although there are many threats against space systems that this case study could have been modelled against, cyber-physical terrorism was chosen as the theoretical extreme due to its versatility of outcomes when used as the adverse event to model resilience against. For example, a cyber warfare scenario would perhaps be more probable, especially as it has been witnessed already on several occasions. However, most capable state-based threats on critical infrastructure witnessed to date have been centred around espionage and passive threat outcomes rather than active threat outcomes, such as a cyber-physical attack. By contrast, a cyber-physical terrorist has the motivation to cause explicit and traceable harm in order to raise awareness for their cause and draw attention to their terrorist group. Although less of a present threat than cyber warfare driven adversities, there is also a notable public interest in the area of cyber terrorism, as demonstrated in the literature review at Section 2.3.3.2. The consequences of a cyber terrorist attack can be just as devastating as a state-based attack, however a cyber terrorist attack can have more visible and far-reaching impacts. The results can also be more extreme as a cyber terrorist is not bound by international law or rules of engagement as most state actors are, and they are often specifically determined to pursue civilian casualties and disruptions.

1.8 Thesis Structure

The dissertation is structured to detail the research approach, methodology, and findings, as well as to provide validation and verification of research outcomes through the Delphi study and case study methods. Finally, it provides commentary on the research outcomes and their relationship to the original research goals outlined in Section 1.6 above.

1.8.1 Chapter 2

Chapter 2 of this dissertation details the literature review and its outcomes, including any secondary research outcomes that were achieved in order to support the primary research outcomes outlined in Chapter 5. The literature review chapter includes the initial research conducted to identify the literature gap that this dissertation intends to fill. It commences with an overview of existing space systems security literature and identifies preliminary definitions and contextual frameworks in section 2.1. It then explores the concept of resilience across critical infrastructure domains, especially investigating power systems and space systems resilience literature in section 2.2. Finally, space security threats are examined in section 2.3, including types of space systems and their relative threat environments, as well as determining

core literature and concepts to support the threat model for the case study component of the research. As part of the threat model, cyber terrorism is explored in depth and a new cyber terrorism taxonomy and definition is presented in section 2.3.3.2.

1.8.2 Chapter 3

Chapter 3 details the methodology and research approaches utilised in pursuit of the research goals. It commences in section 3.1 with an introduction to the study, before addressing the approaches to research in section 3.2, including an investigation into the quantitative, qualitative, and mixed methods approaches in relation to the research goals. Section 3.3 details the specific methods used for this research, including details regarding materials provided to expert respondents and the case study overview. The case study threat model is detailed in section 3.3.3.3 while the case study scenario is defined in section 3.3.3.4.

1.8.3 Chapter 4

Chapter 4 presents the raw data, detailed analysis, and final outcomes and findings of each component of the research, including the Delphi Study at section 4.1, the expert focus group at section 4.1.3, and the case study at section 4.2. It is in this chapter that the evolution of the framework is detailed and documented, with every change made being linked to a specific response and tracked in an outcomes table.

1.8.4 Chapter 5

Chapter 5 provides a final overview of the research findings in relation to the initially described overarching research goals. In this chapter both primary and secondary research outcomes are detailed, with each outcome representing a unique contribution to academia. Primary research outcomes (PRO) are defined to be unique contributions to the field of space systems security, with secondary research outcomes (SRO) relating to other domains such as power systems or general cyber security. Each research goal is then discussed in detail, with a final demonstration of how each goal has been achieved by the research project.

1.8.5 Chapter 6

Chapter 6 closes the dissertation with a final overarching summary of the research and its outcomes, as well as a discussion of the research limitations and recommendations for future research.

2 Literature Review

A graphic illustration of the space eco-system at a high level is provided below to assist in interpreting this literature review chapter. This diagram was produced as a result of the study and findings as detailed in Chapter 4.

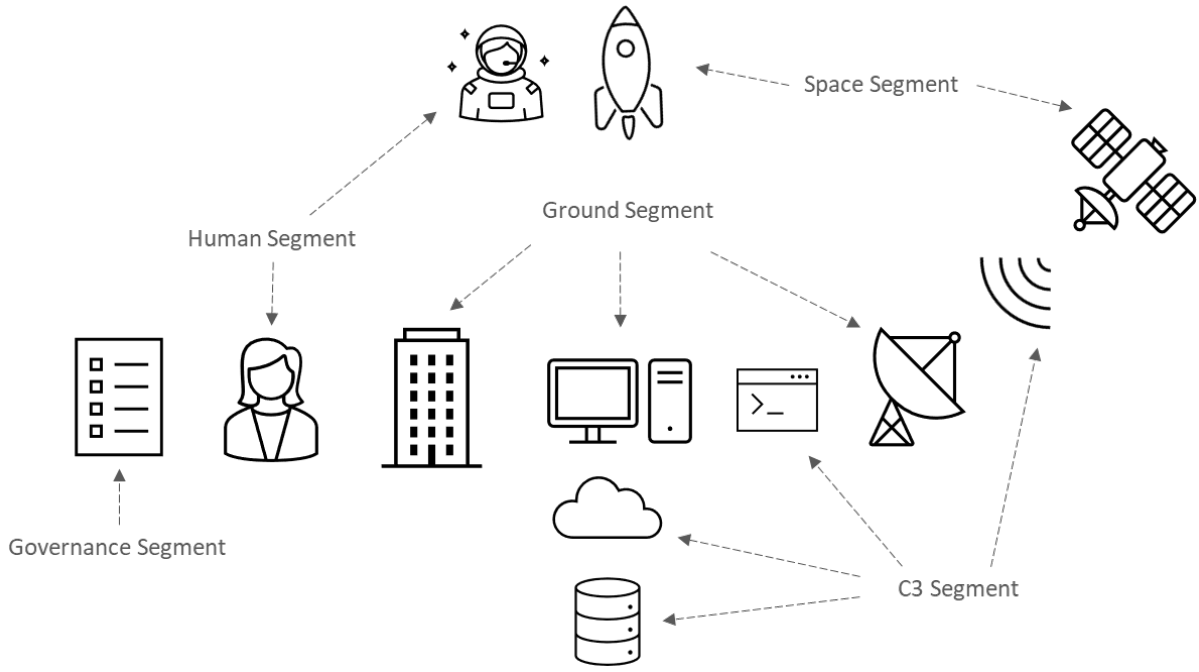

Figure 1 - Space System Segments and Example Components

2.1 Space Systems Security

Of the various disciplines contributing to space security knowledge, the social sciences are by far the most mature with several decades of published history. Traditionally space security has been viewed primarily as a military domain due to Cold War motivations behind the first space race (Sheehan 2015). More recently, however, this view has expanded to include three dimensions of space security (Mayence 2010):

1. security in space (i.e. protecting space systems);
2. space for security (i.e. military space operations); and
3. security from space (i.e. protecting Earth from space-based threats).

This dissertation focuses exclusively on the first dimension of space security, security in space, herein referred to as `space systems security'. Drawing from older literature we can find several space security definitions that can be reapplied directly to space systems security. The

definition provided by Moltz (2011, p.11) serves as a good baseline, defining it as “the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction”.

Although under-studied from a systems engineering perspective, a collection of disparate papers relating to the domain of space systems security were found. A key text in this domain is the book by Georgescu et al. (2019) entitled ‘Critical Space Infrastructures: Risk, Resilience and Complexity’, which successfully introduces space system fundamentals and examining space systems as critical infrastructure but is decidedly lacking in its discussion of cyber security issues. The taxonomy introduced in this book is particularly helpful as it splits critical space infrastructure (CSI) into five key categories:

- Remote Sensing;
- Communications;
- Meteorological;
- Global Navigation Satellite Systems (GNSS); and
- Administrative and Legislative Frameworks.

The Center for Strategic & International Studies (CSIS) conduct annual ‘Space Threat Assessments’ that focus on the threat of counter-space weapons, breaking them down into four broad categories (Harrison et al. 2020):

- kinetic physical;
- non-kinetic physical;
- electronic; and
- cyber.

The remainder of the report is less repurposable and goes on to analyse different nation state capabilities and their threat to the United States at the point in time of the assessment.

Housen-Couriel (2016) published a paper on ‘Cybersecurity Threats to Satellite Communications’ with the goal of establishing a typology of state actor responses. However, it is focuses on international law and thus does not adequately address space security or resilience from a technical perspective. In contrast to the Space Threat Assessment by Harrison et al., the paper identifies only three kinds of satellite `disruptions':

- kinetic (direct impact of one satellite with another);

- virtual (interference with communications); and
- hybrid (electromagnetic pulse, or EMP, weapons).

They then plot these three disruption categories against five stages of satellite operations:

1. pre-launch;
2. at launch;
3. telemetry, tracking, and command (TT&C); and
4. transmissions; and
5. end-of-life.

The stages of satellite operations are also discussed in a cyber security context by Manulis et al. (2020), who define it by four phases:

1. launch;
2. commissioning;
3. in-service; and
4. end of life.

The paper focuses exclusively on satellite systems, defining the space segment architectures as a singular satellite, cluster (a small number of satellites orbiting in close proximity), and a constellation (a large number of satellites in different orbital planes). In terms of threats the paper discusses the ground segment, communications, space segment, and regulatory requirements for space cyber security. The ground segment is deemed vulnerable to attacks such as: physical, computer network exploitation (CNE), cloud infrastructure, data corruption/modification, supply chain, and unpatched/outdated/legacy COTS software. Satellite system communications are described as vulnerable to jamming, eavesdropping, hijacking, and spoofing. Finally, cyber security on the space segment is discussed briefly and in less defined terms, primarily serving to highlight the existing gap in knowledge regarding satellite space vehicle cyber attacks. (Manulis et al. 2020)

A Chatham House research paper by Livingstone and Lewis (2016) takes a high-level approach to space cyber security, discussing topics such as cyber threats and risks to satellite infrastructure as well as challenges and trends in the industry. However, the paper appears to be directed toward a general audience so isn't guided by existing taxonomies, and hence doesn't

serve the purpose of a foundational academic text. It also is limited to cyber threats alone, which form only one threat type that a space security practitioner must be aware of.

A comprehensive paper by Pavur and Martinovic (2020) details the cybersecurity threats to satellites and examines over 100 significant satellite hacking incidents over the past 60 years. The paper identifies four sub-domains that satellite cybersecurity applies to:

- satellite radio-link security;
- space hardware security;
- ground station security; and
- operational/mission security.

Pavur and Martinovic comment on the cross-disciplinary nature of space security but, perhaps due to their narrow focus on cybersecurity, stop short of treating space security as a separate domain in its own right.

A few other papers touch on the subject (Hannan 2018; Ikitemur et al. 2020; Kallberg 2012; Kang et al. 2018; Santamarta 2014; Rose et al. 2022) but are specific to niche technologies or formal methods and hence do not adequately lay the general foundations for future research on space security and resilience.

2.2 Resilience Concepts

2.2.1 Critical Infrastructure Resilience

A whitepaper by the United States Office of the Assistant Secretary of Defense for Homeland Defense & Global Security entitled `Space Domain Mission Assurance: A Resilience Taxonomy' (United States Department of Defense 2015) gets particular attention amongst space resilience advocates, however it does little to set the scene before proposing a resilience taxonomy that is detached from tangential resilience literature. Additionally, and surprisingly, the whitepaper does not acknowledge the security landscape; with ‘cyber’, for example, not earning a single mention.

2.2.1.1 Critical Space Infrastructure

Critical infrastructure is defined differently by each jurisdiction around the world (Critical Five 2014), however it generally refers to any infrastructure on which society has a critical dependency and which, if disrupted, could cause significant and potentially catastrophic

consequences to the safety or security of that society. Space systems are increasingly being recognised as critical infrastructure by federal jurisdictions around the world, with a particular focus on satellites and satellite constellations as critical space infrastructure (CSI). For example, Australia's recent amendments to the Security of Critical Infrastructure Act (SOCI) includes the provision for Space Technology as a designated domain of critical infrastructure and necessitates a base level of security commensurate to other critical infrastructure domains, such as power or water systems (Australian Government 2018).

As our world becomes exponentially more complex critical infrastructures are faced with a growing number of new challenges. Societies are getting bigger and more technologically advanced, which is placing more demand on already strained and increasingly outdated infrastructure. Attempts to upgrade these infrastructures are adding even more complexities to the mix, such as the introduction of Internet of Things (IoT), machine learning (ML) and artificial intelligence (AI), third party software and solutions, and increasingly sophisticated interdependencies with other critical infrastructures, to name but a few. These challenges can make it difficult, if not impossible, to accurately assess causes of failure and to predict threats and impacts for risk management; making critical infrastructure resilience planning more important than ever.

Additionally, it is no secret that a large number of critical infrastructure systems rely on satellites for vital functions like time, geolocation, guidance, communications, and sensory data. Everything from guided munitions to air traffic control and banking to emergency services depend heavily on CSI to function safely and effectively. CSI also provides vital services, data, and imagery to government agencies and civilian populations who could all be significantly impacted in the case of an adverse event, potentially triggering mass panic or fear. Hence it can be understood that catastrophic consequences, including potential loss of life, are sure to follow any major disruptions to CSI; a clear case for its criticality to society (Georgescu et al. 2019).

2.2.1.2 Adapting Critical Infrastructure Resilience to Space Systems

Having established that space systems are indeed critical infrastructure, we can now look to other domains of critical infrastructure resilience to identify commonalities and define a space-specific approach.

There are many different types of critical infrastructure, each with its own peculiarities and approach to resilience, so it is useful to limit the comparative analysis to cyber-physical systems (CPS) only. A CPS includes any system that converts electronic signals to physical actions, such as a satellite receiving control signals.

Some prominent critical cyber-physical infrastructure (CCPI) domains include energy, water and wastewater, manufacturing, and transportation. Some examples of non-cyber-physical critical infrastructure may include the banking sector, the education and research sector, and some aspects of the food and grocery sector, such as supermarkets. For these reasons, not all critical infrastructure resilience literature may be relevant and a specific CCPI sector should be identified and utilised.

Of the CCPI domains, the energy sector stands out in the literature as having invested the most resources into their understanding of resilience (Fraccascia et al. 2018). Power systems also share the most similarities with space systems, such as: aging infrastructure, continuous availability requirements, remote and inaccessible components, vast distance coverage, centralised control, cascading failures (i.e., the Kessler Effect), and complex inter-system dependencies. It thus makes most sense to leverage power systems resilience literature in establishing a baseline understanding for space systems resilience.

2.2.2 Power Systems Resilience

2.2.2.1 Background

Across the globe electric power grids are being upgraded to incorporate modern technologies that promise to overcome a multitude of challenges that the legacy infrastructure is currently facing. Each of these new technologies introduce new complexities and vulnerabilities that can be exploited by adversaries looking to disrupt power supply to the targeted city. As witnessed in recent events in the Ukraine (Lee et al. 2016) and the US (Sobczak 2019), cyber-attacks against the electricity grid can cause prolonged and widespread outages, leading to significant economic costs, public distress, and loss of life (Maynard and Beecroft 2015; Moore 2008; Popik 2017; Wang 2019, p.17). Such attacks are predicted to grow in number and complexity (Glenn et al. 2016; Kshetri and Voas 2017; Kaspersky Lab 2019), with the World Economic Forum (2019) assessing that large-scale cyber-attacks are among the top 5 greatest global risks

affecting humanity in the next 10 years. Hence more severe consequences to the public can be expected without a commensurate increase in smart grid security and resilience.

Smart grid resilience is a relatively new field and thus there is a notable shortage of reputable literature to inform policy, guide public discussion, and drive engineering decisions. Although there are a number of research questions to be addressed in this space, this paper seeks to define Power Systems Resilience, laying the foundations for designing metrics to measure smart grid resilience. Without such a metric it is difficult, if not impossible, to implement appropriate security strategies that effectively combat cyber-physical threats.

2.2.2.2 Literature Search

Figure 2 shows the three overarching research domains related to smart grid resilience and demonstrates how they interrelate. In this figure the arrows are indications of cross-disciplinary research domains specifically relating to the cyber risk equation (i.e. resilience is concerned with minimising impact whilst the smart grid is the source of vulnerability). Based on this figure a large list of reputable journals from the three identified research areas was then compiled and systematically queried, in addition to the Google Scholar database, for keywords shown in the literature map at Figure 3.

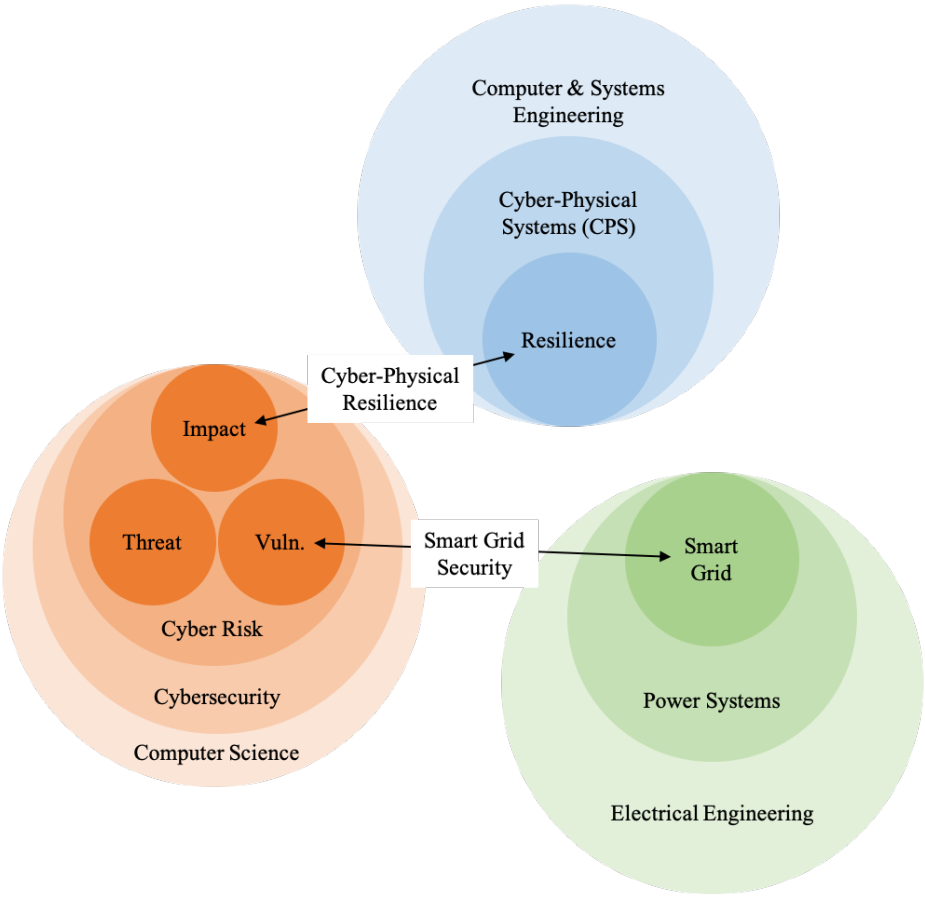

Figure 2 – Cross-disciplinary research interactions.

In the interests of thoroughness, the literature search was done in many stages, starting with combinations of broad search terms (i.e. based on the nodes furthest from the white topic circle in Figure 3) and progressively getting more specific and exclusive to the three key themes highlighted above (i.e. nodes closest to the white topic circle in Figure 3). Only results since 2014 were considered due to the quickly evolving nature of the field. Some definitions prior to 2014 can be found in the analysis by Wang et al. (2019) for historical reference.

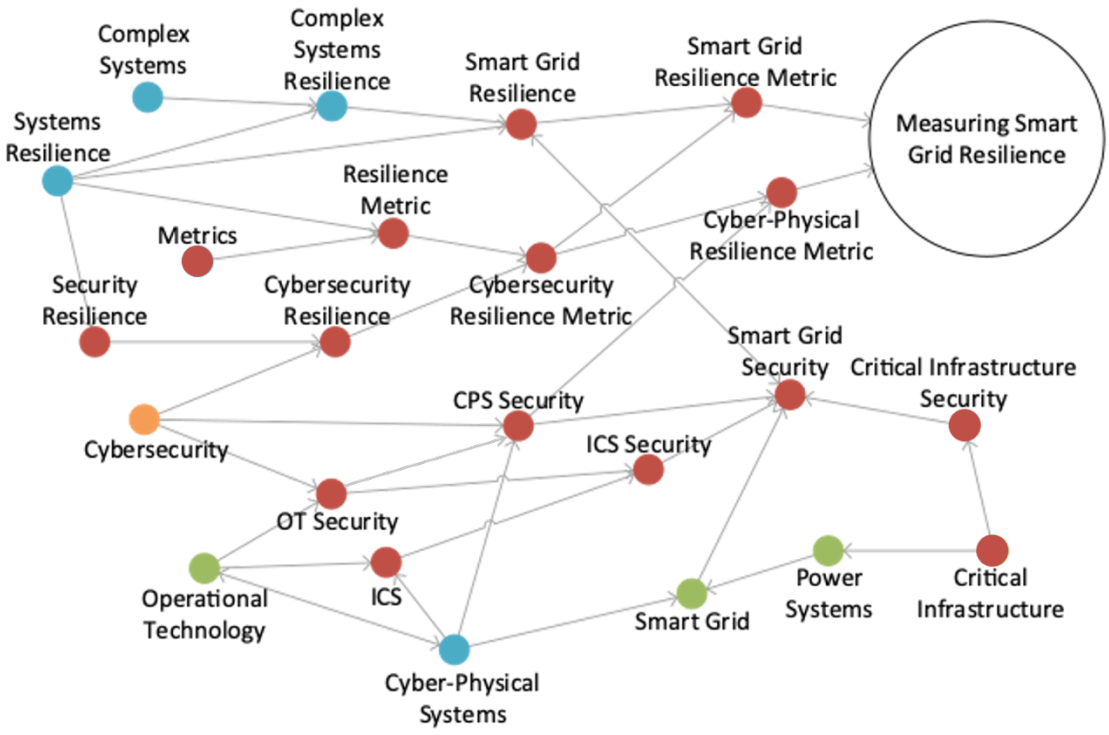

Figure 3 - Literature map used to generate search queries

Figure 3 presents a literature map used to generate search queries in the identified relevant literature databases. Blue points represent topics traditionally found in the systems engineering domain. Orange represents cybersecurity. Green represents electrical engineering. Red identifies strongly cross-disciplinary domains. Note that the diagram shown is for the purposes of this literature review only and is not a comprehensive representation of all cross-disciplinary links between each domain.

Overall, the search returned thousands of results with very few that were found to be directly relevant to the problem at hand (i.e., measuring smart grid resilience to cyber threat). As such, sufficiently related tangential literature was selected (i.e., more general Cyber-Physical Systems (CPS) resilience, or papers with a focus on non-cyber resilience such as weather resilience). From this pool 48 papers, reports, and books defining resilience metrics for systems akin to the smart grid were identified and analysed, with some further albeit older literature being identified through references. After deeper analysis 22 of these 48 papers were deemed irrelevant (due to lack of focus on either resilience, metrics, or systems) and the remaining 26 were categorised by threat and system type, as per Figure 3 (each column totals 26).

Threat		System	
Type	*Count*	*Type*	*Count*
Cyber	8	Power	17
Weather	4	Other Critical Infrastructure	4
Unspecified	14	Cyber-Physical Systems	3
		Complex Systems	2

Table 1 - Categorisation of applicable literature based on threat and system type.

Of all the research reviewed only four papers were specific to both cyber and the smart grid, so the analysis herein was conducted using the 26 broader papers mentioned above. This analysis revealed some valuable insights into the broader state of research on smart grid resilience, which are detailed in the following section.

2.2.2.3 History of Terminology

During analysis it quickly became evident that the exact definition of power systems resilience is still contested, adding a significant challenge to the problem of metric development. Notably, a number of trends began to emerge that demonstrated a significant and ongoing evolution in the understanding of power systems resilience and its resulting metrics within the last five years. These trends are summarised in the list below and expanded on in the subsections that follow:

1. Evolving definitions for power systems resilience;
2. Differing scopes for bounding variables in formal resilience equations; and
3. Diverging opinions on threat-specific metrics versus generic metrics.

2.2.2.3.1 Definition Convergence Over Time

Prior to circa 2016 the term resilience had been used inconsistently and often interchangeably with other related terms, such as reliability, recoverability, availability, robustness, and risk. This dilemma was highlighted by numerous papers published in this period; for example, Roege et al. (2014) showcase over a dozen papers with differing definitions, including presidential executive orders, and Eisenberg et al. (2014) explicitly acknowledge that multiple segregated definitions and theories had often led to a conflation of resilience and risk analysis at the time of publishing.

Some examples of terminology conflation that were seen in the pre-selected literature for this review include:

- Availability: Chiaradonna et al. (2014) consistently refer to resilience alongside Quality of Service (QoS) and define a resilience formula that only considers availability. Kwasinski (2016, p.93) takes this a step further and explicitly disregards all other aspects of resilience in favour of sole reliance on availability, claiming that all other factors are inevitably considered in a simple availability equation.
- Risk: In 2013, The White House of the United States defined resilience as "a risk management approach for critical infrastructure". It is also stated by Watson et al. (2014) that a resilience metric must include threat, consequence, and likelihood, which are the same components of a risk metric and is explicitly refuted in more recent literature such as Gholami et al. (2018) and Arghandeh et al. (2016).
- Recoverability: Albasrawi et al. (2014) base their definition on the one provided by Henry and Ramirez-Marquez (2012), who define resilience purely as "the ability of a system to bounce back from a failure".
- Reliability: the existing confusion between reliability and resilience is made evident by the repeated attempts in multiple papers to clearly distinguish between reliability and resilience. Over time the general consensus came to be that reliability is concerned with Low Impact High Frequency (LIHF) events, whereas resilience is exclusive to HILF events (Gholami et al. 2018; Arghandeh et al. 2016). It wasn't until late 2015 that the concept of High Impact Low Frequency (HILF) events, or Black/Grey Swans as defined by Gholami et al. (2018), started to appear repeatedly as a differentiating characteristic of resilience compared to reliability.

Over time these various interrelated terms became better defined, more distinct from one another, and thus used more consistently in the literature. However, despite the agreement that resilience isn't any of these things, there is still no clear consensus as to what it actually is (Shandiz 2020). From 2016 up until now the rhetoric around power systems resilience has begun to gradually converge around a combination of concepts such as anticipation, adaption, absorption, and recovery from HILF events. A chronological list that demonstrates this convergence is detailed in Table 2, with some noteworthy examples expanded on in the below list:

- Arghandeh et al. (2016) began with the problem statement, “there is no clear and universally accepted definition of cyber-physical resilience for power systems”, and then went on to define resilience as “the system’s ability to reduce the magnitude and duration of the disruption [given an unexpected set of disturbances]” by “downgrad[ing] its functionality and alter[ing] its structure in an agile way.”
- Friedberg et al. (2016), who base their definition on Arghandeh et al. (2016), state that “resilience in a system is rooted in two potentials. The absorbing potential is the degree in which challenges can be handled without performance degradation. The recovery potential describes a system’s ability to restore normal operation in the face of challenges.”
- Thompson et al. (2016b) detail the differences between security and resilience taxonomies, expanding on their earlier resilience definition of “the maintenance of the nominated state of security” (Thompson et al. 2016a), to state that “resilience is maintained if and only if a security breach is detected, contained and resolved.”
- Baros et al. (2017, p.10) also state that no formal definition of resilience had emerged but went on to state that resilience is generally accepted to be “the ability of a CPS to sustain and recover from extreme and severe disturbances that can drive the system to its physical operational limits.”
- Bie et al. (2017) yet again raises the lack of a formally accepted resilience definition, going on to define it as “the ability of an entity to anticipate, resist, absorb, respond to, adapt to and recover from a disturbance.”
- In a later paper, Friedberg et al. (2017, pp. 140–144) add to their 2016 paper to state that the “resilience of a system depends on three potentials. The absorbing potential (the ability to withstand negative effects), the recovery potential (the ability to recover nominal performance during or after a challenge) and survivability (the ability to prevent system collapse).”
- Gholami et al. (2018) define resilience in terms of avoidance, survival, and recovery with respect to a High-Impact Rare Event.
- Published in late 2018, Fraccascia et al. (2018) provide a comprehensive resilience literature review across a number of different complex systems domains and concludes that in every area, except ecology, a common definition of resilience is still to be agreed on. However, the authors also made a point to state that “some dimensions of resilience

(recovery and adaptive capacity) as well as some attributes of the systems (redundancy and connectivity) influencing resilience are shared by a number of research areas."

Since 2016, as can be seen in the list above and in Table 2, the general understanding of power systems resilience has been centred around a few common themes, albeit with varying terminology. Additionally, it is evident that the complexity of the definitions has generally increased with time, however this will be discussed further in subsections 2.2.2.3.2 and 2.2.2.3.3.

A list of proposed power systems resilience definitions over time is presented in the table below:

Reference	**Year**	**Resilience Definition**	**System Features**	**Threat Event Features**
Jackson and Fitzgerald (2016)	2016	"the ability of a system to degrade gracefully under extreme perturbations, and recover quickly after the events have ceased"	degrade gracefully, recover	extreme perturbations
Arghandeh (2016)	2016	"the resilience of a system presented with an unexpected set of disturbances is the system's ability to reduce the magnitude and duration of the disruption. A resilient system downgrades its functionality and alters its structure in an agile way."	reduce magnitude and duration of disruption	unexpected disturbances
Friedberg et al. (2016)	2016	"resilience in a system is rooted in two potentials. The absorbing potential is the degree in which challenges can be handled without performance degradation. The recovery potential describes a system's ability to restore normal operation in the face of challenges."	absorption, recovery	any challenge
Thompson et al. (2016a)	2016	"the maintenance of the nominated state of security"	security maintenance	-
Thompson et al. (2016b)	2016	"resilience is maintained if and only if a security breach is detected, contained and resolved"	detection, containment, resolution	security breach

Liu et al. (2016)	2016	"resilience focuses on low-probability, high-consequence events"..."extending the focus beyond preparedness, mitigation, response, and recovery, the measure of a resilient system should assess whether social well-being has indeed been preserved after a critical event."	preparedness, mitigation, response, recovery, preservation of social well-being	low-probability high-consequence events
Baros et al. (2017)	2017	"the ability of a CPS to sustain and recover from extreme and severe disturbances that can drive the system to its physical operational limits"	sustainment, recovery	extreme and severe distrubances
Bie et al. (2017)	2017	"the ability of an entity to anticipate, resist, absorb, respond to, adapt to and recover from a disturbance"	anticipate, resist, absorb, respond, adapt, and recover	any disturbance
Friedberg et al. (2017)	2017	"resilience of a system depends on three potentials. The absorbing potential (the ability to withstand negative effects), the recovery potential (the ability to recover nominal performance during or after a challenge) and survivability (the ability to prevent system collapse)."	absorption, recovery, survivability	negative effects, challenges
Panteli et al. (2017)	2017	"the ability of a system to anticipate and withstand external shocks, bounce back to its pre-shock state as quickly as possible and adapt to be better prepared to future catastrophic events"..."operational resilience, as its name suggests, refers to the characteristics that would secure operational strength for a power system, e.g., the ability to ensure the uninterrupted supply to customers or generation capacity availability in the face of a disaster. The infrastructure resilience refers to the physical strength of a power system for mitigating the portion of the system	withstand, bounce back, adapt	high impact low probability catastrophic events

		that is damaged, collapsed or in general becomes nonfunctional."		
Gholami et al. (2018)	2018	No succinct definition is provided, but the following statement is made which summarises the paper's perspective on resilience: "assess the resilience by evaluating the system performance in each sequential phase of the system temporal behavior (i.e., avoidance, survival, and recovery) following the given HR [High-impact Rare] event."	avoidance, survival, recovery	high-impact rare events
Zhang et al. (2018)	2018	"anticipate possible disasters, adopt effective measures to decrease system components and load losses before and during disasters, and restore power supply quickly. Additionally, valuable experience and lessons can be absorbed from disasters suffered, to prevent or mitigate the impact of similar events in future."	anticipate, adopt measures to decrease losses, restore, learn from experience	disasters
Hickford et al. (2018)	2018	"resilient infrastructure systems should be able to anticipate and absorb any disruptions, then adapt and recover quickly"	anticipate, absorb, adapt, recover	any disruptions

Table 2 - Examples of Power System Resilience Definitional Convergence Since 2016

2.2.2.3.2 Incongruent Scope

Outside of the definitional evolution detailed in Section 2.2.2.3.1, another inconsistency in the literature relates to what is considered in scope of the power systems' resilience formula. Most early literature defined power systems resilience in a purely technical manner, using primarily formal and mathematically-derived definitions. However, over the last five years an increasing number of papers have begun including human aspects in the scope of their resilience considerations. Aspects of this can be seen in the definitions in Table 2, however most papers discussed socio-technical aspects outside of the written language definitions themselves. For example, Liu et al. (2016) state that "a resilient system should assess whether social well-being has indeed been preserved after a critical event", and Kwasinski et al. (2016) consider human influence on power grid resilience "through the influence on the management and implementation of restoration, repairs, logistics and other processes". Additionally, Gholami

et al. (2018) state that “the defined performance index goes beyond the system’s technical characteristics and assesses the social welfare (e.g., the level of economic activity)”. Genge et al. (2015) consider Human-Machine Interfaces (HMI), and thus humans, as part of the control loop due to the human's ability to “influence the behavior of a physical process”. To highlight how resilience isn't purely a technical function, Eisenberg et al. (2014) provide an example where human bureaucracy between the Korean Power Exchange and the Ministry of Trade, Industry, and Energy exacerbated the size of the 2011 brown-out that left large portions of Seoul and other major metropolitan areas without power.

Most papers that extend their resilience definitions to include human components do so in terms of processes, such as planning, responding, and learning from experience (i.e., anticipate, recover, adapt); all aspects which understandably greatly impact a system's overall level of resilience and bear on the effectiveness of surviving and sustaining power delivery during an event and the efficiency of recovering and adapting post-event.

The definition proposed at Section 2.2.2.3.1 can easily incorporate both the mathematical and social aspects of resilience as the five components (anticipate, survive, sustain, recover, and adapt) are agnostic to either methodology.

2.2.2.3.3 Metric Conflicts

The third major area of contention in power systems resilience literature up until now is to do with the metric used to measure resilience. Understandably, given the lack of consensus surrounding the definition of resilience, there are just about as many competing resilience metrics as there are resilience definitions. Significant differences were observed between the various metrics depending on the definition statement (as at Section 2.2.2.3.1), the scope of consideration (as at Section 2.2.2.3.2), and the type of disruptive event against which resilience is being measured.

Where a generic event scope was set the proposed metrics also tended to be generic. Such generic resilience metrics were found to either be so high level that they were hardly measuring resilience (e.g. Kwasinski et al. (2016), where resilience is abstracted to the point of conflation with availability), or they considered elements that don't map very easily to cyber events – for example, Dessavre et al. (2015) refer to a ‘stress force’ that needs to be assigned to the disruptive event as part of the resilience metric. Additionally, Friedberg et al. (2017) include a

‘normative factor’ in their resilience definition for CPS, which is intended to be applied in a similar manner to the ‘stress force’ variable in order to normalise the intensity of disruptive events to allow for inter-system comparison. For extreme weather events, such as earthquakes, this can be applied in a straightforward manner through existing methods such as the Richter scale, however such precise and reliable scales don't yet exist for categorising disruptive cyber events.

On the other hand, specific metrics were, as one would expect, specific to the types of disruptive events and hence offered widely differing metric definitions. Resilience definitions that focus on weather events and climate change often include variables in their metrics that are unattainable or irrelevant for cyber-attacks (e.g., fragility curves based on weather intensity, physical resilience of infrastructure, exact start and end time of event, intensity of force applied to the system, or brace time for active preparedness leading up to an event (Panteli et al. 2017; Gholami et al. 2018). Those focused on measuring resilience to cyber events were either specific to non-power systems (e.g., Wadhawan and Neuman 2015, p.8), stopped short of defining an actual metric (e.g., Friedberg et al. 2015), didn't objectively assess resilience in a way that allows for comparison (e.g., Al Majali 2014), relied on data collection methods that are either theoretical in nature or are not widely available (e.g., Eshghi et al. 2015), are too generic to bear meaningful results across systems (e.g., Chiaradonna et al. 2014, which tried to account for both accidental and malicious events), or don't adhere to the resilience definition proposed herein (e.g. Clark and Zonouz 2019, which equates the state of security to the level of resilience).

In addition to the above issues, some papers (e.g., Eshghi et al. 2016) recommended modifying critical infrastructure networks to deploy agents or other advanced monitoring software in order to enhance the data gathering process for metric generation. Although this might be an available option for newly built power grids, the far more common application of resilience assessment applies to existing infrastructure where such modifications are not very pragmatic.

A number of papers recognised these issues and concluded that for a resilience metric to be usable it must be system and event specific. Recognising the need for a system-specific metric, Jackson and Fitzgerald (2016) state that “given the range of facets of resilience that are important in different application sectors, it is apparent that a nuanced characterisation of resilience is needed to facilitate disciplined engineering”. In the same paper they claim that “a

system cannot simply be said to either be resilient or not, but may be said to show some characteristics of resilience in response to a certain set of faults or attacks under certain circumstances". Chanda and Srivastava (2015) agree with Jackson and Fitzgerald (2016), stating that "resiliency is to be measured against some form of threat (e.g., weather, cyber-attack, terrorism, continuity of supply of raw materials, etc.)", and so does Bie et al. (2017), outlining that "the very first step to evaluate resilience is to identify the extreme events, as resilience is event specific". This common idea that resilience should be system and event specific is summed up nicely by Watson et al. (2014) with the statement that "resilience is always defined with respect to a disruption or threat. For example, an electric infrastructure system may be resilient to hurricanes, but that says little about its resilience to ice storms, cyber-attacks, or heat waves". In addition to the idea that metrics should be unique to each system and threat type some papers also highlighted that a resilience metric can be based on a multitude of different measures – for example, Friedberg et al. (2017) propose a metric that "allows to evaluate resilience with respect to different performance dimensions (e.g. monetary loss as well as system availability)".

Thus there exists somewhat of a tension between finding one common power systems resilience definition (i.e. the definition proposed at the end of Section 2.2.2.3.1) whilst simultaneously developing many different resilience metrics that are specifically tailored to the desired scope (as per Section 2.2.2.3.2) and disruptive event in question, as well as the organisational preference (such as financial vs operational based metrics). This does not invalidate the need for a common definition, but conversely necessitates that each assessing entity define their own purpose-specific metrics that align to the common definition provided in this dissertation.

2.2.2.4 New Taxonomy and Definition

The terminology describing the system features of a resilient system according to the literature, as highlighted in column 4 of Table 2, can be taxonomically grouped according to the common intention behind each word (for example, the words anticipate and preparedness can be understood synonymously in this context). The results of mapping these word relationships for resilient power systems can be seen in Figure 4. A noteworthy grouping is the terms absorb and resist, which are seemingly listed as separate features of resilience in the definition by Bie et al. (2017), as described at Table 2. However, referring to Figure 2 of the same paper, it can

be seen that both these attributes, along with various other attributes identified in the literature, pertain to different features of the same stage of resilience herein referred to as ‘Survive’.

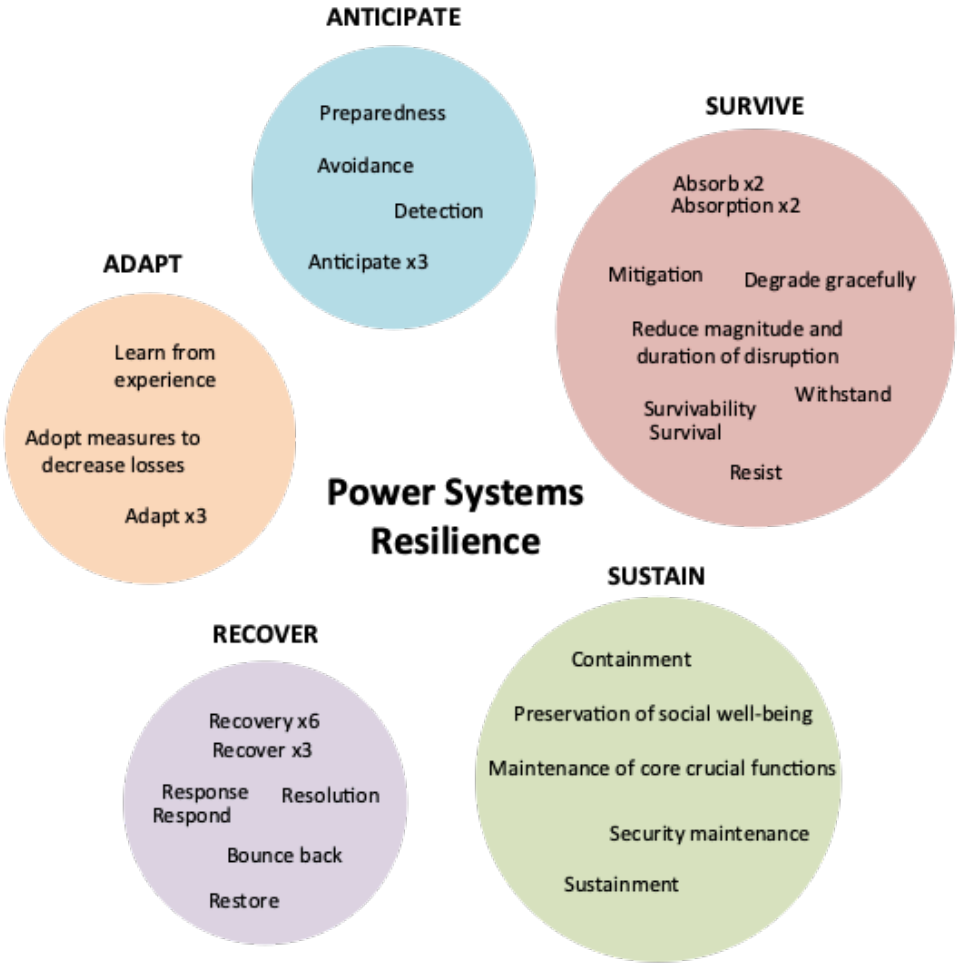

Figure 4 – Features inherent to resilient power systems

Figure 4 demonstrates the features inherent to resilient power systems, as defined in current literature, grouped according to synonymity. An 'x' is used to denote the number of occurrences where the term appeared more than once, with detailed definitions in Table 2. According to Figure 4, a power system should possess five common features to be considered resilient, including the ability to anticipate, survive, sustain, recover from, and adapt to a given threat event. These five features therefore become the basis for a newly proposed power systems resilience taxonomy, as per Figure 5. The scope of what constitutes a ‘power system’ is varied and is discussed further in Subsection 2.2.2.3.2.

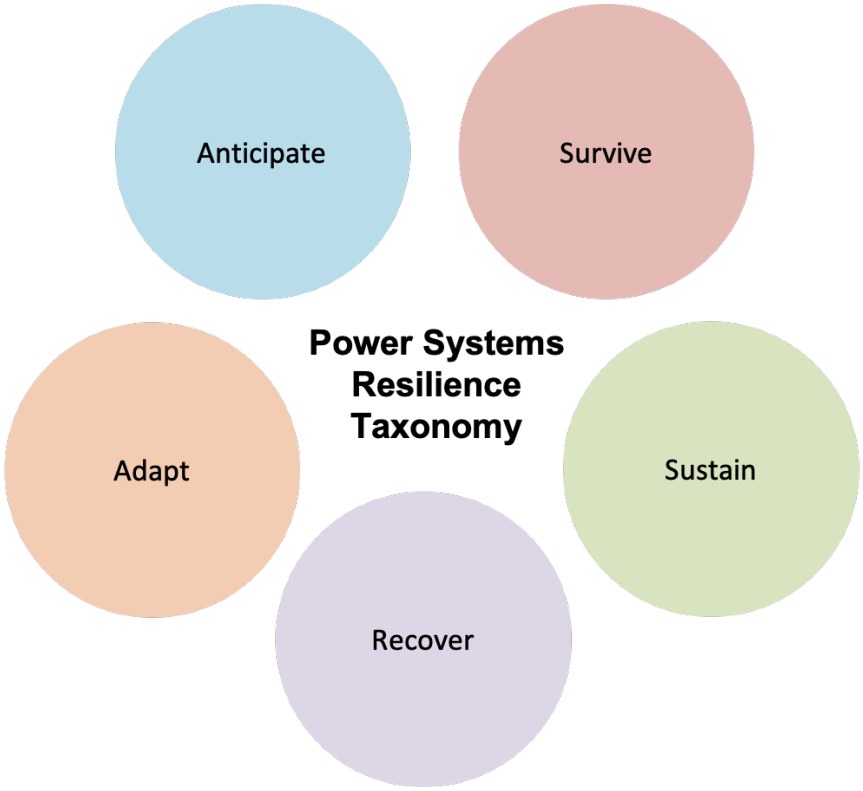

Figure 5 – Power systems resilience taxonomy.

Existing literature contains variations in terms of the types of events to which a power system should be resilient to, as can be seen in column 5 of Table 2. Power systems face a multitude of different types of events, ranging from frequently occurring minor disturbances (i.e. LIHF events) all the way through to rare disasters (i.e. HILF events). Although a power system should and must successfully survive any adverse event that occurs, most surveyed literature agreed that resilience is focused solely on HILF events whilst other disciplines are tailored to cover off on the rest (e.g. reliability is concerned with surviving LIHF events and risk management focuses on mitigating high consequence high likelihood events, accepting low consequence low likelihood events, and monitoring everything else).

In light of the increasingly established distinction that resilience concerns itself with HILF events, the threat event definitions provided in the power systems resilience literature were mapped onto a risk chart in Figure 6, whereby four quadrants are mapped against two low/high binary scales representing likelihood and consequence (i.e. low likelihood low consequence = acceptable risk, high likelihood low consequence = reliability management, low likelihood high consequence = resilience management, high likelihood high consequence = unacceptable risk). This figure highlights the commonalities between provided definitions but also identifies

where some definitions were broader than the general consensus regarding HILF events. Definitions that were found to be too broad to belong to any one particular quadrant have been denoted with an asterisk.

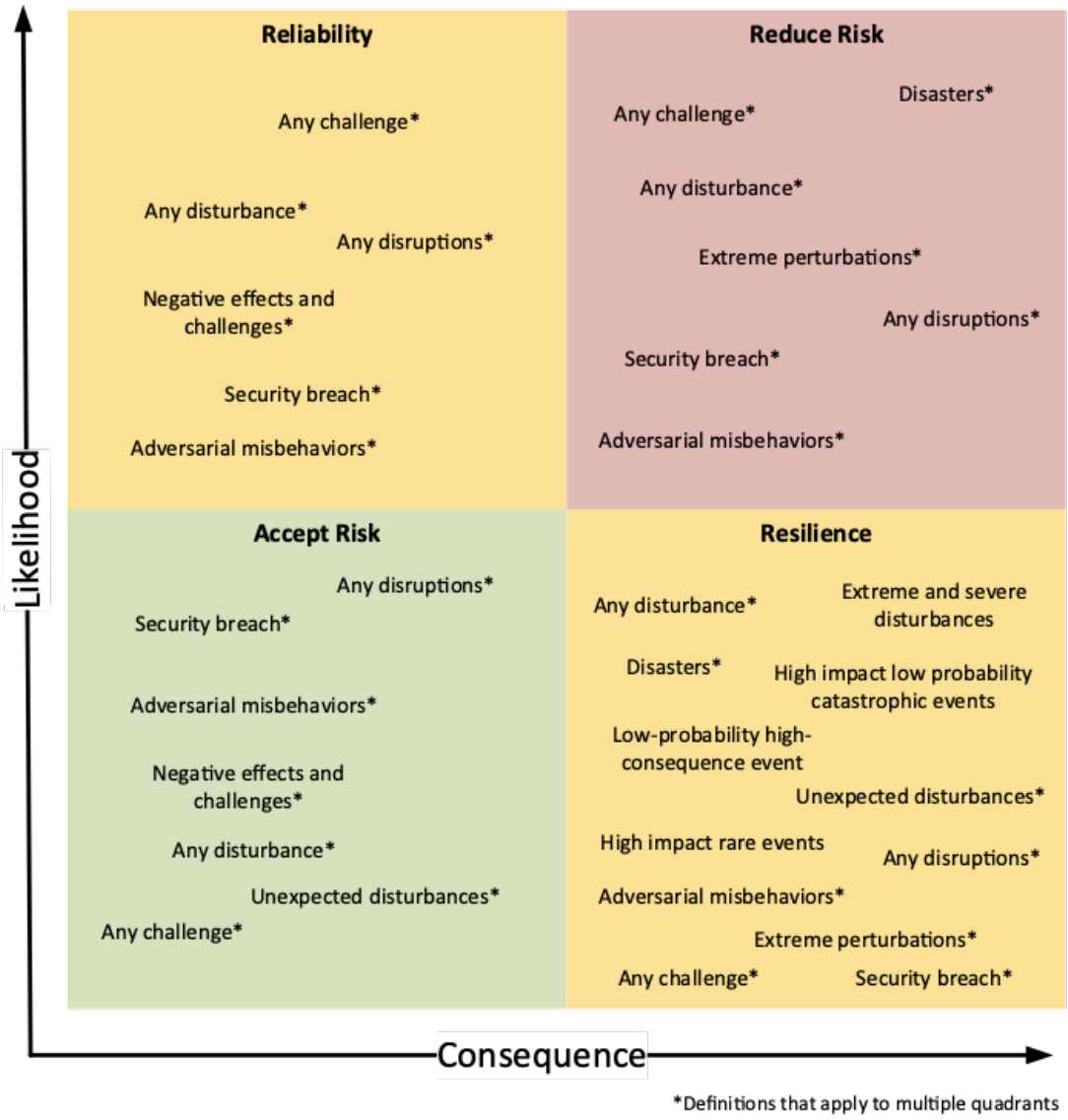

Figure 6 – Risk Comparison of Resilience vs Reliability

Figure 6 above demonstrates types of events that resilient power systems should anticipate, survive, sustain, recover from, and adapt to, as defined in the literature. Each event definition has been placed in a risk quadrant based on the consequence and likelihood described respectively.

As can be seen in Figure 6, every threat event type specific enough to belong to only a single quadrant (i.e. without an asterisk) falls in the 4th quadrant (low likelihood high consequence) titled “Resilience”. This demonstrates that throughout the power systems resilience literature, either the resilience definition doesn't include a specific threat event type, or it specifically defines HILF events as the threat that resilience aims to deal with.

Given the findings discussed above and summarised in Figure 5 and Figure 6, Power Systems Resilience may be universally defined as:
“the recurring ability of a power system to anticipate, survive, sustain, recover from, and adapt to high impact low frequency events”

As suggested in the above definition, resilience occurs on a cyclical basis whereby the default state is ‘Anticipate’, as depicted in Figure 7 and Figure 8.

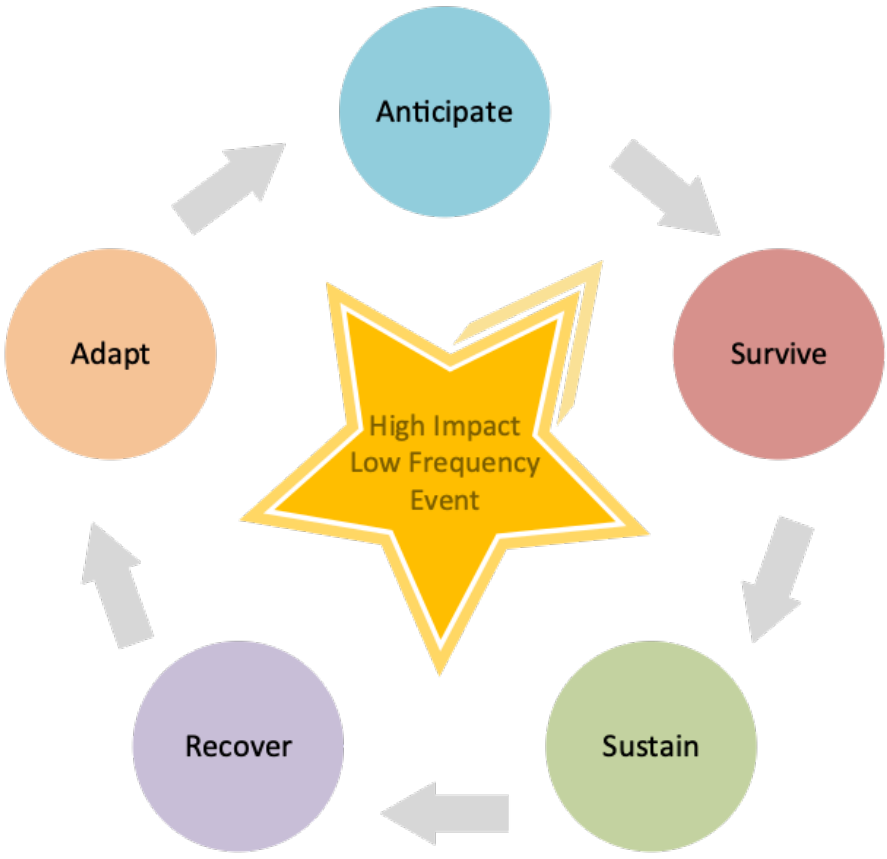

Figure 7 – Resilience taxonomy represented as a cycle.

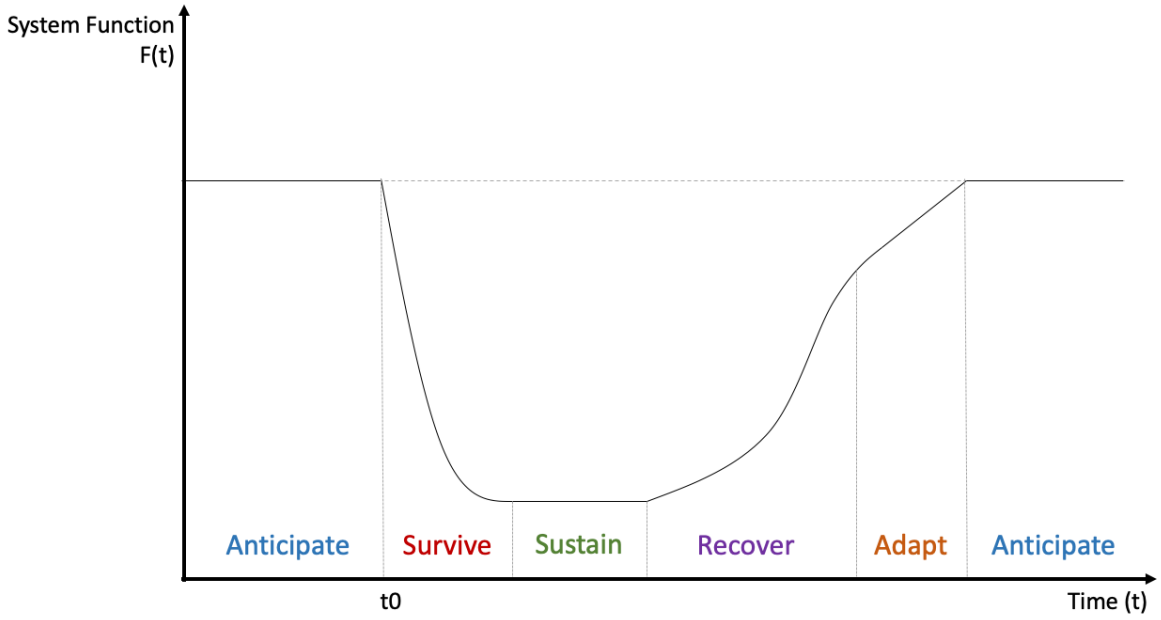

Figure 8 – Resilience cycle plotted against system function over time, where a HILF event occurs at time t0.

2.2.3 Space Systems Resilience

2.2.3.1 Taxonomy

With an understanding of both the criticality of space infrastructure and the unpredictable threat environment within which it is situated, it is easy to see the importance of resilience in space systems. In fact, there are a number of niche areas within space resilience that have already been studied to some degree, such as: satellite resilience (Ormrod et al. 2021, p.257), operations resilience (McLeod et al. 2016), mission resilience (Straub 2014), material and structural resilience (Naser and Chehab 2018), software resilience (Phillips et al. 2018), among others. Each of these different aspects of space resilience were researched according to individual definitions, meaning that the overall space system resilience picture becomes diluted and incoherent.

A more reliable strategy is for each of the various aspects of space resilience to reference a common baseline space resilience definition. As discovered in Section 2.2.2, system resilience is a function of anticipating, surviving, sustaining, recovering from, and adapting to HILF events. Additionally, resilience should account for socio-technical factors and be broad enough to allow for tailoring to each specialist subdomain's metric measurement needs.

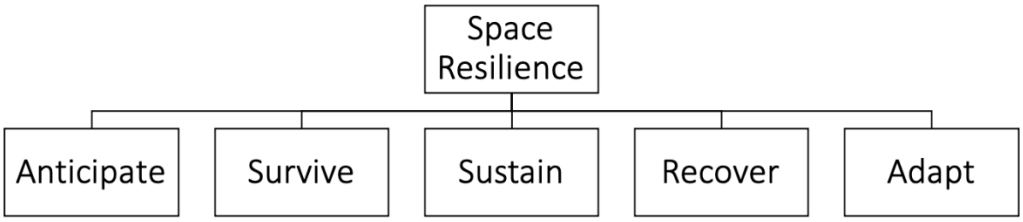

Figure 9 – Space Resilience Taxonomy

Before attempting to define resilience for space systems, it is helpful to understand it from a taxonomical perspective. This aids in breaking the problem of resilience down into smaller focus areas for easier measurement and management, as per Figure 9. This taxonomy can be agnostically applied to any niche area of space resilience, where:

- Anticipate refers to the resilience enhancing mechanisms in place to prevent, detect, and avoid HILF events
- Survive refers to the resilience enhancing mechanisms in place to mitigate, absorb, and withstand the impacts of the HILF event
- Sustain refers to the resilience enhancing mechanisms in place to contain any impacts and preserve core functions during a HILF event
- Recover refers to the resilience enhancing mechanisms in place to respond, restore operations, and 'bounce back' from a HILF event, and
- Adapt refers to the resilience enhancing mechanisms in place to reflect on lessons learned and adopt new mechanisms to increase resilience for any similar events in future.

Not all five aspects of space resilience will be relevant to every system subcomponent or supporting function, but each subcomponent and supporting function is relevant to the system's resilience as a whole. For example, anticipation is a difficult mechanism to embed into structural integrity designs, but a structurally resilient bus will feed into the overall space system's ability to survive and sustain core functionality during a HILF event.

2.2.3.2 The Resilience Cycle

These five taxonomical categories can also be understood as phases within an indefinitely recurring resilience cycle, as per Figure 7. The residual impact seen in this figure refers to the post-event impact after resilience enhancing mechanisms have mitigated the impacts of a HILF

event. As shown, the residual impact can both weaken overall system resilience as well as going on to cause impacts external to the space system, such as to the wider mission or social well-being.

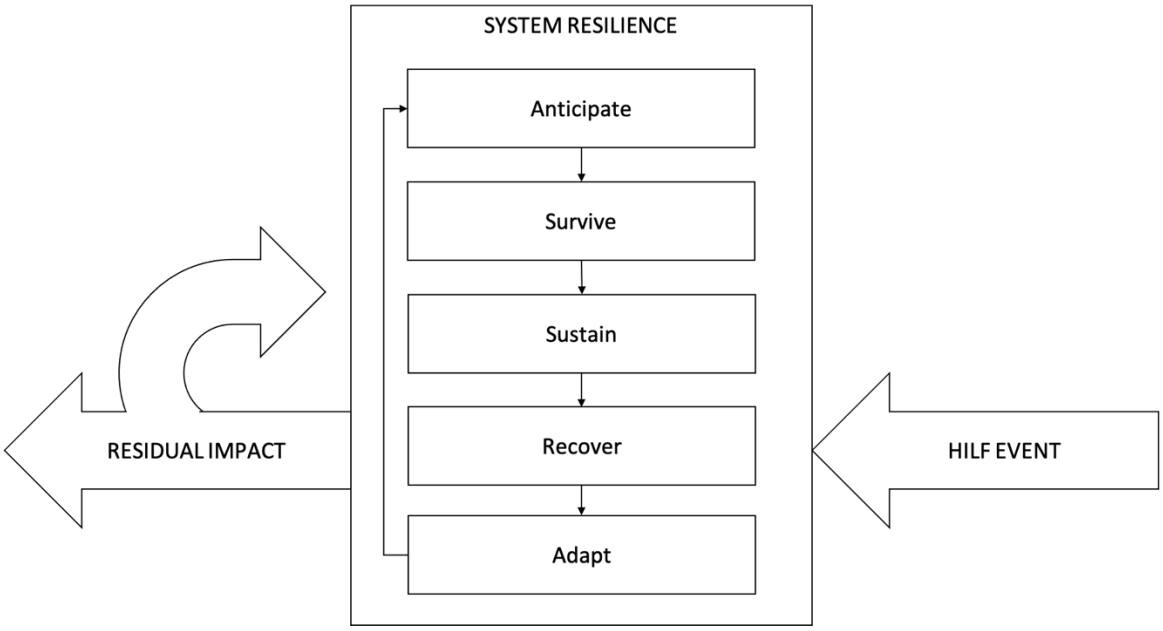

Figure 10 – Resilience cycle in response to High-Impact Low-Frequency (HILF) threats

2.2.3.3 Definition

With a preliminary space resilience taxonomy and understanding of how each resilience aspect cyclically interacts, a preliminary definition may be established as follows:

Space resilience is the recurring ability of a space system, including all sub-components and supporting functions, to anticipate, survive, sustain, recover from, and adapt to high impact low frequency events.

2.3 Space Security Threats

2.3.1 Types of Space Systems

There are an increasing number of innovative space systems being developed as part of the second space race commercial push. As far as space systems knowledge is concerned, most literature focuses on satellite systems, particularly PNT satellites, and ground stations. This often leaves a gap for innovation that is being witnessed in industry at present, for example; orbital factories or Martian rovers. For the purposes, and due to the resourcing limitations, of this research dissertation, the focus of this section will be skewed towards satellite systems due

to available research. The potential for future research on this matter is discussed in Section 6.2.

Georgescu et al. split CSI into five key categories (Georgescu et al. 2019a, pp. 21–36):

- remote sensing;
- communications;
- meteorological;
- Global Navigation Satellite Systems (GNSS); and
- administrative and legislative frameworks.

The technological systems falling under each of these categories are predominantly artificial satellites, but can also include space stations, rovers and vehicles, rockets, space probes, ground stations, and terrestrial communications links. Naturally each of these systems have various unique processes, technologies, and vulnerabilities.

Remote sensing involves the passive or active collection of data about a subject of study without making physical contact. Space infrastructures that fall under this category include systems that conduct surveillance, scientific monitoring, or information gathering for things like terrain mapping and military reconnaissance. For the purposes of this dissertation, this may also include interplanetary rovers such as lunar or Martian rovers. These kinds of systems are particularly vulnerable to laser attacks as they allow for electromagnetic penetration to achieve their primary function (Georgescu et al. 2019a).

Communications Satellites (COMSAT) provide global telecommunications coverage and are useful for aviation and long-distance connections where earth's curvature inhibits the line of sight; communications which if interrupted could result in significant loss of life here on earth. A study done by Steinberger at the US Joint Electronic Warfare Center found that the most vulnerable component of satellite communications infrastructure is the antenna, which exposes the satellite to attacks such as jamming or spoofing (Steinberger 2008). The earth segment was also found to be particularly vulnerable to jamming, but also to threats stemming from internet connectivity.

Meteorological space infrastructures are generally used to monitor Earth's climate and weather and are critical for tasks like extreme weather prediction and monitoring. These satellites are generally quite minimal in build as their primary purpose is simply to transmit photos and meteorological data to earth. There is yet to be any published research specific to meteorological satellite vulnerabilities, however due to their simple anatomy it can be inferred that they share general commonalities with other satellite systems.

GNSS includes navigation, positioning, and timing applications, and is perhaps most recognisable in satellite technologies such as the Global Positioning System (GPS). GNSS are heavily relied on by terrestrial applications such as the electric grid and guided weapons systems, whereby a satellite failure could cause far-reaching and catastrophic consequences, including loss of life. Due to the relatively long history of such systems, satellites delivering GNSS capabilities have been privy to greater levels of security research compared to other space-based systems. Across the literature jamming and spoofing surface as the primary vulnerabilities of GNSS (Ioannides et al. 2016; de Abreu Faria et al. 2016; Amin et al. 2016).

Administrative and Legislative Frameworks are undoubtedly a quintessential component of CSI and are also notably immature at this point in time (Planck 2009). A growing number of countries around the world are recognising space systems as critical national infrastructure and hence the administrative and legal frameworks to support them are gaining global attention and prioritisation. One notable example is The Woomera Manual project, which is an international research collaboration to articulate existing international laws applicable to military space operations (Stephens 2021). Recent times have also seen some security standards and policies being adapted to the space environment, such as the NIST Cyber Security Framework (CSF), however to date no standards have been designed exclusively to guide space security or resilience governance as a whole (Tsamis et al. 2021). Space as a legal domain is notoriously complex due to its international significance and lack of any divisible territory (del Monte 2013). For space security purposes this category functions as more of a supporting component because, although frameworks are not targetable by a threat actor, they can aid in data collection and retention standards, post-compromise forensics, and attribution, prosecution and retaliation.

2.3.2 Space Threat Environment

Space systems operate in one of the most naturally hostile environments known to man, constantly facing threats such as electromagnetic radiation and space debris. In addition, systems deployed in space also face a variety of unique challenges that don't commonly apply to terrestrial infrastructure, such as lack of redundancy or maintenance options (Georgescu et al. 2019). Although non-malicious threats should definitely be considered when risk assessing space technologies, this is outside the scope of this dissertation. There is plenty of literature available to help guide environmental threat assessments of space infrastructure however there is a notable lack of literature discussing the malicious threats, particularly with respect to cyber security, which are detailed herein.

When discussing targeted threats it is helpful to break them down into three components:

- the actor;
- the vector; and
- the attack.

The threat actor is the person or organisation behind the attack and can be assessed by considering their capability to conduct an attack versus their intent behind the attack. The threat vector refers to the vulnerable point of entry used by the threat actor to successfully carry out the attack; for example if a ground system is air gapped (i.e., not connected to any network) then the threat vector may be a flash drive. Finally, the attack itself is the exploit used by the threat actor to achieve their objectives and cause the desired impact, for example malware or spoofing. This is visually summarised in Figure 11, whereby the threat vector is the actor's entry to the system, on which the attack is conducted, and from which the impact extends back to the environment.

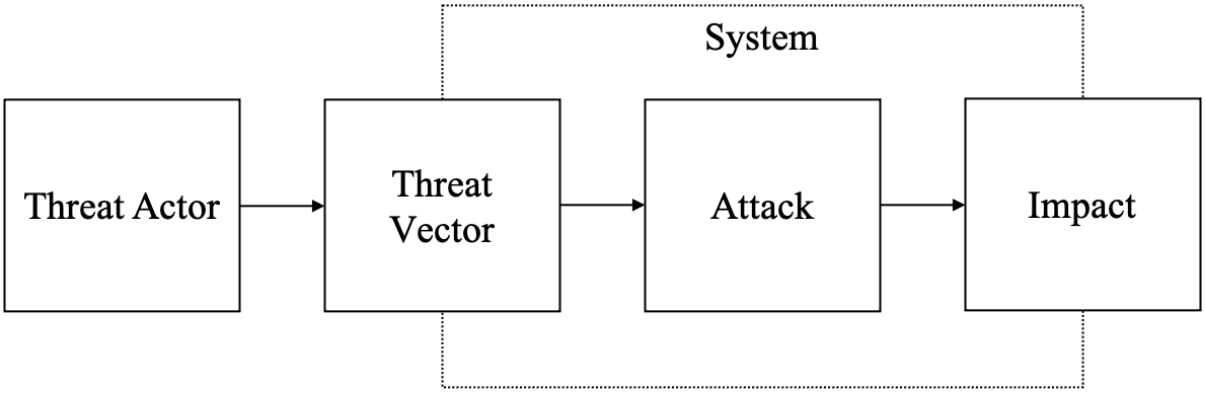

Figure 11 – Anatomy of a targeted threat

2.3.2.1 Threat Actors

Although a formal threat actor taxonomy is yet to emerge in the literature, a threat actor is generally categorised as one of the following (Livingstone and Lewis 2016):

- nation-state;
- terrorist;
- criminal group; or
- individual (e.g. insider threat or 'lone-wolf' hacker).

Sometimes hacktivism occurs on a larger scale (e.g., Anonymous) and can be treated as a separate category, conforming to neither terrorist nor criminal motivations. Bradbury et al. (2020) broke these high-level categories down further and provided space-specific examples in Figure 12. As this figure demonstrates, each actor type has their own intent (e.g., goals & motivations) and capability (e.g., capabilities, environment, resources) that drives their decision-making process when considering the carrying out of a cyber attack against targeted space infrastructure. Pavur and Martinovic (2020) produced a similar yet simpler version of this threat actor table, expanding beyond just cybersecurity considerations in Figure 13.

	Threat Actor	Example	Goals & Motivations	Capabilities	Environment	Resources
Individual	Outsider	Hacktivist	Personal satisfaction; Passion; Ideology. Doesn't believe in climate change, wants to impact functioning of climate satellite	Limited	Remote access	Minimal
	Insider	Cleaner	Financial gain; Discontent	Limited	Permission-less internal access	Internal knowledge
	Trusted Insider	Contractor	Financial gain; Discontent	Moderate	Internal access with some permissions	Internal knowledge
	Privileged Insider	Employee	Financial gain; Discontent	High	Internal access with high permissions	Internal knowledge
Group	Ad hoc	A group coming together over a time-critical event (e.g. Brexit, or a collective movement of Extinction Rebellion)	Dependant on group purpose: Ideological, financial, political	Limited to Moderate	Remote access	Limited knowledge and financial
	Established	A group(e.g. the Anonymous group)		Moderate to High	Remote access	Moderate knowledge and financial
Organisation	Competitor	An organisation about to compete for a tender for services	Corporate espionage; Financial gain; Reputation damage	Organisation size related	Remote access	Organisation size related
	Supplier	A supplier who fears their services are soon to be relinquished	Information gain; Financial gain		Remote access; Knowledge of internal structure	
	Partner	A partner with whom a relationship is starting to sour or is soon to end	Information gain; Financial gain		Limited internal access; Knowledge of internal structure	
	Customer	A customer who feels they have had poor or unfair service	Information gain; Financial gain		Remote access; Knowledge of internal structure	
	Nation-State	Geopolitical rival	State rivalry; Geopolitics	Sophisticated; Coordinated; Access to state secrets	Remote and internal access	Extensive knowledge; Extensive financial; Advanced equipment

Figure 12 – Threat actor examples by Bradbury et al. (2020)

Attacker Type	Example Motivations	Technical Capabilities
National Military	• Space Control • Anti-Satellite Weapons	High
State Intelligence	• Counter-Intelligence • Technology Theft • Eavesdropping	High
Industry Insiders	• Sabotage • Technology Theft	High
Parts Suppliers	• Sabotage • Espionage	High
Organized Crime	• Eavesdropping • Ransom • Technology Theft	Moderate
Commercial Competitors	• Sabotage • Technology Theft	Moderate
Terrorists	• Societal Harm • Notoriety • Message Broadcasting	Low
Individuals	• Notoriety • Personal Challenge	Low
Political Activists	• Message Broadcasting	Low

Figure 13 – Summary of Satellite Threat Actors by Pavur and Martinovic (2020)

2.3.2.2 Threat Vectors

Threat vectors need to be assessed on a case-by-case basis as every system will have its own processes and procedures, inputs and outputs. Wheeler et al. identify four common attack surfaces for deployed space systems (Wheeler et al. 2018):

- inputs (e.g. sensors and RF antennae);
- outputs (e.g. telemetry transmitters);
- internal communications (e.g. Spacewire buses); and
- computing (e.g. the internal system that integrates each components).

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. Bradbury et al. (2020) propose a reference architecture for assessing space system threat vectors and attack surfaces.

2.3.2.3 Malicious Space Threats

Targeted attacks to space infrastructure can be broken down, as per the threat assessment published by Harrison et al. (2020), into:

- kinetic physical;
- non-kinetic physical;
- electronic; and
- cyber.

In this context, both kinetic and non-kinetic physical threats aim to impact the physical components of a space system. The difference between the two is somewhat self-explanatory, with kinetic referring to tangible threats such as anti-satellite (ASAT) missiles and non-kinetic referring to intangible threats such as lasers and EMP weapons. It's worth noting here that kinetic weapons are particularly risky as any ensuing space debris could cause a cascading failure, where one collision leads to the next and a large number of satellites are suddenly transmorphed into space junk; including your own ones (Wright et al. 2015).

Electronic threats do not aim to have a permanent physical impact, and so are not to be confused with non-kinetic physical threats that do. An electronic threat generally involves interfering with RF signalling, for example signal jamming or spoofing, to interfere with the availability or integrity of communications, with the consequences to the space infrastructure itself usually being temporary.

Finally, cyber threats seek to interfere with the confidentiality, integrity, or availability of space infrastructures through the manipulation of data and code. Cyber threats are the most flexible of the categories, with a wide range of malicious options and outcomes available to the adversary (Pavur and Martinovic 2020, Falco et al. 2021). Different types of satellites, such as LEO, GEO, or MEO, may also have differing vulnerabilities to cyber attacks given the differences in system architecture and space vehicle design required to achieve the differing mission objectives. For example, many satellites being launched into LEO orbit are smaller and have shorter lifespans, such as CubeSats and NanoSats, and therefore may be more susceptible to attacks against the onboard power system (Falco et al. 2021). However, given the smaller coverage LEO and MEO offers, these satellites are also more likely to be part of a constellation which could have positive outcomes for mission resiliency. GEO satellites, by

contrast, are often bigger and more expensive than LEO and MEO but are more susceptible to single-point failures. However, GEO satellites may provide enough power to run specialised cyber monitoring or alerting software as well as to incorporate redundancy in the onboard design in case of failure.

2.3.2.4 Cyber Attacks

Cyber-attacks are rapidly growing in occurrence and severity due to their accessibility, affordability, and the increased level of control an actor has over the impact compared to alternative forms of attack. As such cyber-attacks deserve special attention when researching threats to space systems. There are many resources available with literature regarding cyber-attacks, however to understand the anatomy of a cyber attack it is common practice to refer to what has become known as the Cyber Kill Chain (CKC). The CKC is a conceptual model invented by Lockheed Martin to understand the various stages of a cyber attack (i.e., reconnaissance, weaponisation, delivery, exploitation, installation, command & control, and actions on objectives), and helps to analyse attacks and attack vectors for prevention and incident response. In a conference paper, Van der Watt and Slay (2021) adapted the CKC model to Low Earth Orbit (LEO) satellites; a useful reference for developing a detailed cyber threat model (Van de Watt and Slay 2021).

2.3.3 Threat Model

Pulling together the different research threads identified in Section 2.3.2 paints a picture of the current state of space security as a domain, but also serves as the foundation for building a space-cyber threat model. As shown in Figure 14, we have gathered a preliminary understanding of attack surfaces, threats, and actors, as well as past events and future predictions which are not shown in the diagram.

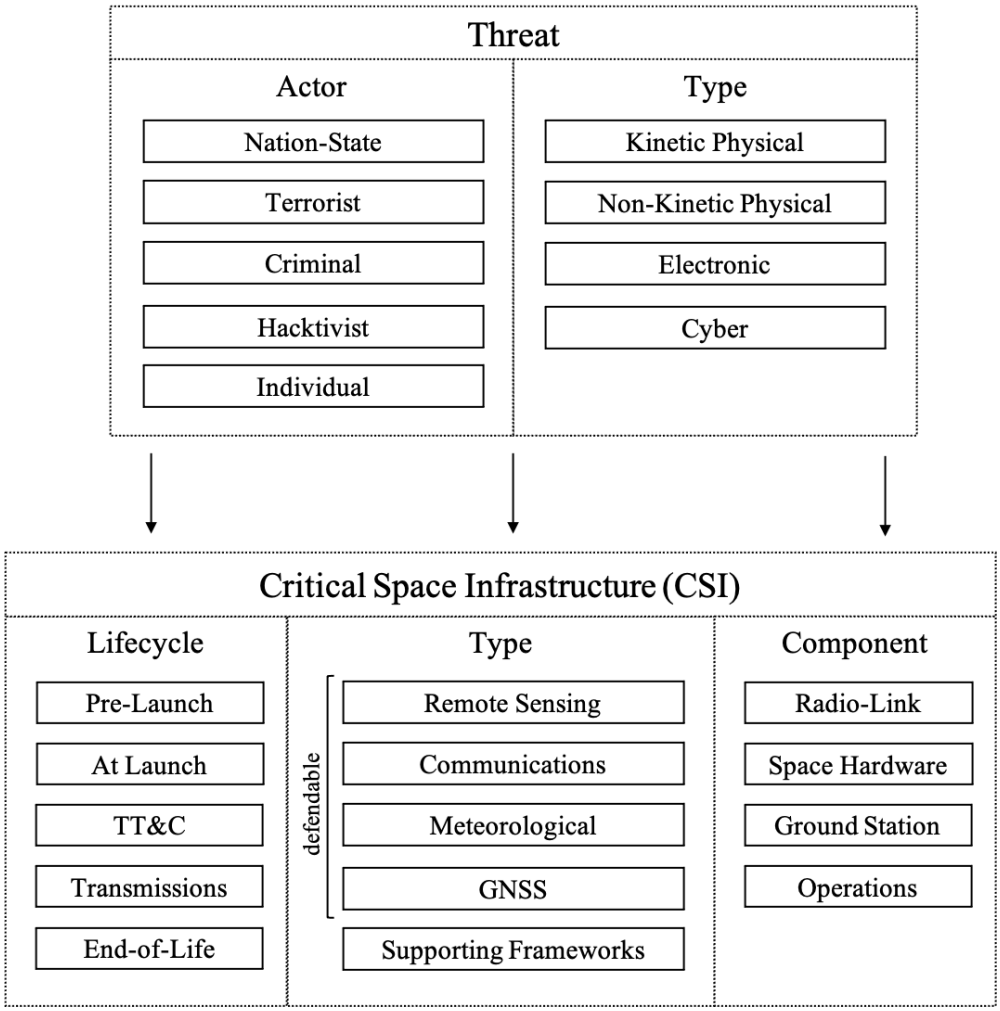

Figure 14 – Threats to CSI broken down into taxonomical sub-categories as per available literature

2.3.3.1 Selecting the Threat Model

In reference to Figure 14, modelling the threat to space systems requires an understanding of the upper box, 'Threat', in relation the lower box, 'CSI'. Ordinarily, assessing a threat environment for the purposes of generating a detailed model should account for every known threat combination, mapped against every known combination of the target system's type (i.e., mission), lifecycle stage, and component category. For the purposes of this thesis, however, a full-scale threat model is not feasible and so this dissertation focuses primarily on cyber-type threats that seek to cause physical impacts; herein referred to as cyber-physical attacks.

Scoping out threat actors presents a different challenge as there are no immediately obvious candidates for exclusion from, or inclusion in, the study. It would provide most utility to identify a single threat to model resilience against, preferably one with the most potential to cause large impacts to each aspect of resilience identified in Section 2.2.3. This method not

only allows for more efficient verification and validation of the resilience assessment framework, but also provides a threat-agnostic approach to practitioners wishing to study a space system's resilience without deep knowledge of its threat environment.

One approach is to model the threat actor with the highest technical capabilities to carry out an attack. In this regard, Figure 13 suggests that Nation State and Criminal threats (including threats from malicious competitors and industry insiders) have the highest technical capabilities to carry out an attack, with all other threats being assessed as moderate to low capability. An issue with this scoping approach, however, is that it does not take into account the motivations of the actors to cause noticeable impacts. In both cases of nation state and criminal oriented threats, there generally exists little desire for the actors to be discovered on the network – assuming that the assessment takes place during a period of peace or cold war, where covert operations and Advanced Persistent Threats (APT) are much more likely and valuable. Additionally, this modelling approach requires some-what up-to-date intelligence on threat actor capabilities within the given threat environment. Although possible, such intelligence is often expensive and speculative.

State actors engaging in cyber warfare activities against critical space infrastructure has been observed in recent times (Pearson 2022), which further emphasises the points made above. Namely, the intent of a state actor to cause damage is largely politically motivated and so the desired outcomes of a related cyber-physical attack may shift depending on a wide range of unpredictable factors. This in no way is to say that nation-state actors should remain unconsidered in future threat modelling. However, in consideration of the primary objective of this research being the resilience framework itself, a complex threat actor for the case study threat model may prove undesirable within the constraints of the project.

Noting the above, a second modelling approach is to select the threat actor with the highest motivation to cause resilience-related impacts to space systems. Although trusted insiders (i.e., the most powerful of the "Individuals" threat category) can certainly deliver severe damage to a targeted system, the associated threat is too broad given virtually unlimited access to the system in question, and hence must be managed through separate internal, and often procedural, security controls.

The final two threat types, ‘Terrorists’ and ‘Hacktivists’, present intriguing prospects for modelling against. Both have similarities in their motivation to disrupt systems and processes in pursuit of their goals. Indeed, hacktivism is so poorly defined that security professionals often group hacktivism under the banner of terrorism. For example, a politically motivated hacktivist may attempt to hack satellite communications to prevent a particular broadcast from taking place; as has already previously occurred (Knittel 2013). The key distinction between a hacktivist and a terrorist is that terrorists will often intentionally inflict damage or harm in pursuit of their goals (Plotnek and Slay 2021b), whereas a hacktivist will generally opt for less violent methods due to the difference in intent.

Therefore, in consideration of the various aspects factoring into what constitutes an ‘ideal threat’ against which to test the resilience framework, terroristic cyber-physical threats offer the most theoretical potential as a case study due to their preoccupation on unhindered disruptive and destructive techniques. Thus, cyber terrorism will be explored in the following section with the intent to build a descriptive threat to model the resilience framework against.

2.3.3.2 Cyber Terrorism

The threat of terrorism has been increasingly publicised as being one of the biggest threats to western society (Australian Government 2017; Kellner 2015), with media conjecture about cyber-terrorists and nation states causing widespread damage and mayhem contributing to public fear and driving potentially misdirected security countermeasures (Jarvis et al. 2016; Nacos 2016). The fact that cyber acts are notoriously difficult to attribute to specific actors accurately and definitively, and that, even if attributed, geolocation and prosecution rarely succeed, makes cyber terrorism highly attractive to terroristic minds.

Cyber terrorism is a relatively young field and hence there is a notable shortage of reputable literature to inform policy, guide public discussion, and drive decision-making. One fundamental issue that remains unsolved and is delaying all other developments in this area is the question of definition – what is cyber terrorism? A number of definitions have been proposed since the mid-eighties, however none of these definitions have proved sufficient for universal agreement and adoption. The goal of this section is to analyse the major definitional contributions over time in order to propose a unified definition, grounded in existing literature and current usage.

2.3.3.2.1 History of Terminology

There is no universally accepted definition of cyber terrorism. The term cyber terrorism was first coined in the mid-eighties by Barry C. Collin, a senior person research fellow of the Institute for Security and Intelligence in California (Akhgar et al. 2014). Collin had, at that time, defined cyber terrorism simply as "the convergence of cybernetics and terrorism". Due to this definition's over-simplicity and resulting lack of specificity, a myriad of other attempts at defining cyber terrorism have since emerged in the literature. The confusion surrounding cyber terrorism is even more-so apparent in public discourse and media usage; as examined in depth in by Jarvis et al. (2016), where the authors analysed 535 articles across 31 media outlets that used the term cyber terrorism between 2008 and 2013.

A large proportion of the definitions available in the literature have arisen out of the need for jurisdiction-specific legal terminology to aid with deterrence and prosecution of would-be cyber-terrorists (Hardy and Williams 2014). Another driving factor that complicates the ability for a unified definition includes the ongoing evolution and widely acknowledged inconsistency of the use of the parent term, "terrorism". Additionally, definitions for cyber terrorism are even further complicated by the fact that they must be specific enough to be understood distinctly from other types of cyber attack, such as cyber warfare and hacktivism (Kenney 2015). Even so, the majority of the definitions in the literature, as per Table 64 at Appendix A, assert similar requisite features.

Among the sample definitions in Table 64 it can be seen that there are two opposing tendencies in the quest to define cyber terrorism; broad vs narrow. Broad definitions are in danger of including an incredibly vast array of cyber activities under their umbrellas, including some which label any activity conducted within cyberspace that aids terrorism as "cyber terrorism" (e.g., a phone call or text message between two terrorists). Narrow definitions, on the other hand, are often in danger of being so specific that they become purely hypothetical (Jarvis and Macdonald 2014).

Given the ongoing debate surrounding the scope and nature of cyber terrorism, this term can become confusing to use as a benchmark for which to legislate and protect against. As such, it is beneficial to define 'cyber terrorism' in a somewhat broad manner that includes all the key features witnessed in existing literature, and then from this define specific subsets as distinct

aspects of the broader definition that are purpose-specific (e.g., ‘cyber-physical terrorism’ for critical infrastructure protection).

2.3.3.2.2 Methodology

The first stage of research involved a literature review to identify all the key existing literature that has attempted to define cyber terrorism. The publication time period was not restricted in order to ensure a comprehensive representation of the evolution of understanding surrounding cyber terrorism. Every identified definition was then chronologically arranged and presented in Table 64 at Appendix A.

A cyber terrorism taxonomy was then used to identify and categorise related keywords in each definition. For example, a number of identified definitions required an event to be premeditated to be considered cyber terrorism. This requirement can be extracted and grouped under the taxonomical banner of ‘Intent’. A pre-existing cyber terrorism taxonomy proposed by Al Mazari et al. (2018) was initially used to conduct the analysis, however a new taxonomy was eventually developed due to an identified gap in the taxonomy (see Figure 15). Following this discovery all definitions were reanalysed using the proposed new taxonomy.

After all keywords were extracted from every definition and taxonomically categorised, they were then simplified to identify duplicates and synonyms. The simplified lists were then arranged into a graphic (see Figure 16) for ease of reference.

From this reference diagram synonymous keywords were merged and graphs were constructed to gain a statistical understanding of each keyword's frequency in existing definitions. With this newfound insight, each category was then analysed to determine keyword importance based on prevalence and meaning, and, in some instances, conflicting keywords were discussed to determine which one is more appropriate in today's context.

Finally, every important element of each existing cyber terrorism definition was able to be condensed and reconstructed into a concise new definition, which is proposed in section 2.3.3.2.5.

2.3.3.2.3 Cyber Terrorism Taxonomy

In order to define cyber terrorism effectively, the key features of cyber terrorism, as defined in the literature, must first be identified. The most effective way to do this is by way of a taxonomy that designates the key features of cyber terrorism, and against which each definition can be segmented and contrasted by the relevant components. Al Mazari et al. (2018) made a first attempt to define a cyber terrorism taxonomy using five key components: Target (military forces, government cyber and physical infrastructures, critical national infrastructures, social and national identity, and private industry or entities), Motive (social, cultural religion, political, ideological, etc), Means (computer and communication technologies and networks), Effect (violence, destruction and/or disruption of services, physical, operational and informational damages, and harm individuals and groups), and Intention (gain political, social, militarily or ideological advantages). During analysis however it was noted that more recent literature emphasises aspects relating to threat intent (Yunos et al. 2015; Macdonald et al. 2013; Plotnek and Slay 2019), which led to the discovery of a vital gap regarding the threat actor in the cyber terrorism taxonomy proposed by Al Mazari et al. (i.e., who constitutes a Cyber Terrorist; non-state actors, terrorist groups, nation states, undefined, etc.). Therefore, a revised taxonomy is proposed in Figure 15, which includes the aforementioned five components proposed by Al Mazari et al. (2018) but with an additional component, Actor. The remainder of this paper uses this newly proposed taxonomy for analysis.

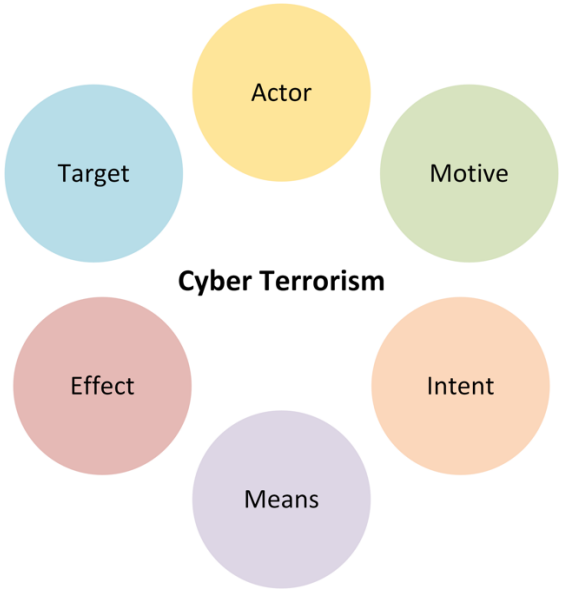

Figure 15 – Cyber terrorism taxonomy

2.3.3.2.4 Analysis

Upon collecting and chronologically arranging existing definitions at Table 64, the first stage of analysis involved segmenting each definition into keywords and grouping them according to the newly proposed taxonomy. For example, the definition of cyber terrorism proposed by Mantel (2009) is: "highly damaging computer attacks by private individuals, designed to generate terror and fear to achieve political or social goals". This can be segmented into the following keywords: "highly damaging", "computer attacks", "private individuals", "to generate terror and fear", "to achieve political or social goals". These keywords can then be assigned to the taxonomy components at Figure 15, e.g., "private individuals" can be assigned to "Actor". Once this process was applied to every definition available, the resulting categorised lists were simplified to reduce duplicate keywords and finally presented in Figure 16 (with numbers indicating the number of repeated occurrences) for ease of reference.

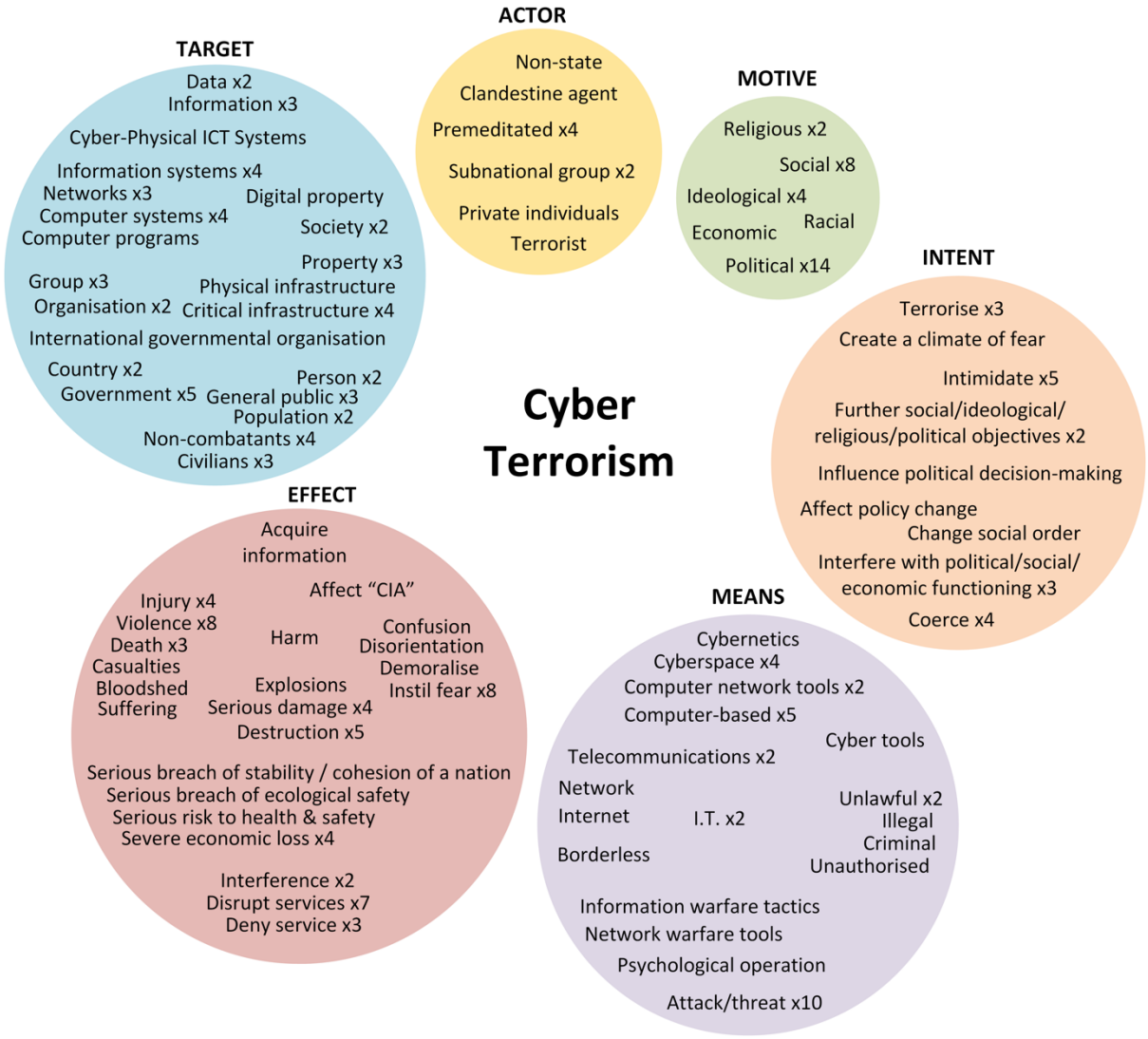

Figure 16 – Taxonomically grouped features inherent to cyber terrorism as defined in literature

For further guidance, Figure 16 can also be compared to Figure 17, taken from Jarvis and Macdonald (2014), where the authors had surveyed 115 researchers and policymakers on what they deem to be important elements of cyber terrorism.

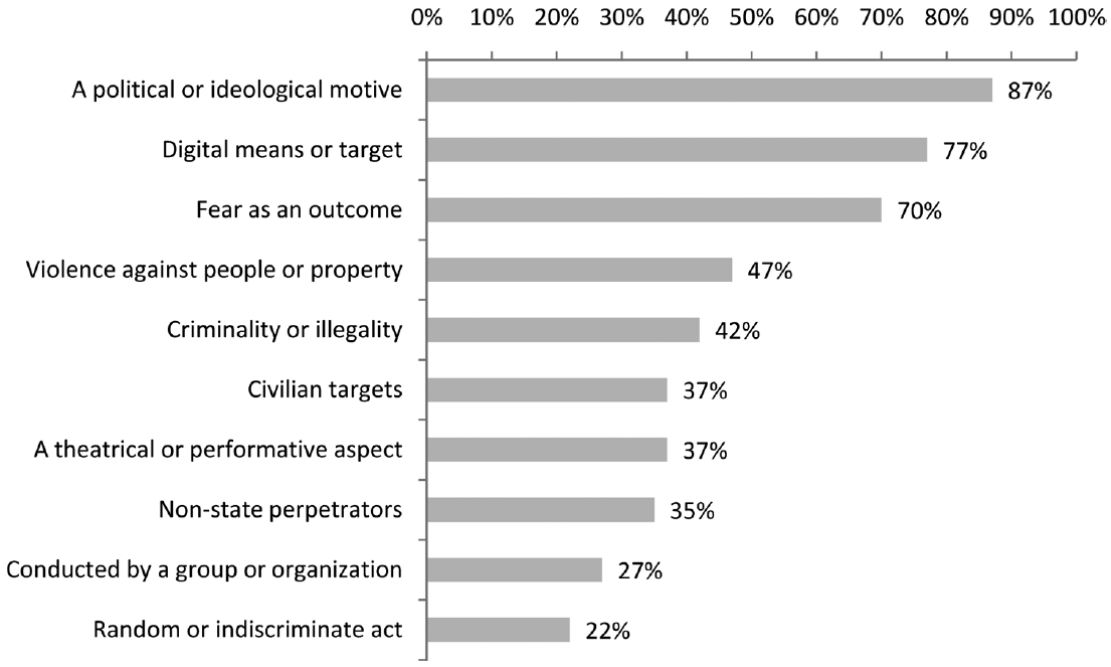

Figure 17 – Important elements of cyberterrorism according to 115 researchers and policymakers (Jarvis and Macdonald 2014)

Actor

The first of the six cyber terrorism features at Figure 15, 'Actor', describes the requisite traits of the so-called cyber terrorist. Within this category there are five unique attributes that emerge in the literature; non-state, clandestine agent, subnational group, private individuals, and terrorist, as shown in Figure 16. Some of these attributes are synonymous (e.g., non-state, private individual, and subnational group) and can be grouped together for simplification. Doing so results in three distinct attributes that can be ascribed to the cyber terrorist as an actor: Non-state, Terrorist, and Clandestine.

Figure 18 highlights that non-state origination is by far the most prominent actor description within the surveyed literature, with the other two descriptors only being mentioned once. The first of these singular descriptors, 'terrorist', provides an interesting method of tying the cyber terrorism definition to its parent definition, terrorism. This, however, is problematic as there is still ongoing debate as to whether an actor need be a terrorist, by traditional definitions and

understanding, in order to commit cyber terrorism. The second singular descriptor, 'clandestine' (Stambaugh et al. 2001), is broad enough to apply to any group or action and so does not provide any added value to the definition.

As such, amongst the authors that included a description of the actor within their proposed cyber terrorism definitions, and in line with the Jarvis and Macdonald (2014) study, there appears to be general agreement that a cyber terrorist is a non-state actor. The other two identified keywords can be excluded as outliers.

Figure 18 – Tally of requisite attributes ascribed to a cyber terrorist actor according to existing literature.

Motive

The second category in the cyber terrorism taxonomy at Figure 15 is 'Motive', which is concerned with the motivating factors behind a cyber terrorism plot. Figure 16 highlights seven different motives identified within the surveyed literature; premeditated, religious, social, ideological, racial, economic, and political. As seen in Figure 19, these seven descriptions can be simplified down to four keywords; ideological (including religious, political, ideological), social (including racial and social), economic, and premeditated.

Figure 19 demonstrates a clear preference in the literature towards defining ideological and social motives as being primary drivers behind cyber terrorism. This finding is also consistent with the 2014 study done by Jarvis and Macdonald (2014) (see Figure 18). The economic motive to conduct cyber terrorism was only mentioned once, however it was in one of the most recent papers (Yunos et al. 2015) and is plausible given the ongoing digitisation of modern banking.

The final keyword, ‘premeditated’ posits that for an act to be terroristic in nature it must have elements of planning, as opposed to being purely ad-hoc or impulsive.

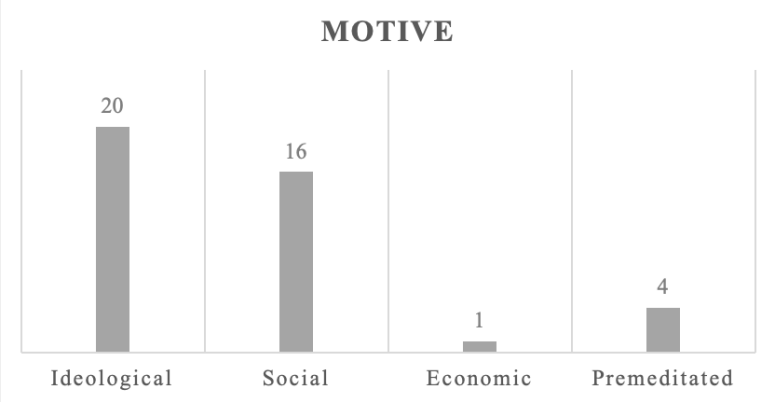

Figure 19 – Tally of requisite attributes ascribed to a cyber terrorist actor according to existing literature

Intent

‘Intent’ is the third component of the updated cyber terrorism taxonomy at Figure 15 and describes a cyber terrorist’s intended goals. Figure 16 shows that nine different phrases emerged from the literature regarding the current academic understanding of a cyber terrorist’s intent. These nine phrases have been condensed into five general objectives, as can be seen in Figure 20; those being to induce fear, coerce, effect change, further objectives, and interfere. This figure highlights that two-thirds of prescribed intent characteristics relate to coercion and inducing fear, which is generally used to coerce. Of the remaining intent descriptors, two categories can be disregarded – ‘further objectives’ is non-descriptive and hence provides little value, and ‘interfere’ is an intention that is by no means unique to terrorism (e.g., a thrill seeker might interfere with services but would not aim to induce fear). The final remaining characteristic, ‘effect change’, is useful when understood in combination with a motive, however it is clearly a minority opinion that this should be a requisite component of what defines cyber terrorism.

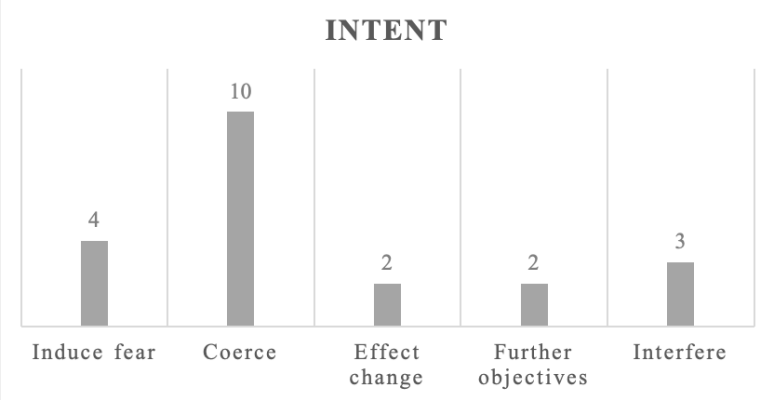

Figure 20 – Tally of requisite attributes ascribed to the intent of cyber terrorism according to existing literature

Means

The final three components of the cyber terrorism taxonomy were found to have the most definitional diversity. Starting with 'Means', 17 differing descriptions were identified, with nine overall concepts emerging; as demonstrated in Figure 16. It is interesting to note that an attack or a threat of attack was only mentioned ten times in the surveyed definitions, with a number of these instances occurring within the same statement (e.g., the proposed definition by Foltz 2004). Also worth noting is that 'cyberspace', 'computer', and 'network' were only mentioned 19 times, with some of these also occurring in the same definitions.

The term 'illegal' was used in four separate definitions and is problematic for a number of reasons. The first is that what is considered legal or illegal differs between jurisdictions and thus is an imprecise measure (as alluded to by the term 'borderless'). The second issue with this terminology is that the legality of an action or threat is relative to the actor. For example, the United States of America can commit a vastly greater range of acts within the realms of legality than an individual or subnational group might be able to. Finally, some acts may very well be legal in a particular jurisdiction but could still fall under the banner of cyber terrorism.

The term 'unauthorised' is also problematic as it raises the question of who authorised the action, which circles the discussion back to the 'Actor' element of the taxonomy. For example, what if a military officer of a rogue state authorises the shutdown of a civilian hospital's facilities? These semantic issues can be avoided by not specifying whether the act is criminal or authorised and instead rely on aspects pertaining to other elements of the taxonomy in the broader definition to help differentiate cyber terrorism from other forms of cyber attack.

The final two categories, ‘cyberwarfare’ and ‘PsyOps’ (psychological operations), are quite peculiar as they are generally ascribed to state-sponsored military operations. The term ‘cyberwarfare’, in particular, is an entirely separate category of cyber operations and cyber-attack that has its own ongoing definitional battles. In fact, a significant proportion of the surveyed literature went to great efforts to distinguish cyber terrorism from other types of cyber operations such as cyberwarfare (see Kenney 2015 for example). ‘PsyOps’ is less contradictory as it can, and most likely would, indeed occur alongside a cyber terrorism plot. However, much like with cyberwarfare, the term carries its own weight, distinct definitions, and debates, and so is problematic for inclusion in the definition of cyber terrorism.

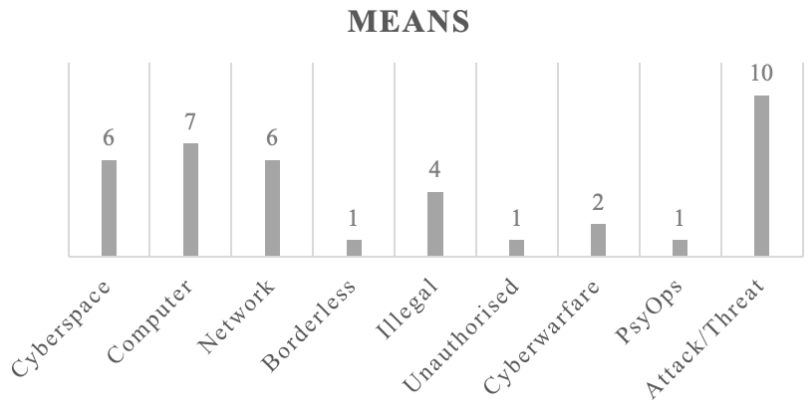

Figure 21 – Tally of attributes ascribed to the means by which cyber terrorism is perpetrated

Effect

‘Effect’ was attributed 23 different statements in Figure 16, each with varying levels of specificity and severity. These have been grouped under the seven categories shown in Figure 22. The four most agreed-on effects of cyber terrorism are: violence, service disruption, physical damage, and psychosocial impact; each of which emerged at significantly higher rates than the three least common. ‘Violence’ is a standout attribute, with 19 separate definitions using this as a requisite effect of cyber terrorism. Service disruption (i.e., interference, disruption, or denial of the integrity or availability of critical services) comes in at second, with physical and psychosocial impacts (i.e., fear, confusion, disorientation, or demoralisation, each of which can reduce the stability or cohesion of a society) ranking as third most important in the literature. Of the three least common effects cited in the surveyed definitions, ecological and economic damage appeared as potential, but not necessary, effects of cyberterrorism, whilst data breach (i.e., unauthorised access to information) was used in a way that is

inconsistent with the rest of the literature. Defining a breach of confidentiality as an act of cyber terrorism is not only problematic, but it doesn't match the required intentions described in Figure 20.

The key theme amongst the defined effects seems to be an impact or effect that occurs outside of cyberspace, whether that be psychological, social, political, physical, economic, or ecological.

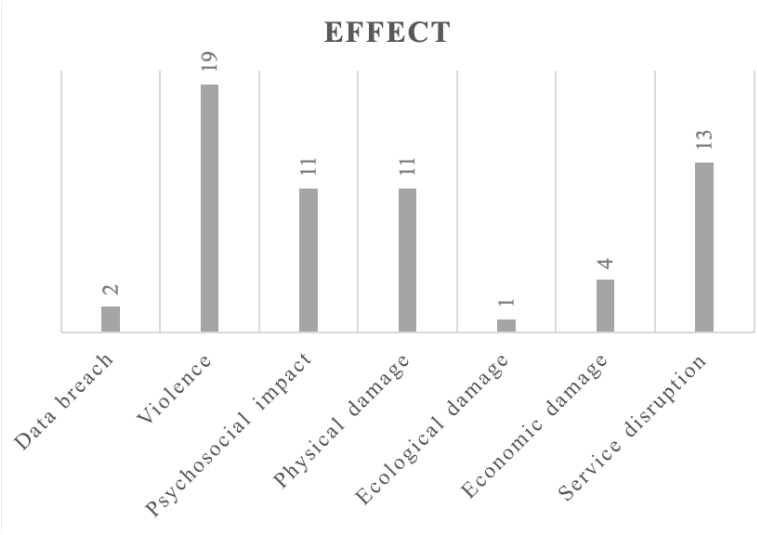

Figure 22 – Tally of requisite attributes ascribed to the effect of cyber terrorism according to existing literature

Target

The final attribute in the cyber terrorism taxonomy is 'Target'. Figure 16 shows the 22 different descriptions of what constitutes a cyber terrorist's target according to the currently available literature. From these descriptions nine categories were established (see Figure 23), four of which are technological in nature, two which are physical, and three which are human-oriented.

The number one most commonly cited target throughout the surveyed definitions was 'civilians' (i.e., general public, population, non-combatants, civilians, persons, and society), which together appeared 16 times. An interesting finding regarding the proposed technological targets is that control systems of physical processes (i.e., CPS, or Cyber-Physical Systems) were only once mentioned as an explicit target (see Akhgar et al. 2014); although the eight definitions citing critical and physical infrastructure as targets could also be understood to allude to the same thing, albeit less explicitly. The three other technically oriented targets (data, software, and ICT) don't provide much value in the way of understanding exactly what a cyber

terrorist might target as they could describe almost any technology these days; not to mention that they also don't fall firmly within the restriction of generating effects outside of cyberspace as concluded earlier.

Finally, both government and non-government establishments (e.g., groups, organisations, international governmental organisations, and governments) were defined as targets 13 times in total. Each of these targets have obvious links with the intent of the cyber terrorist; for example, if fear is the desired outcome, then a civilian target might make sense, however if the intent is disruption then perhaps a technical or organisational target would be selected as an end goal without paying too much attention to the secondary impacts that may occur. In combination with the other factors, each of these targets would result in slightly differing campaigns, whilst still remaining identifiable as cyber terrorism.

From this analysis it can be seen that the scope of what might constitute the target of cyber terrorism is largely variable, covering everything from technological to infrastructural, and civilian to organisational to government; all depending on the cyber terrorist's intent. This not only confirms the need for more specific sub-definitions of cyber terrorism (such as cyber-physical terrorism), but also demonstrates the need for generality in the attribution of a target to the broader definition of cyber terrorism itself.

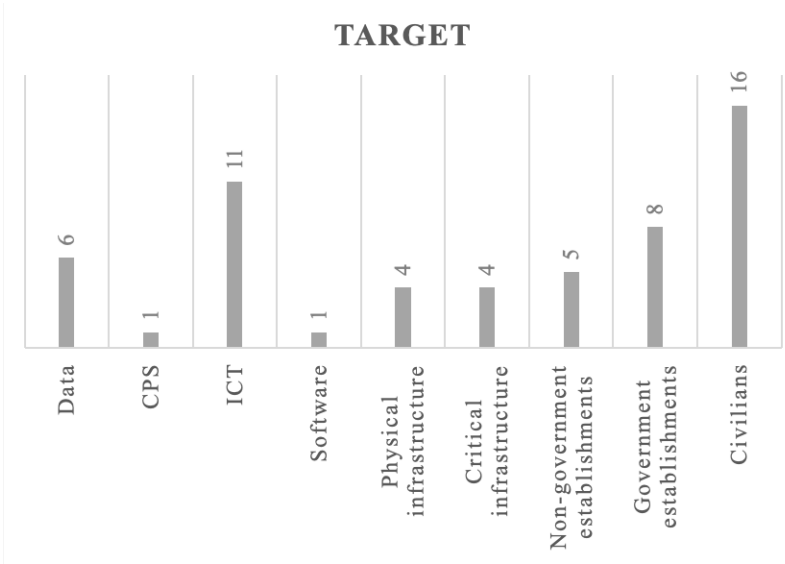

Figure 23 – Tally of requisite attributes ascribed to the target of cyber terrorism according to existing literature

2.3.3.2.5 Cyber Terrorism Definition

All up, Figure 24 demonstrates that 'Effect' and 'Target' are by far described the most throughout the literature; having been ascribed attributes 61 and 56 times across the cyber terrorism definitions respectively, and together making up over 50% of prescribed attributes. By contrast, the 'Actor' element carries far less importance in the surveyed definitions, having only been described as a requisite feature of some sort six times throughout the literature; with all other definitions leaving the type of perpetrator open to any actor (e.g., state actors).

These results can be due to a few different reasons. The first and perhaps most obvious one is that a single actor can cause multiple different effects on numerous targets, and hence more target and effect attributes might be able to be described than the qualities inherent to a cyber terrorist actor. Another reason for this disparity could be that certain aspects of the taxonomy, such as 'Intent', might be better understood (stemming from pre-existing research into traditional terrorism, for example) and hence can be described more efficiently than other aspects. This possibility is particularly relevant to the 'Actor' component of the definition, noting that until now it has not been considered a fundamental component of the cyber terrorism taxonomy. Finally, such a disparity could indeed indicate the comparative definitional importance between each element of the taxonomy (e.g., target and effect may be more important elements of cyber terrorism than actor or intent). It should also be acknowledged that the results presented above are a direct function of previous publications on the topic, so with an expanded dataset the final distributions of terms could be different, especially in relation to less popular terms.

Acknowledging that the answer is likely a combination of these speculations, it provides the most utility to treat each element of the taxonomy in its own right and avoid diminishing attention to any particular aspect. This is reinforced by the observation that 'Means' is only seen to make up 17% of the weight despite the fact that this element is relatively known and rather important given the term 'cyber terrorism' inherently alludes to the means by which it is perpetrated.

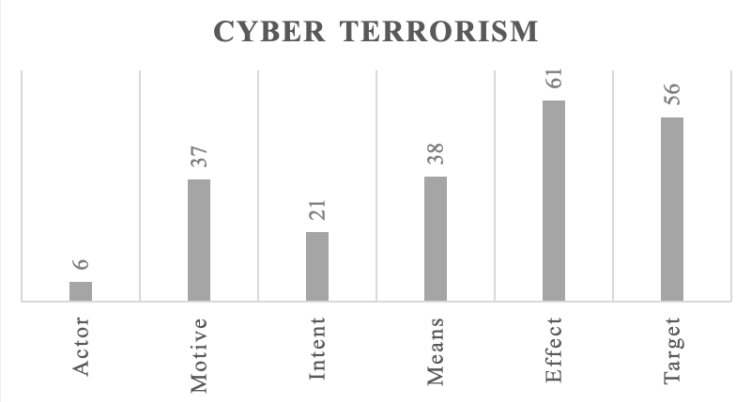

Figure 24 – Summary of attributes ascribed to each element of the cyber terrorism taxonomy in existing literature

In light of the findings detailed throughout this section it is now possible to construct a new universally applicable definition of cyber terrorism that acknowledges the major contributions to the subject up until now. In order to do this the important attributes ascribed to each element of the taxonomy must first be summarised, the results of which are listed below:

- Actor: non-state;
- Motive: premeditated, ideological, social;
- Intent: induce fear, coerce;
- Means: attack or threat of attack, originates in cyberspace;
- Effect: a consequence that occurs outside of cyberspace (e.g. psychological, social, political, physical, economic, ecological); and
- Target: civilian, government, non-government.

Having identified the critical attributes assigned to each element in the cyber terrorism taxonomy, a written definition may now be proposed as such:

"Cyber terrorism is the premeditated attack or threat thereof by non-state actors with the intent to use cyberspace to cause real-world consequences in order to induce fear or coerce civilian, government, or non-government targets in pursuit of social or ideological objectives. Real-world consequences include physical, psychosocial, political, economic, ecological, or otherwise that occur outside of cyberspace."

2.3.3.3 Modelling the Threat

Having selected a specific threat against which to model the final resilience framework outcomes and having developed a suitable taxonomy and definition to shape the model, the case study component of the literature review can be concluded.

In summary, to achieve the primary objective of this research project, which is to produce a high-level space system resilience assessment framework, it provided most utility to select an extreme threat with overt objectives for the case study. Cyber-physical terrorism was identified as an ideal candidate and was explored with a literature review that culminated in a new homogenised taxonomy and definition for 'cyber terrorism'.

The following six aspects should be considered when defining a cyber terrorist threat:

- Actor: non-state;
- Motive: premeditated, ideological, social;
- Intent: induce fear, coerce;
- Means: attack or threat of attack, originates in cyberspace;
- Effect: a consequence that occurs outside of cyberspace (e.g. psychological, social, political, physical, economic, ecological); and
- Target: civilian, government, non-government.

Each of these aspects must be defined for the specific threat that will be utilised in the case study threat model, as detailed at section 3.3.3.3. Once the specificities of the cyber-physical terrorist threat have been defined it can be modelled against a specific space system and its resilience functions to theoretically test the final resilience framework. The Van der Watt and Slay paper, which adapts the cyber kill chain (CKC) to LEO satellite systems (Van der Watt and Slay 2021) was broadly used to guide the threat scenario for the case study.

The CKC has seven distinct and chronological phases that can be correlated against the resilience cycle defined in section 4.1.4.5:

1. Reconnaissance;
2. Weaponisation;
3. Delivery;
4. Exploitation;

5. Installation;
6. Command & Control; and
7. Action on Objectives.

A general approach must be determined in order to contextualise these phases to the specific cyber-physical terrorist threat model for the case study component of the research project. To do this, a correlation must first be made between the CKC phases above and the space systems resilience phases at section 4.1.4.5. The analysis and outcomes of this approach are detailed in the subsections below. The application of the findings below are detailed in the Methodology chapter at section 3.3.2.6.

2.3.3.3.1 Reconnaissance

The first phase of the CKC is 'Reconnaissance', which may involve social engineering and passive and active monitoring and surveillance, such as vulnerability scanning, social media monitoring, dumpster diving, and spear phishing attempts. The commencement of the reconnaissance phase by a malicious actor is the first step toward carrying out an attack. It generally consists of research and data gathering activities to identify and scope the target space system and its associated people, processes, and technologies.

A target is often identified based on the space system's function or purpose, such as communications or surveillance operations. In a space system context, the victim could be the owner and/or operator of the space system such as a private company or government organisation and may extend down the supply chain to other secondary organisations such as third-party service providers or manufacturers of key components for the space system. Impacts to end users of the service and broader society should also be considered as secondary effects. For the purposes of this research the target system will be taken to be the space systems that the survey respondents are able to detail in section 4.2.

Reconnaissance activities include the technology-level assessments made by the threat actor to determine which specific system components are vulnerable for initial access prior to launching a full-scale attack. In the high-profile high-stakes case of space systems and their effective delivery of services, it should be assumed that the system is constantly undergoing reconnaissance from threat actors. A resilient space system, as defined in section 2.2.3.3, should be able to identify suspicious activity related to the reconnaissance phase across each

system segment, as defined in section 4.1.4.2, and determine the risk of the activity leading to the triggering of the 'React' phase. It should be noted that a large proportion of detected reconnaissance activity does not necessarily lead to a correlated attack, with a great deal of passive reconnaissance being automated or benign in nature.

2.3.3.3.2 Weaponisation

The 'Weaponisation' phase of the CKC commences when the threat actor has gathered sufficient preliminary information to determine a viable way into the system in pursuit of effecting the final attack. During this phase the actor, in this case a cyber terrorist, chooses or develops their choice of cyber weaponry and associated tools required to increase their chance of success in infiltrating the space system and carrying out the attack against the selected target (Yadav and Mallari 2016).

The weaponisation phase may involve threat actor activities such as designing a backdoor or developing a piece of targeted malware for delivery to the system. The aim of this phase is to enable successful delivery and exploitation, as detailed in the following phases. There are various methods and toolsets that can be used to aid the cyber-terrorist threat actor in aiming to gain access to the space system, including (Van der Watt and Slay 2021):

- Online hacking toolkits;
- Remote services, such as Malware as a Service (MaaS) and Ransomware as a Service (RaaS);
- Tools for persistent attacks and obfuscation;
- Cross-site Scripting (XSS) tools;
- Malware, including padded, disguised, packed or hybrid variants;
- Stolen PII for fraudulent activities, credential access and privilege escalation, assuming certain identities and social engineering.

The weaponisation phase is often undetectable from the target system as it relies primarily on data and information gathered during the reconnaissance phase. As such, the only correlation of this phase to the resilience cycle defined in section 2.2.3.3 would be that within the 'Anticipate' function a risk assessment should be conducted on any notable unexpected traffic, significant phishing attempts, or suspicious activity noted by personnel within scope of the system's governance framework. Combined, reliable threat intelligence and an active

awareness of the system's vulnerabilities, the system will remain best placed to react to any incumbent adversities.

2.3.3.3.3 Delivery

The 'Delivery' phase of the CKC is concerned with deploying the cyber weapons selected in the previous phase to the target system. Delivery activities may involve a complex combination of different threat vectors and attacks and often includes the delivery of malicious code. Space systems often have a broad international supply chain and may contain features to install software and security upgrades, which can involve remote connections that serve to make the system vulnerable to attack (Livingstone and Lewis 2016).

There are various methods that can be used to aid the cyber-terrorist threat actor in delivery of cyber weaponry to the space system, including (Van der Watt and Slay 2021):

- Use of cloud-based architecture and connectivity by external parties;
- Business Email Compromise (BEC);
- Spear-phishing;
- Unauthorised access and hacking;
- Web shells and XSS;
- Jamming and DDoS (both in orbit (i.e., upstream) and terrestrial (i.e., downstream)); and
- Spoofing.

It should be noted that some attacks may serve as a distraction for system responders whilst another attack is coordinated to occur simultaneously. The effectiveness of each of these methods of delivery depends on the system in question, including its vulnerabilities, critical functions, and any incorporated technologies. Therefore, for the purposes of this research dissertation, the case study scenario should take an agnostic approach to specific attacks and instead assume the successful delivery of whichever method the hypothetical cyber terrorist actor would choose.

In a resilient space system, the commencement of the delivery phase should be flagged in the 'Anticipate' function to trigger the 'React' function. At the point of successful completion of the delivery phase the system must be assumed to be compromised and therefore confidentiality can no longer be assured. In this stage the system has a limited time to

successfully contain the threat and bypass the resilience loop prior to the threat actor carrying out the 'Exploitation' phase of the CKC and triggering an adverse impact.

2.3.3.3.4 Exploitation

The 'Exploitation' phase of the CKC refers to the threat actors' taking advantage of technical and non-technical vulnerabilities, including any backdoors established in the delivery phase, to execute code on the target system (i.e., Installation) and assist in achieving the attack objectives.

In the context of the research outlined in this dissertation, the exploitation phase is primarily concerned with exploiting vulnerabilities in the target space system, as identified by case study participants. In line with the resilience framework, this phase of the CKC directs attention to the vulnerabilities in the space system. The final resilience assessment framework can be applied to any given space system to identify such vulnerabilities that could be exploited and determine appropriate measures to reduce risk exposure to this critical step in the CKC process. This activity was performed as part of recording responses to the case study and is documented in section 4.2.2.

Preventing the success of a threat actor's exploitation activities requires a pro-active security stance commensurate to the capability of the threat actor. When dealing with advanced persistent threats (APT) this level of defence may not be achievable, and so it should be assumed that a threat actor will successfully exploit the system in one way or another at any given point in time. It is for this reason that the concept of resilience is so important. To this end, the case study assumes successful exploitation of the system based on documented vulnerabilities identified in the interview process.

2.3.3.3.5 Installation

The 'Installation' phase of the CKC involves the threat actor installing malware or running unauthorised software within the targeted system in pursuit of the overarching attack objectives.

There are various methods that can be used to aid the cyber-terrorist threat actor in the installation of cyber weaponry and other unauthorised code to the space system, including (Van der Watt and Slay 2021):

- Manufacturing and supply chain processes, where multiple parties have access to satellite system hardware and software;
- Padding and packing or disguising of malware and undetectable hybrid versions of malware that bypass traditional detection methods and systems;
- Failure to patch software (Unal 2019) or hiding malware within seemingly legitimate software patches;
- Privilege escalation granting administration access rights;
- Credential access facilitating lateral movement through networks to various locations suitable for installation of malware;
- Distraction or deception using obfuscation techniques to disguise or hide primary malware installation locations and associated activities;
- Persistent-XSS (Nidecki 2019) and browsing the Internet (Santamarta 2014);
- Rootkits and bootkits;
- Remote Access Trojans (RAT).

A resilient system should be hardened against malicious activities required for the threat actor to successfully complete the installation phase and be able to detect and prevent such activity or respond and recover from a successful breach. Such aspects of resilience fall under various functions across the React, Sustain, and Recover phases, as well as Adapt after the incident has been remediated and system restored to its usual secured state.

2.3.3.3.6 Command and Control

The ‘Command and Control’ phase of the CKC occurs after successful installation of the relevant exploits required to conduct the attack. It is in this phase that the threat actor maintains control of their position in the system and enacts their final movements before initiating the ‘Action on Objectives’ phase and completing their attack execution.

Command and control activities are used to aid the cyber-terrorist threat actor in positioning for their final attack on the space system and may include actions such as the below (Van der Watt and Slay 2021):

- redirection and modification of OS, kernel, or other software instructions;
- corruption of data;
- DDoS attacks;

- jamming and spoofing of satellite signals and associated data;
- remote takeover of satellite control; and
- maintaining persistence in ICS such as SCADA.

Livingstone and Lewis (2016) also note that persistent attacks may be achieved through the ability to emulate a network and its access mechanisms and configure and control communications devices to remain latent within the system indefinitely, until the final action can be executed at a time of the adversary's choosing.

In the context of this research project, once command and control objectives are achieved by the threat actor the system's resilience will rely primarily on the functions contained under the 'Survive', 'Sustain', and 'Recover' phases. It may still be possible to identify a persistent threat actor and react prior to any adverse impact on service availability, however depending on the nature of installations made in the previous CKC phase any detections made through the 'Anticipate' function will be challenging. In the case of a cyber terrorist actor, however, it is likely that the attack will not be persistent over long periods of time prior to executing the final action on objectives.

2.3.3.3.7 Action on Objectives

The final stage of the CKC is 'Action on Objectives', which concerns achieving the threat actor's ultimate goals and objectives. This may include maintaining a covert system presence and launching persistent attacks over extended periods of time; however this is unlikely in the extreme case of a cyber terrorist actor.

Livingstone and Lewis (2016) describe a number of different objectives that may be desired by cyber threat actors. Although their work specifically concerns LEO satellite system breaches, each point can also be understood in the broader context of space systems. Expanding on Livingstone and Lewis's paper, the final actions on objectives may include:

- a reduction in national security or defence capability;
- a reduction in communications capacity, observation capability, or navigation precision;
- corruption of communications, including precise timing systems;
- destruction of space systems and denial of orbits following organised collisions;

- holding space systems to ransom, potentially using ransomware;
- destruction of launcher and payload assembly, possibly during the launch phase;
- corruption or deletion of data being transmitted from space systems;
- interception of communications including sensitive Intellectual Property (IP);
- rerouting of communications to allow easier interception; and
- jamming of signals or spoofing of data.

The success and impact of each of the above listed adversities (i.e., threat actor objectives) depend on the nature of each individual space system and its critical functions and services. Cyber-physical impacts are considered in the case study detailed in section 4.2.

In relation to the resilience cycle, each object listed above could trigger different impacts and response requirements. In the case of a significant impact to a resilient space system, the system's Survive function should enable system stabilisation post-incident, supported by the Sustain function which ensures minimum service availability until the threat is successfully contained and the system is able to enter the Recover phase. The resilience cycle is displayed in Figure 34 on page 206.

2.4 Outcomes of Literature Review

Due to the significant gaps in space systems security and resilience literature, and the limited related literature from other domains to adequately inform the desired research goals, the literature review necessarily covered a wide range of topics and to a level of depth that was not initially expected when setting out to undertake this research project. Definitions, taxonomies, and models were developed based on meta-analyses of related domains in critical infrastructure resilience and cyber threat literature in order to provide an appropriate baseline for space systems security and resilience outcomes prior to initiating the iterative Delphi study process. This section provides a summary overview of the outcomes of the literature review.

The literature review commenced with analysis of available literature on the topics of space systems security, as well as broader analysis of more general critical infrastructure and cyber security literature. It was identified that there are three different dimensions related to the holistic discipline of space security (Mayence 2010):

1. security in space (i.e. protecting space systems);

2. space for security (i.e. surveillance or military space operations); and
3. security from space (i.e. protecting Earth from space-based threats).

This finding allowed for the narrowing of the scope of research to the first dimension of space security, herein referred to as 'space systems security'. Drawing from older literature, Moltz's definition of space security was identified with the possibility for direct application to the more specific domain of space systems security. The Moltz (2011) definition defines space security as "the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction". This outcome has direct application to the first objective of the Delphi study, to determine a definition for space systems security.

As demonstrated in section 2.2.1, the lack of existing literature on security resilience in the space systems domain required that the study investigate resilience models of alternate but comparable systems, which can then be utilised as a starting point for the study. Through the literature review process power systems resilience was identified as a viable candidate upon which to model space systems resilience, as detailed in section 2.2.1.2. As such, it was first required to leverage existing power systems resilience literature to develop a comparable resilience model to that outlined in the research goals, a body of work which is represented by Secondary Research Outcome 1 (SRO-1) at Table 60. The outcomes of the power systems resilience literature review and resulting resilience taxonomy and model analysis are detailed in section 2.2.2, representing SRO-2 at Table 60. In summary, power systems resilience was defined as, "the recurring ability of a power system to anticipate, survive, sustain, recover from, and adapt to high impact low frequency events", representing SRO-3 at Table 60. The taxonomical representation of this definition is provided at Figure 7 on page 55. These outcomes, SRO-1 to SRO-3, provide the foundational model to develop a taxonomy and definition for space systems, as shown in Figure 36 and Figure 37. This was modelled functionally to account for both phasal and temporal requirements to attain resiliency in a power system, as documented at SRO-4 of Table 60.

The power systems resilience model was then translated into the space systems context, leveraging any available existing literature on the subject. The final definition, at least as necessary to commence the Delphi study process with expert feedback, is stated below:

“Space resilience is the recurring ability of a space system, including all sub-components and supporting functions, to anticipate, survive, sustain, recover from, and adapt to high impact low frequency events.”

Space security threats were then investigated through the literature process, with the ultimate definition of a CKC-based threat model being produced to support the case study component of the research project. This body of work represents Primary Research Outcome 1 (PRO-1), as shown in Figure 36 and Figure 37. It was identified that targeted attacks to space infrastructure can be broken down, as per the threat assessment published by Harrison et al. (2020), into:

- kinetic physical;
- non-kinetic physical;
- electronic; and
- cyber.

The remainder of the literature review, and indeed the Delphi study, uses these four key threat types to guide development and discussion.

The second part of the threat research concerned the specific type of threat to be utilised for the theoretical case study tests on real-world operational space systems. In consideration of the various aspects factoring into what constitutes an ‘ideal threat’ against which to test the availability-oriented resilience framework, terroristic cyber-physical threats were determined to offer the most theoretical potential as a case study due to their preoccupation on unhindered disruptive and destructive techniques. This was due to the reason that cyber terrorism represented the ideal threat case for testing the extremities of the resilience model to provide for more robust research outcomes, as discussed in section 2.3.3.

In combination with the CKC model, a well-defined threat actor is required to reflect potential real-world outcomes adequately and accurately in the case study. For this reason, the definition and taxonomy of cyber terrorism was investigated, identifying yet another gap in existing literature. Through a comprehensive meta-analysis of existing cyber terrorism literature to date, a new homogenised definition and taxonomy was developed and published, representing SRO-5, SRO-6, and SRO-7 of Table 60 and demonstrated in Figure 36 and Figure 37. In accordance with the outcomes described above, cyber terrorism can be defined as below:

“Cyber terrorism is the premeditated attack or threat thereof by non-state actors with the intent to use cyberspace to cause real-world consequences in order to induce fear or coerce civilian, government, or non-government targets in pursuit of social or ideological objectives. Real-world consequences include physical, psychosocial, political, economic, ecological, or otherwise that occur outside of cyberspace.”

The taxonomical analysis of existing definitions is summarised in Figure 14, with a final taxonomy being provided at Figure 15 on page 72. This taxonomy and definition are used to produce a detailed threat model against the seven phases of the CKC in section 3.3.3.3. It is important to note that this literature review was only conducted across open-source English resources, not only skewing the threat context to a Western bias, but also excluding any additional or conflicting research that may exist within classified archives.

3 Methodology

3.1 Introduction to the Study

This chapter provides an explanation of the research methodology for the study taken to address the research questions stated in Section 1.5, in pursuit of the research goals stipulated in Section 1.6. For added clarity, the research questions and goals have been combined and re-phrased into objectives for the study, as per below:

1. Determine the scope of the space systems security domain through the identification and critical evaluation of research related to space systems security.
2. Establish a definition and taxonomy for space systems resilience.
3. Develop a resilience assessment framework for determining the high-level resilience status of a space system to malicious cyber-physical threats.

Chapter 2 provided both the research context and the foundations to achieve these three study objectives. It established 'space systems security' as one of the three key sub-domains to the over-arching, multi-disciplinary 'space security' domain, as well as critically evaluating available literature on the subject. The chapter then went on to propose a novel definition and taxonomy for space systems resilience, derived from both the pre-identified space security literature, as well as published literature on the resilience of comparable critical infrastructures, such as power systems resilience. The academic foundations for achieving the third objective was also established in Chapter 2, through the review and analysis of opinions on the theoretical space-cyber threat landscape, and the establishment of a high-impact threat actor (i.e. cyber terrorists) against which the resilience framework can be tested.

Chapter 3 commences with a brief description of the three standard approaches to research; qualitative, quantitative, and mixed approach; before finally evaluating and selecting, the optimum approach for the study.

The methodology for the study is then outlined in three phases, as per below:

- Phase 1 – Literature Review;
- Phase 2 – Delphi Study;
- Phase 3 – Case Study.

The chapter concludes with a final summary of the overall methodology and approach for the dissertation.

3.2 Approaches to Research

A research method must be established prior to commencing research in order to ensure consistency and to maximise the possibility for successful outcomes. It is therefore pertinent to first consider the various methodological approaches available for the study.

It is commonly accepted that there are three main approaches to designing a research method (Creswell 2009):

- Quantitative (i.e. positivist);
- Qualitative (i.e. interpretivist); and
- Mixed-Method.

Where, quantitative research considers 'numbers as data and analyses them using statistical techniques', whereas qualitative research considers 'words as data, collected and analysed in all sorts of ways' (Braun and Clarke 2013).

The following sections discuss the three research approaches; qualitative, quantitative and mixed method; before analysing them in the context of this study to determine the most appropriate method.

3.2.1 Quantitative Approach

Quantitative research was made popular by the natural sciences due to its focus on the tangible and measurable aspects of reality and its pre-occupation with maintaining objectivity. According to Kaplan and Duchon (1988), "research designs should be based on the positivist model of controlling (or at least measuring) variables and testing pre-specified hypotheses". In his paper published three decades later, Creswell (2009) agrees, stating that quantitative research, "is a means for testing objective theories by examining the relationship among variables".

Creswell (2009) posits that quantitative methods are most appropriate for studies where researchers possess 'assumptions about testing theories deductively, building in protections against bias, controlling for alternative explanations, and being able to generalise and replicate the findings'. He also highlights two key strategies for conducting quantitative research:

- **Survey** based research is useful to gain 'a quantitative or numerical description of trends, attitudes, or opinions of a population by studying a sample of the population'. The data generated by a survey can be analysed to make generalised statements about the population being studied.
- **Experiment** based research 'seeks to determine if a specific treatment influences an outcome'. Although experiments often involve making generalised claims about a population, their primary goal is instead to "test the impact of a treatment (or an intervention) on an outcome, controlling for all other factors that might influence that outcome".

While the research related to this dissertation will indeed involve a survey, it is not concerned with statistically describing trends, attitudes, or opinions. Hence, the survey-based approach, as described above, is not deemed appropriate for this study.

Experimental research, on the other hand, is concerned with testing the effectiveness of a solution, which can be useful for validating conceptual frameworks. Framework validation is possible through modelling, which is a technique that is used widely in systems engineering to describe a physical, mathematical, or logical representation of real-world processes, devices, or concepts (Zelkowitz and Wallace 1998). An experiment-based approach would prove effective in testing the final resilience framework that this dissertation seeks to produce and can be achieved by way of cyber-physical threat modelling.

3.2.2 Qualitative Approach

In contrast to the quantitative approach, qualitative research adopts an "interpretive, naturalistic approach to its subject matter" (Denzin and Lincoln 1994). Kaplan and Duchon (1988) came to a similar conclusion, stating that "qualitative strategies emphasize an interpretive approach that uses data to both pose and resolve research questions".

A qualitative approach is beneficial for studies where the observations of the researchers themselves are the key data to be analysed. Creswell (2009) states that qualitative data is most often collected by researchers, through examining documents, data, and people, and is analysed by way of an inductive data analysis process to build patterns, categories, and themes from the bottom up.

He also highlights five key strategies for conducting qualitative research (Creswell 2009):

- **Ethnography** is "a strategy of enquiry in which the researcher studies an intact cultural group in a natural setting over a prolonged period of time by collecting, primarily, observational and interview data";
- **Grounded theory** is "a strategy of inquiry in which the researcher derives a general, abstract theory of a process, action, or interaction grounded in the view of the participants", involving "multiple stages of data collection and the refinement of and interrelationship of categories of information";
- **Case studies** are "a strategy of inquiry in which the researcher explores the depth of a program, event, activity, process, or one or more individuals";
- **Phenomenology** is "a strategy of inquiry in which the researcher identifies the essence of human experiences about a phenomenon as described by participants"; and
- **Narrative** research is "a strategy of inquiry in which the researcher studies the lives of individuals and asks one or more individuals to provide stories about their lives".

As outlined above, ethnographic, phenomenological, and narrative-based qualitative research are all geared towards research that seeks to better understand human nature and society; such as culture, experience, and life. Although the studies related to this dissertation will indeed involve interactions with people, it is not for the purpose of understanding humanity, but rather to ground research outcomes in expert consensus. Therefore, the ethnographic, phenomenological, and narrative approaches are inappropriate for this dissertation.

The remaining two qualitative research strategies; grounded theory and case studies; are instead focused on abstract concepts and processes, with a goal to understand the interrelation and depth of information categories in order to refine and present them more effectively. These approaches are better suited to the study of space security and resilience ontology due to the methods' strength in verifying abstract processes and frameworks.

3.2.3 Mixed Approach

Although the aforementioned quantitative and qualitative research approaches have been successfully applied for many decades, some commentators argue that these exclusive approaches "fail to meet the needs of an increasing number of practice-led researchers" (Haseman 2006). The implication being that mixed qualitative and quantitative approaches hold the potential to deliver better research outcomes. Supporting this idea, Kaplan and Duchon

(1988) argue that qualitative methods "provide less explanation of variance in statistical terms than quantitative methods" yet can offer "richer explanations of how and why processes and outcomes can be developed".

In their case study, Kaplan and Duchon (1988) found that combining qualitative and quantitative methods in information systems research provided a richer contextual basis for the interpretation and validation of results. They also found that mixing methods can "lead to new insights and modes of analysis that are unlikely to occur if one method is used alone", and that researchers can be made aware of potential errors in their analysis through the triangulation of data. Bryman describes this process as "using more than one approach to the investigation of a research question in order to enhance confidence" in the results (Bryman 2003).

Additionally, Creswell explains that utilising a mix of both qualitative and quantitative research approaches provides the most useful outcomes when "there is more insight to be gained from the combination of both qualitative and quantitative research than either form by itself", and where the combined use of both qualitative and quantitative research provides an 'expanded understanding' of the research problem (Creswell 2009).

3.3 Study Methodology

The previous section explored the various strategies and approaches to developing a research methodology and identified both quantitative (i.e., experimental) and qualitative (i.e., grounded theory and cases studies) as being appropriate for this particular study.

Noting both the variety of available methods and the presented benefits of adopting a mixed approach, it was decided to design a research methodology that incorporates aspects of each applicable strategy. A quantitative experimental research approach is utilised for testing the resilience model, controlling for all factors that hold the potential to influence the outcomes of the study. Whilst, qualitatively, a grounded theory approach is adopted for running expert focus groups, and a case study will constitute the final phase of testing the findings. In practice, the study will rely predominantly on qualitative data, with all analysis being informed and reinforced by quantitative methods. For example, qualitative research will serve to collect data, utilising statistical meta-analyses to identify and homogenise key taxonomical components and concepts. For the case studies quantitative methodologies, such as statistical analysis, are used to prioritise feedback and determine consensus.

Revisiting the study objectives established in Section 3.1 provides a clearer perspective on the purpose of this study:

1. Determine the scope of the space systems security domain through the identification and critical evaluation of research related to space systems security.
2. Establish a definition and taxonomy for space systems resilience.
3. Develop a resilience assessment framework for determining the high-level resilience status of a space system to malicious cyber-physical threats.

With the above in mind, a clear research progression can be seen. An initial perspective on each of these objectives can be achieved through qualitative document collection and inductive analysis in the form of a literature review. The outcomes of the literature review will then need to be validated, which can reliably be achieved through qualitatively grounded approaches, such as expert input through surveys and focus groups with interdisciplinary, but appropriately knowledgeable, participants. A final quantitative validation exercise, in the form of an experimental case study, can then be conducted to test the qualitatively constructed framework and to bring further assurance to the research outcomes.

Structured precautions were taken to avoid bias throughout the entire research process. A thorough literature review process was first conducted to account for all available literature, avoiding any undue bias towards literature selection from specific researchers, disciplines, or countries. Survey Monkey was selected for the Delphi study as the platform anonymises all feedback from the researchers to avoid any conscious or subconscious preferentialism towards respondents. All surveys were pre-vetted by independent research supervisors through processes established by the University of South Australia and all expert respondents received the same survey at the same time, with any iterative modifications being strictly documented and discussed in Chapter 4. Finally, the case study was conducted individually and independently with each participant to avoid any cross-contamination of feedback or outcomes. All discussion was recorded and transcribed, with transcriptions available at Appendix C, Appendix D, and Appendix E, for transparency.

In terms of selecting the survey approach, one mature and commonly utilised method for gathering and analysing survey responses is the Delphi method. The Delphi method was developed in the 1950s by the RAND Corporation and is described as “a set of procedures for

eliciting and refining the opinions of a group of people" (Dalkey 1967). According to Okoli and Pawlowski (2004), the purpose of the Delphi survey approach is to develop "the most reliable consensus of a group of experts". The method is known to be particularly suited to research where an incomplete understanding exists regarding a particular problem. It is "an iterative process to collect and distil the anonymous judgements of experts using a series of data collection and analysis techniques interspersed with feedback" (Skulmoski et al. 2007).

Utilising the Delphi method, questionnaires containing open-ended questions about specific problems and solutions form the primary method of collecting data. The data collection activities are performed in an iterative manner, with subsequent questionnaires being developed and issued based on the results of the previous questionnaire, until the research question is either answered or a consensus is achieved. In this manner, expert participants are enabled to provide iterative feedback in order to fully express their opinions and perspectives on the manner at hand. In contrast to the Delphi survey method, conventional surveys do not provide such opportunities for conversational closure. Finally, an expert focus group is offered to participants to provide open-ended and unstructured feedback in the form of a verbal conversation and/or written communication.

3.3.1 Phase 1 – Literature Review

The literature review serves to provide an initial understanding of the research domain and any literature gaps that exist. Due to the cross disciplinary nature of the research problem at hand, the literature review was split into two sections; resilience and threat.

The analysis of existing critical infrastructure resilience literature led to a preliminary definition and taxonomy for space systems resilience, as well as an improved scope of understanding of space systems security as a professional domain. This foundational research serves as the baseline for conducting the Delphi study with expert participants. In this instance, the outcomes of the resilience literature review were used to prompt questions and challenges, and to direct constructive conversation in pursuit of developing a robust and comprehensive space resilience framework.

The second half of the literature review examined cyber-physical threats to space systems. This analysis outlined the space-cyber threat environment and defined cyber terrorism as an 'ideal' threat model against which to test the framework. As explored in Section 3.2.1, a model can be

qualitatively tested using a case study approach, which therefore forms the final phase of this research.

3.3.2 Phase 2 – Delphi Study

The Delphi approach is a methodical and interactive research procedure for obtaining the opinion of a panel of independent experts concerning a specific subject (Skinner et al. 2015). This method is particularly useful for this research as it is tailored to scenarios where an incomplete understanding of a subject domain exists, which is indeed the case for space systems security and resilience. The most common data collection technique used in Delphi studies are surveys, which are often utilised to explore and define variables and their respective interrelations.

In reference to Linstone and Turoff's work (Linstone and Turoff 2002), Okoli and Pawlowski (2004) state that "Delphi may be characterized as a method for structuring a group communication process so that the process is effective in allowing a group of individuals to deal with a complex problem. To accomplish this "structured communication" there is provided: some feedback of individual contributions of information and knowledge; some assessment of the group judgment or view; some opportunity for individuals to revise views; and some degree of anonymity for the individual responses.". Therefore, in the context of this study, the Delphi method enables individual space security experts to operate effectively as a group in determining a collective decision on desired research outcomes.

According to Skulmoski et al. (2007), the key to success in employing this method is to provide "an iterative process used to collect and distil the judgments of experts using a series of questionnaires interspersed with feedback. The questionnaires are designed to focus on problems, opportunities, solutions, or forecasts. Each subsequent questionnaire is developed based on the results of the previous questionnaire. The process stops when the research question is answered: for example, when consensus is reached, theoretical saturation is achieved, or when sufficient information has been exchanged".

Skulmoski et al. (2007) report that, while the Delphi method is simple and flexible, researchers must take into account a number of specific design considerations to be successful. They summarised these considerations as follows:

- **Methodological Choices**. The methodology must be appropriately selected for the purposes of the investigation but may be qualitative, quantitative, or mixed method (Day and Bobeva 2005; Skulmoski et al. 2007).
- **Initial Questions – Broad or Narrow**. Questions must be designed to allow for a focus towards the desired goal in two to three rounds.
- **Expertise Criteria**. Delphi participants must meet four "expertise" requirements (Adler and Ziglio 1996):
    - knowledge and experience with the issues under investigation;
    - capacity and willingness to participate;
    - sufficient time to participate in the study; and
    - effective communication skills.
- **Number of Participants**. For a reasonably homogeneous group, approximately 10 participants are considered appropriate to yield a reliable outcome (Day and Bobeva 2005; Skulmoski et al., 2007). Some researchers further conclude that, under ideal conditions, groups as low as four can be deemed acceptable (Skinner et al. 2015).
- **Number of Rounds**. Two to three rounds are generally sufficient to obtain a consensus in a successful Delphi study (Day and Bobeva 2005; Skulmoski et al. 2007).
- **Methodological Rigour**. Rigour is improved when researchers leave an audit trail, regardless of whether the study in question is primarily qualitative or quantitative in nature.
- **Results**. The accuracy of study results must be demonstrated through suitable analysis techniques. Due to this study's mixed method approach and relatively small number of Delphi respondents, a detailed statistical analysis of research outcomes is not deemed necessary or appropriate.
- **Further Verification**. Generalising results obtained from a small group of respondents to a wider population size is often challenging due to the specifics of the environment of the study (Day and Bobeva 2005). Yin clarified the distinction between analytical generalisations based on qualitative methods (e.g., the surveys) and statistical generalisations based on quantitative methods (e.g., the case study) in order to reinforce the reliability of research outcomes generated by smaller group sizes (Yin 2014). In the research related to this dissertation, the triangulation of qualitative Delphi studies with quantitative experimental case study-based research will further enhance the reliability of and confidence in research outcomes.

The key design considerations and requirements are integrated into the Delphi methodology processes, which are described in the following subsections.

3.3.2.1 Delphi Study Overview

The goal of the Delphi study conducted in support of this dissertation was to obtain expert input into the definitions and models for space systems security and resilience, based on the findings from the literature review process. The Delphi study has been approved by the University of South Australia's Human Research Ethics Committee (Ethics Protocol 204283).

Expert respondents were assessed to be an expert in a field associated with space systems security or resilience and with more than seven years postgraduate or equivalent experience. Approximately 65 experts were identified internationally, 24 of which responded to every round of the survey. The survey was sent out electronically via an online survey service provider, Survey Monkey. All responses were anonymised to avoid intentional or unintentional weighting of feedback by the researchers.

3.3.2.2 Materials and Resources

The preparation of preliminary survey materials entailed a number of steps which were common to both the Phase 2 Delphi Study and the Phase 3 Case Study. These common materials and resources are summarised as follows:

- Contact List. A preliminary list of potential Delphi and case study participants was compiled based on relevant expertise and experience to the field of space systems security. This list was generated based on known academics in the field, senior engineers in space-related fields and/or organisations, and relevant industry leads and government officials in the area of space security and resilience.
- Introductory Letter. A letter introducing the study and its purpose was prepared and tailored to each identified individual and formed the basis of establishing initial contact with the survey and case study respondents. In the cases where initial contact was established through a representative organisation instead of any particular individual, it was requested that the introductory letter be circulated to appropriate members within the organisation who may be interested to participate in the study.
- Participant Information Sheet, Consent Form, and Delphi Participant Background Form.

3.3.2.3 Survey Round 1 – Preliminary Feedback and Scoping

Having gained a fundamental understanding of the space systems security context through the literature review, a first survey was designed to obtain expert input on the definition of space systems security and its knowledge domain.

The questions in the survey were presented as per the subsections below. The anonymised responses to each question were then collated to identify common themes and concerns among the respondents. Individually unique feedback was also taken into consideration, albeit with less conclusive weight on the research outputs.

3.3.2.3.1 Question 1 – Space Systems Security – Definition

Background

Traditionally space security has been viewed primarily as a military domain (Sheehan 2015). More recently, however, this view has expanded to include the following three dimensions of space security (Mayence 2010):

1) security in space (in other words, space systems security);
2) space for security (for example, military space operations); and
3) security from space (such as protecting Earth from space-based threats).

Drawing from traditional space security literature, Moltz (2011) proposes a definition that can be applied directly to the more specific domain of space systems security: "[Space systems security is] the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction".

Question

Taking into account your own experiences and understanding of the domain, does Moltz's definition adequately define 'Space Systems Security'? If not, please explain what you believe is missing or inaccurate.

3.3.2.3.2 Question 2 – Space Systems Security – Domain Background

Background

Space systems security is, by nature, an interdisciplinary knowledge domain. Various technical disciplines form an integral component in protecting the space technology ecosystem from external threats.

Table 3 below attempts to map the Space Systems Security domain. Each row of the table represents a different threat to space systems in general (Harrison et al. 2022), whereas the columns approximate the attack surface (for example, vectors and entry-points into the system).

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

Table 3 – Originally Proposed Space Systems Security Knowledge Domain

Definitions:

- Cyber 3PP: Cyber security assurance of Third Party Purchasing (3PP) and outsourced services;
- Cyber IAM : Cyber Identity & Access Management;
- Cyber Threat: A software-based threat that occurs via computing and telecommunications infrastructure;
- ECM: Electronic Countermeasure (ECM) Analysis to protect against Electronic Warfare (EW) tactics;
- Electronic Threat: An electronic threat that causes non-physical impact, such as a Radio Frequency (RF) Denial of Service (DoS);
- Emanations Security: Electronic protection against Radio Frequency (RF) attacks, such as TEMPEST;
- Kinetic Physical: A physical threat that causes a physical impact, such as an Anti-Satellite weapon (ASAT);
- Non-Kinetic Physical: An electronic threat that causes a physical impact, such as an Electromagnetic Pulse Weapon (EMP) or social engineering;
- Non-Malicious Threat: An unintentional threat, such as environmental or accidental;
- OT Security: Operational Technology (OT) and cyber-physical systems (CPS) security;
- Teleport Engineering: Telecommunications port (teleport) & RF antennae reliability engineering.

Question

Based on your experiences working with space technologies, do you believe anything is missing or inaccurate in the table above? If so, please explain what is missing or what should be modified.

3.3.2.3.3 Question 3 – Space Systems Resilience – Definition & Taxonomy

Background

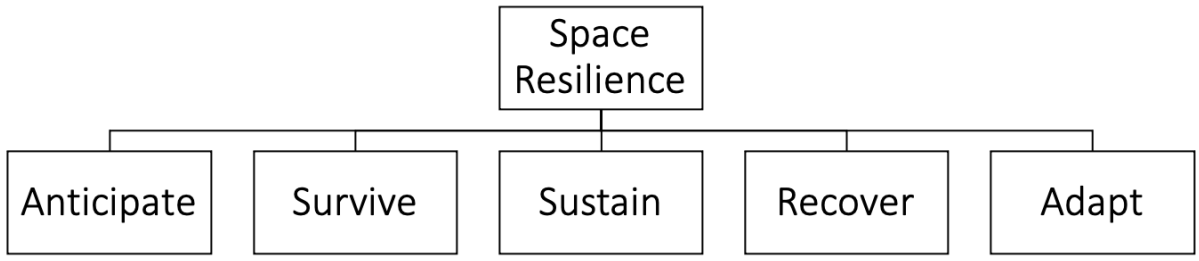

Figure 25 - Space Resilience Taxonomy

The space resilience taxonomy presented at Figure 25 has been produced based on existing resilience models published in critical infrastructure literature, where:

- Anticipate refers to the system's resilience enhancing mechanisms in place to prevent, detect, and avoid HILF cyber events;
- Survive refers to the system's resilience enhancing mechanisms in place to mitigate, absorb, and withstand the impacts of the HILF cyber event;
- Sustain refers to the system's resilience enhancing mechanisms in place to contain any impacts and preserve core functions during a HILF cyber event;
- Recover refers to the system's resilience enhancing mechanisms in place to respond, restore operations, and 'bounce back' from a HILF cyber event; and
- Adapt refers to the processes and procedures in place to reflect on lessons learned and adopt new mechanisms to increase resilience for any similar cyber events in the future.

Based on the above, Space Systems Resilience can be defined as:

"the recurring ability of a space system, including all sub-components and supporting functions, to anticipate, survive, sustain, recover from, and adapt to high impact low frequency events"

Question

In your opinion, does the above definition and taxonomy adequately capture the concept of Space Resilience? If not, please detail what you believe is missing or inaccurate.

3.3.2.3.4 Question 4 – Space Systems Resilience – Model

Background

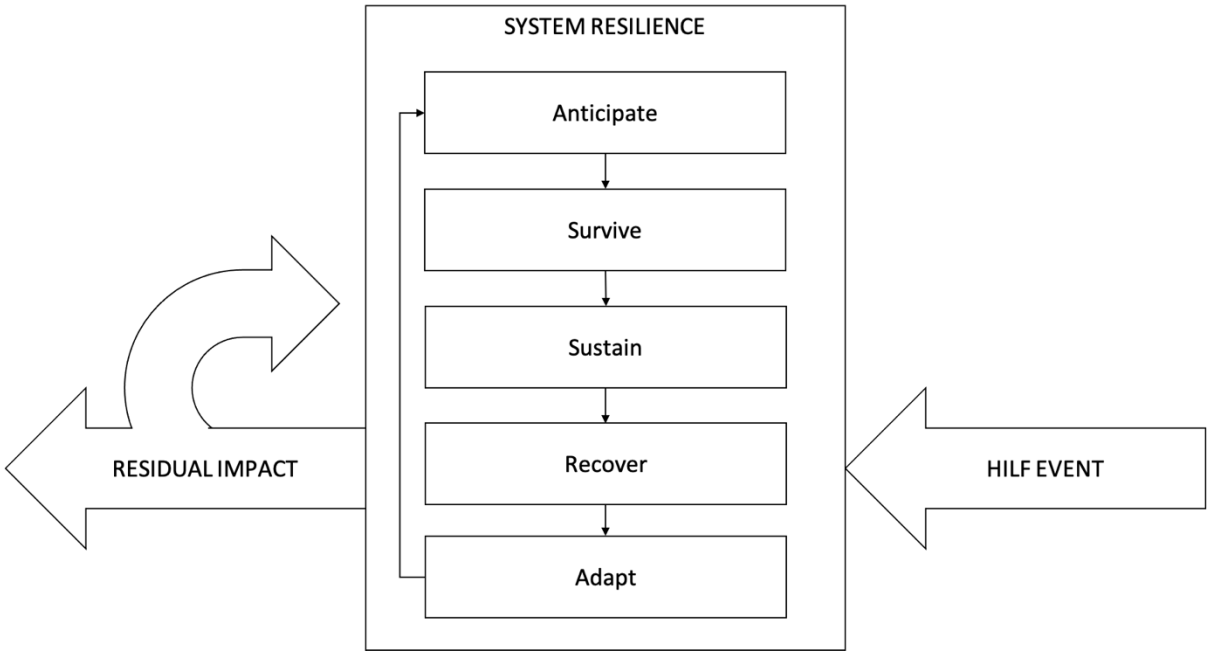

Figure 26 - Space System Resilience Lifecycle (Plotnek and Slay, 2021)

In the model above, a High Impact Low Frequency (HILF) event, sometimes referred to as a 'black swan' event, impacts the system in question, triggering a survival response (i.e., a state transition from Anticipate to Survive). The system then cycles through each phase listed below andbefore the final post-cycle residual impact is delivered to the system and its environment.

1) Survive – initiated by HILF event;
2) Sustain [baseline operations];
3) Recover [from any impact]; and
4) Adapt [to the new threat], before finally returning to the default state;
5) Anticipate [a HILF event].

Question

In your opinion, does the model at Figure 2 adequately explain the space resilience cycle? If not, please detail what you believe is missing or inaccurate.

3.3.2.4 Survey Round 2 – Feedback on Modified Framework

In response to the findings from round 1, a second survey was developed that took into account the initial feedback and recommendations into two newly modified definitions and two newly modified models.

The questions in the second round of surveys were presented as per the subsections below. As with the first round, the anonymised responses to each question were collated to identify common themes and concerns among the respondents.

3.3.2.4.1 Question 1 – Space Systems Security – Definition

Background

In Round 1 we acknowledged the three dimensions of Space Security (security in space, from space, and space for security) and tailored Moltz's 2011 definition of Space Security to the first dimension.

The resulting definition based on your collective responses is:

"Space Systems Security is the ability to assure 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."

Question

Does this new definition adequately define Space Systems Security? If not, please explain what you believe is missing or inaccurate.

3.3.2.4.2 Question 2 – Space Systems Security – Domain Background

Background

In Round 1 we examined a table that attempted to identify the various interdisciplinary domains that together form the knowledge base needed to ensure space systems security and resilience. Based on the expert feedback received, the table has been modified as shown below:

THREAT TYPE / TARGET	Governance Segment	Ground Segment	Space Segment	C3 Segment
Non-Malicious	**Protecting governance components from non-malicious threats** through Security Training & Awareness, BCP/DRP, Legal Compliance, V&V, RF Spectrum Management and OH&S	**Protecting ground components from non-malicious threats** through Debris / Celestial Monitoring and Reliability Engineering (Telecomm, Software, Aerospace, ICT)	**Protecting space components from non-malicious threats** through Human Factors, Safety, Materials and Reliability Engineering (Elec., Aero., Mech., Software, Electronics, Robotics)	**Protecting C3 components from non-malicious threats** through Data Management, Redundancy / Reliability Engineering (Telecomm., Software, ICT)
Cyber	**Protecting governance components from cyber threats** through Cyber GRC, Cyber Assurance Testing, Supply Chain Security, Cyber Training & Awareness, Access Management, Threat Intel. & Cyber Law/Reg.	**Protecting ground components from cyber threats** through IT / OT/ IoT Security Engineering, Security Monitoring (e.g. SOC), and Cyber Incident Response	**Protecting space components from cyber threats** through OT/ IoT Security Engineering, Security Monitoring (e.g. IDS/IPS), Resilience Engineering (e.g. D4P2), Offensive Defence	**Protecting C3 components from cyber threats** through IT / OT / IoT Security, Secure Coding, Cryptography, Security Monitoring (e.g. IDS/IPS), Anti Malware, Redundancy Engineering, Integrity Checks
Electronic	**Protecting governance components from electronic threats** through Electronic Assurance Testing, Threat Intel., and EW Law/Reg.	**Protecting ground components from electronic threats** through EMSEC / TEMPEST, ECM / EW, Physical Security (e.g. perimeter, surveillance)	**Protecting space components from electronic threats** through EMSEC / TEMPEST, ECM, EW Counterspace Operations, Resilience Engineering (e.g. D4P2)	**Protecting C3 components from electronic threats** through Redundancy Engineering, Integrity Checks

Kinetic	**Protecting governance components from kinetic threats** through Surveillance / Threat Intelligence, International Space Law / LOAC	**Protecting ground components from kinetic threats** through Physical Security (e.g. safes / locks, building, perimeter, surveillance)	**Protecting space components from kinetic threats** through Counterspace Operations / Weapons, Space Monitoring, Resilience / Redundancy Engineering	**Protecting C3 components from kinetic threats** through Counterspace Operations / Weapons, Space Monitoring, Resilience / Redundancy Engineering

Table 4 – Round 1 Outcome: Space Systems Security knowledge domain

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

Table 5 - Round 1 Outcome: Space systems segments

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

Table 6 - Round 1 Outcome: Threats to space systems

Question

Does this new table adequately cover the important high-level disciplines that are required to effectively protect the confidentiality, integrity, and availability of space systems? If not, please explain what you believe is missing or inaccurate.

3.3.2.4.3 Question 3 – Space Systems Resilience – Definition & Taxonomy

Background

In Round 1 we critiqued a proposed Space Systems Resilience Taxonomy that had emerged out of a cross-disciplinary literature review.

In response to the expert opinions provided, the 5 taxonomical aspects of resilience have been modified to be:

- Adapt, which refers to the system's mechanisms in place to continuously evolve based on threat events and intelligence to increase resilience to threats.
- Prevent, which refers to the system's mechanisms in place to detect, avoid, and deter or counter-act threats;
- Survive, which refers to the system's mechanisms in place to mitigate, absorb, and withstand the impacts of a threat event;
- Sustain, which refers to the system's mechanisms in place to contain any impacts and preserve core functions and services during a threat event; and
- Recover, which refers to the system's mechanisms in place to respond, restore operations, and 'bounce back' from threat events.

Based on the above, the proposed definition has been modified to be:

"Space Systems Resilience is the ability of a space system, including its services, sub-components, and supporting functions to continuously adapt in order to prevent, survive, and recover from threat events whilst sustaining core operations"

Question

Does this new definition adequately define Space Systems Resilience? If not, please explain what you believe is missing or inaccurate.

3.3.2.4.4 Question 4 – Space Systems Resilience – Model

In Round 1 we critiqued a diagram that visually represented how the 5 aspects of Space Systems Resilience interact with each other and the system/environment in question. Based on changes made in Q3 and the feedback on the original model, the below was produced:

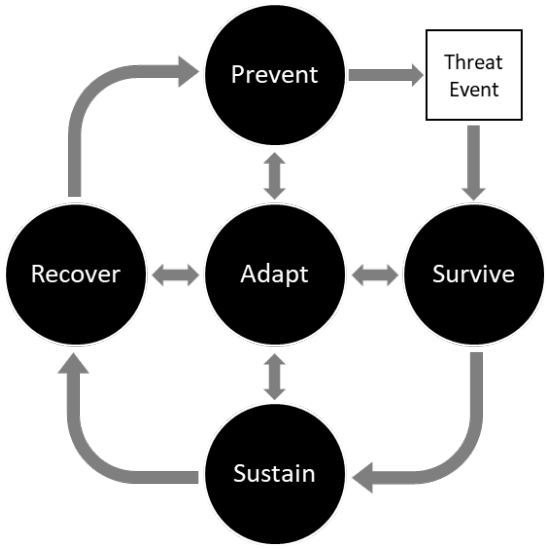

Figure 27 - Space Systems Resilience Model after modifications based on the Delphi Study Round 1 analysis

Question

Does this new model adequately represent the Space Systems Resilience cycle? If not, please explain what you believe is missing or inaccurate.

3.3.2.5 Survey Round 3 – Final Verification

The Delphi Study Round 3 survey pack included a summarisation of the changes made between Round 1 and Round 3 based on the expert responses provided and resulting analysis. It then provided the final proposed definitions and models based on the Round 2 suggestions for improvement. Expert participants were finally encouraged to provide any final feedback or objections to the proposed model.

This section details the questions posed to the participants, including the related definitions, models, and supporting materials that were provided as part of the survey questionnaire. Responses and analysis are detailed in Section 4.1.2.1.3.

3.3.2.5.1 Question 1 – Space Systems Security Definition

We commenced the Delphi study with Moltz's definition below:

"Space security is the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction"

The new proposed definition based on your collective input is:

"Space systems security is the assurance of the services, control, and confidentiality of a space system throughout its lifecycle, including all ground, communications, and space components, as well as the people, data, processes, and supply chains that enable it."

Please provide any final feedback or comments on the new space systems security definition.

3.3.2.5.2 Question 2 – Space Systems Security Domain

We commenced the Delphi study with a preliminary knowledge domain mapping, as shown in Table 3. The new proposed knowledge domain based on your 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.

Table 7 - Delphi Study Round 3 Question 2 Space Systems Security Knowledge Domain

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

Table 8 - Delphi Study Round 3 Question 2 Segment Definitions Supporting Table

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

Table 9 - Delphi Study Round 3 Question 2 Adversity Definitions Supporting Table

The segments in the tables above can be understood to interact at a high-level as per below:

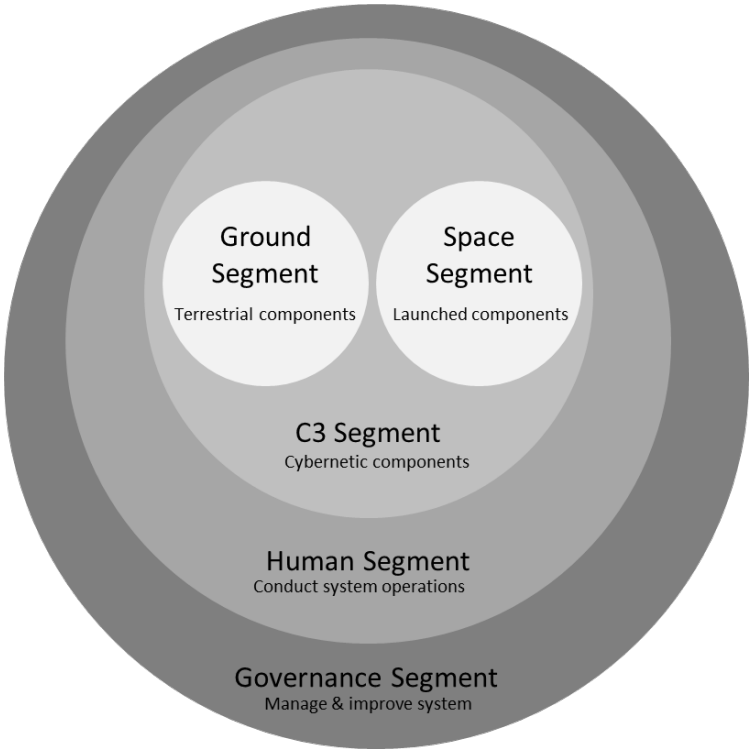

Figure 28 - Delphi Study Round 3 Question 2 Knowledge Domain Segmental Interrelationships

Please provide any final feedback or comments on the new space systems security knowledge domain.

3.3.2.5.3 Question 3 – Space Systems Resilience Taxonomy

We commenced the Delphi study with a 5-stage taxonomy that had emerged out of critical infrastructure resilience literature:

- **Anticipate** refers to the system's resilience enhancing mechanisms in place to prevent, detect, and avoid high impact low frequency (HILF) cyber events;
- **Survive** refers to the system's resilience enhancing mechanisms in place to mitigate, absorb, and withstand the impacts of the HILF cyber event;
- **Sustain** refers to the system's resilience enhancing mechanisms in place to contain any impacts and preserve core functions during a HILF cyber event;
- **Recover** refers to the system's resilience enhancing mechanisms in place to respond, restore operations, and 'bounce back' from a HILF cyber event; and
- **Adapt** refers to the processes and procedures in place to reflect on lessons learned and adopt new mechanisms to increase resilience for any similar cyber events in the future.

The new proposed Space Systems Resilience taxonomy based on your collective input is:

- **Anticipate**, which refers to the system's ability to maintain situational awareness and proactively detect potential threats;
- **React**, which refers to the system's ability to avoid, deter, or neutralise detected threats and respond to adverse events;
- **Survive**, which refers to the system's ability to mitigate, absorb, or withstand the impacts of an adverse event;
- **Sustain**, which refers to the system's ability to retain control and preserve core functions and services in a degraded state;
- **Recover**, which refers to the system's ability to respond, restore operations, and 'bounce back' from adverse events.
- **Adapt**, which refers to the system's ability to evolve based on threat intelligence and lessons learned from adverse events.

Please provide any final feedback or comments on the improved space systems resilience taxonomy.

3.3.2.5.4 Question 4 – Space Systems Resilience Definition

We commenced the Delphi study with the definition below:
"Space systems resilience is the recurring ability of a space system, including all sub-components and supporting functions, to anticipate, survive, sustain, recover from, and adapt to high impact low frequency events"

The new proposed definition based on your collective input is:
"Space systems resilience is the ability of a space system, including its services, sub-components, and supporting functions, to anticipate, react to, survive, recover from, and adapt to adverse events whilst maintaining control and sustaining core operations and services in a degraded state."

Please provide any final feedback or comments on the improved space systems resilience definition.

3.3.2.5.5 Question 5 – Space Systems Resilience Model

In Round 1 we contextualised a critical infrastructure resilience model to the space context, as shown in Figure 26.

Based on your collective input, the new proposed resilience cycle is:

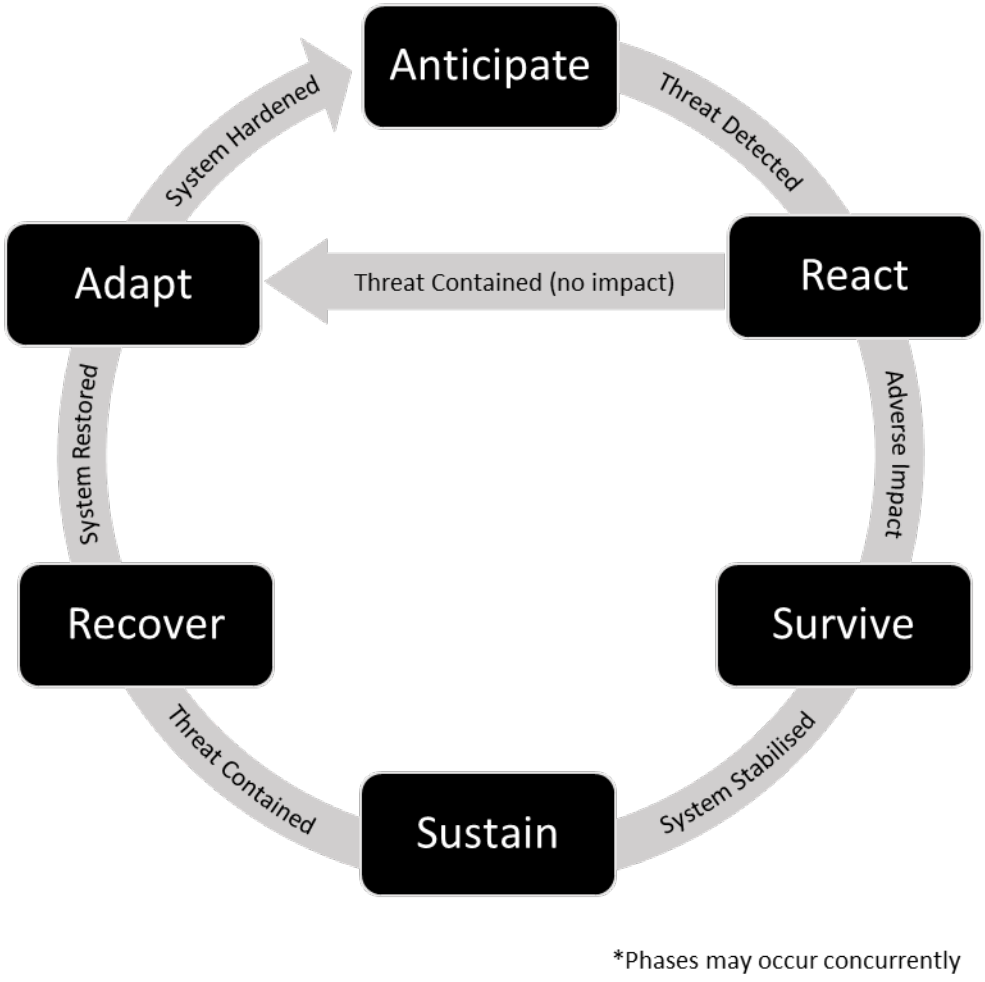

Figure 29 - Delphi Study Round 3 Question 5 Space Systems Resilience Cycle

The model can also be represented as a function of time, seen below:

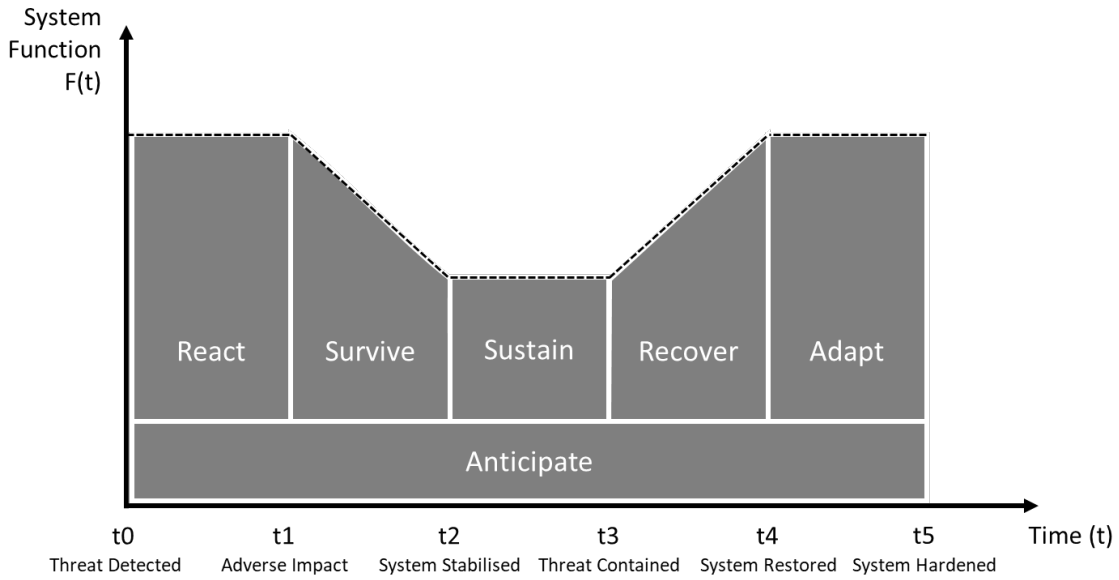

Figure 30 - Delphi Study Round 3 Question 5 Space Systems Resilience Model as a function of time

Please provide any final feedback or comments on the new space systems resilience model (including both the resilience cycle and the resilience x time chart).

3.3.2.6 Expert Focus Group

To conclude the Delphi study an expert focus group was proposed to Delphi respondents to enable unstructured feedback in case anything was missed by the structured nature of the survey. As such, all participants in the expert focus group are familiar with the iterative progression of the framework and appropriately qualified and experienced to provide meaningful feedback.

The expert focus group is voluntary if participants opt to provide additional open-ended feedback on the final outcomes via voice or text. This allows for any final criticisms, disagreements, or comments to be made without any unintended bias introduced by the nature of the survey process. Any final modifications are then incorporated into the framework in preparation for the case study.

3.3.3 Phase 3 – Case Study

To support the research goals outlined in section 1.6, a case study methodology was applied to validate the outcomes of the Delphi Study detailed in the previous section. Yin's 2009 book on

"Case Study Research" provides the basis for the case study activities carried out in support of this dissertation (Yin 2009). According to Scholz and Tietje (2002), the case study methodology provides an empirical inquiry approach to investigate a contemporary problem within its real-life context. Yin (2009) defines doing case study research as a linear but iterative process that may be used to contribute to our knowledge of individual, group, organisational, social, political, and related phenomena. The case study method allows researchers to retain the holistic and meaningful characteristics of real-life events, such as the operation of space systems, when in pursuit of answering 'how' and 'why' questions, such as how a space system responds to a specific threat scenario.

Yin (2014) divides the case study approach into two aspects, its scope and its features. Both the aspects have been recounted below for ease of reference.

Scope

A case study is an empirical inquiry that investigates a contemporary phenomenon (the 'case') in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident.

Features

A case study inquiry should:

- cope with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result;
- rely on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result; and
- benefit from the prior development of theoretical propositions to guide data collection and analysis.

In addition to the above, Yin (2014) also notes that case study research can involve one or more case studies and use either qualitative or quantitative evidence, or a mix of the two. In the context of the research project outlined in this dissertation, the outcomes of the literature review (see chapter 2, especially section 2.3.3) and the Delphi study (see section 4.1) were strengthened by the triangulation of data using a case study approach to validate the space system resilience assessment framework in several real-world contexts.

Yin (2014) states that there are four criteria that should be used for assessing the quality of a case study research design:

1. Construct Validity: identifying correct operational measures for the concepts being studied.
2. Internal Validity: seeking to establish a causal relationship, whereby certain conditions are believed to lead to other conditions, as distinguished from spurious relationships.
3. External Validity: defining the domain to which a study's findings can be generalised.
4. Reliability: demonstrating that the operations of a study – such as the data collection procedures can be repeated with the same results.

Construct Validity

Operational measures of the resilience framework have been determined and verified through the iterative Delphi study process. Construct validity has been managed through a clear and documented scope of research, which formed the basis for guiding the case study interview discussion and data collection and has been communicated to each stakeholder throughout the various stages of research, including the case study component. The scope of questions, process of inquisition, and format of documentation was predefined through the knowledge domain table at Table 44 and conducted in a way to minimise any subjective input by the interviewer.

Internal Validity

According to Yin, internal validity is primarily a concern for explanatory research where the study seeks to explain why one event leads to another (Yin 2014, p.47). In the case study undertaken as part of this research project respondents are not asked to make causal judgements but instead are interviewed to gain their opinions and feedback on the high-level resilience controls in place on the space systems, they are responsible for, accompanied by open-ended discussion on the reasons behind their opinions. The level of internal validity required for this study is demonstrated through the clear documentation of supporting evidence to the model, which is used to guide the discussions and outcomes of the case study. All case study discussions were also recorded, and corresponding transcriptions provided to enhance transparency and provide detailed evidence for proof of internal validity.

External Validity

The purpose of the case study undertaken as part of this research is provide triangulation of the interrelated research findings, including the findings of both the literature review and Delphi study, which together aim to provide a robust ontology derived from and validated by expert opinion. One objective of the research was indeed to define a domain to which the study's findings can be generalised (i.e., the space systems security domain at Table 44), against which the case study data collection approach was designed. The case study is based on the input of a small group of expert respondents (two completed case study interviews were documented) who have advanced and current knowledge of an operational space system. It is relevant to note that the respondents were chosen from a homogeneous group (cyber security managers of operational Australian space systems) which aims to minimise any divergent outcomes due to hidden variables such as cultural differences in response. The outcomes of the case study component of the research are based on empirical evidence using a qualitative methodology and are therefore appropriate for analytical generalisation to a breadth of space systems.

Reliability

As stated above, reliability aims to demonstrate that the operations of a study, such as the data collection procedures, can be repeated with the same results. Although individual respondents will inevitably vary in response, particularly in considering that different space systems were the subject of different interviews, various measures were effectively put in place to assure the repeatability of the case study in applying the resilience assessment framework. Reliability aspects of the case study research have been managed through the implementation of the following measures:

- the recruitment and selection of respondents was restricted to a limited scope with strict requirements surrounding:
    a. a minimum of 7 years of expert knowledge in space systems security;
    b. ongoing access to currently operational space systems; and
    c. up to date knowledge of the status of any security and resilience controls in place on the space system (including governance and personnel segments).
- an overview of the study, methodology, and research goals was provided to all survey respondents;
- the use of pre-prepared slides to guide the discussion and data collection process throughout the survey, supported by open-ended questions to facilitate discussion;

- the acknowledgment and conscious management by the interviewer of the implicit risk arising from open discussion, in that the researcher may generate bias through providing input;
- a transcription of all survey discussion is documented, with minor redactions made to protect individual privacy and limit any confidential or corporate information from being disclosed; and
- the case study is based on the validated resilience assessment framework produced as a result of the Delphi study process and was used in a structured and documented manner to record all data collected during interviews in a repeatable way.

The case study itself is detailed in the following sections.

3.3.3.1 Case Study Overview

A case study scenario was designed by combining input from the threat model and the resilience assessment framework and tested using data recorded from interviews with expert participants. The case study aims to theoretically validate the research outcomes arising from the Delphi study by testing the framework against a real-world space system. This is achieved by using the threat model in section 3.3.3.3 as a reference to step through each phase of the CKC, as discussed in section 2.3.3.3. At each stage of the CKC, the threat actor's actions are theoretically simulated against the space system in question, as detailed by the case study expert participants, with potential outcomes being modelled based on gaps in resilience posture identified through the interviews. The scenario is then re-run with those resilience gaps that were identified through the framework being 'plugged' in order to perform a 'before and after' analysis on the threat outcomes. In carrying out this exercise, the case study demonstrates both the theoretical effectiveness of resilience controls already in place on the real-world space system, as well as the benefits of implementing controls in-line with the resilience framework.

The details of the interviews and the threat model are provided in the following sections. The interview component of the case study has been approved by the University of South Australia's Human Research Ethics Committee (Ethics Protocol 204283).

3.3.3.2 Case Study Interviews

Case study interviews were conducted by videocall, recorded, and transcribed. All verbatim transcriptions are provided in section 4.2.2, with minor editing to retain both personal and corporate confidentiality of the respondents.

Case study interviews formed the data collection phase of the case study. Participants were presented with the knowledge domain in Table 44 and asked a series of questions in a guided open-discussion format in order to ascertain the high-level security and resilience controls in place on their operational space systems. Two long-form interviews were conducted with individual participants over approximately 1-2 hours each. Survey participants were selected based on their security expertise and security management positions, with a requirement that they oversee the security activities for an operational space system. Each respondent was identified as responsible for different space systems at separate organisations, covering both domestic and international applications. All data was recorded in a blank version of the knowledge domain, as shown in Table 10 below.

	Governance Segment	**Human Segment**	**Ground Segment**	**Space Segment**	**C3 Segment**
Non-Malicious					
Cyber					
Electro-magnetic					
Kinetic					

Table 10 - Case study data capture template

3.3.3.3 Case Study Threat Model

The research detailed in this dissertation aims to produce a framework for assessing the high-level resilience of a space system. As identified in section 2.2.3, in order to assess resilience a

specific threat to the system must first be identified, against which the system's resilience may be tested. Due to the limitations and scope of this thesis, all possible threats to space systems are not able to be identified or modelled. Section 2.3.3 details the approach taken to identify and select an appropriate threat for modelling space system resilience against, which resulted in the definition of cyber terrorism as an ideal choice. The case study data collection, threat model outcomes, and resulting findings are detailed at section 4.2.

As determined in section 2.3.3.3, the following six taxonomical components of cyber terrorism must be considered when defining a cyber terrorist threat:

- Actor;
- Motive;
- Intent;
- Means;
- Effect; and
- Target.

For the case study these factors have been defined as follows:

Aspect	Case Study Definition
Actor	A state-sponsored terrorist organisation with high cyber capability
Motive	Pre-meditated political motivations stemming from ideological foundations
Intent	Damage trust in critical infrastructure organisations and generate instability
Means	Cyber attack
Effect	Availability of services reduced due to cyber-physical impact
Target	Space system (as defined in section 4.2.2 by the case study respondents)

Table 11 - Cyber terrorist threat model definition for the case study

The features defined in Table 11 are utilised in section 4.2.3 to simulate a cyber-physical attack against the real-world space systems defined by the case study respondents. The Van der Watt and Slay paper, which adapts the cyber kill chain (CKC) to LEO satellite systems (Van der Watt and Slay 2021) can broadly be used to guide the threat scenario for the case study. Although other more comprehensive attack frameworks exist, such as the ICS MITRE ATT&CK Matrix (MITRE 2022), the CKC provides a relatively simple and logical flow that is ideal for the high-level nature of the case study. The CKC has seven distinct and

chronological phases that can be correlated against the resilience cycle defined in section 4.1.4.5:

1. Reconnaissance;
2. Weaponisation;
3. Delivery;
4. Exploitation;
5. Installation;
6. Command & Control; and
7. Action on Objectives.

The literature review and contextualisation provided at section 2.3.3.3 examines the relationship between the CKC above and the final resilience model at section 4.1.4.5. After capture of the expert respondent discussion data, as provided in section 4.2.2, the cyber terrorism case study scenario was played out phase by phase of the CKC, theoretically simulated against the real-world space systems identified in the case study. The manner in which each distinct phase of the CKC is handled by the resilience model is demonstrated in below.

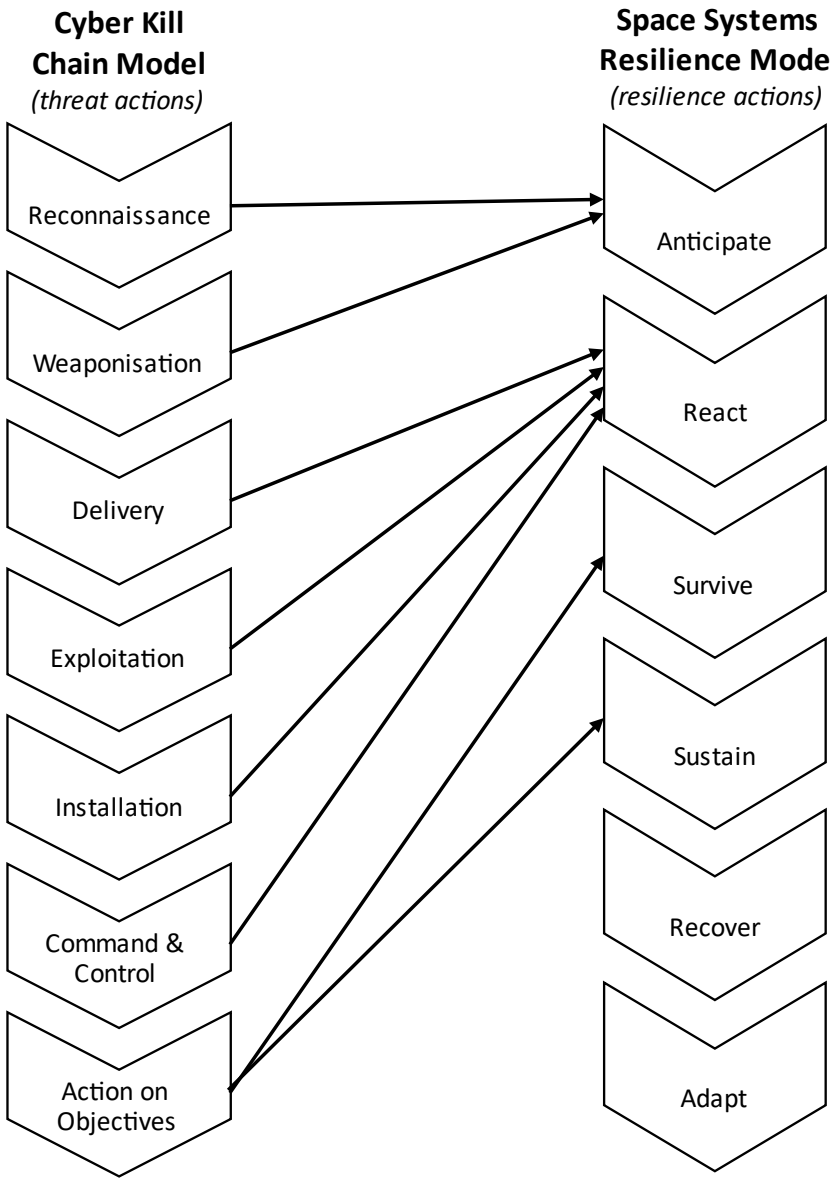

Figure 31 - Cyber Kill Chain Threat Model mapped to the Space Systems Resilience functions

3.3.3.4 Scenario Construct

The overall approach to applying the threat model to the case study methodology, particularly in light of the identified threat actor and target systems, can be broken down into four distinct phases and is detailed further in Figure 32 and the rest of this section:

1. **Scoping.** The first phase of the scenario covers all scoping activities conducted by both the threat actor and the defending space system. This includes scanning, target/threat identification, and preliminary assessments and decisions to both weaponise and prepare a response.

2. **Instigation.** The second phase of the scenario concerns the initial actions carried out by both the threat actor and the defending space system in the lead up to an attack. This includes activities by the threat actor to compromise the system and pre-position themselves for their final action on objectives, as well as activities by the defenders to react to identified malicious activity, such as delivery of malicious code or unexpected privileged activity.
3. **Adverse Event.** In the third phase of the scenario, the cyber terrorist threat actor completes their action on objectives, causing a cyber-physical impact to the system and triggering the Survive and, later, Sustain response from the space system. It is in this critical phase that either the threat actor achieves their goal, or the space system proves resilient and successfully manages to contain the threat whilst maintaining baseline services and operations in a degraded state.
4. **Remediation.** The fourth and final phase of the scenario refers to the remaining resilience phases of Recover and Adapt, which take place after the threat actor has completed their attack, any cascading impacts have been contained, and the system is no longer under direct threat. Activities conducted in the phase include restoring the system back to its pre-event baseline and improving the resilience posture based on findings made during the adverse event.

Figure 32 - Case Study Threat Scenario Phases

In the case study, the goal of the system is to maintain the three core features ascribed to space systems security in section 4.1.4.1. The three core features of security, as familiarised in the domain of cyber security, are confidentiality, integrity, and availability, also commonly

referred to as the CIA Triad. Through the Delphi study process, these elaborated on in a space systems context to be:

1. Control;
2. Services; and
3. Confidentiality.

As shown in Figure 31, the Reconnaissance and Weaponisation phases of the CKC model map directly to the Anticipate function of the space systems resilience model. This is due to the fact that in both the Reconnaissance and Weaponisation phases no actual harm has yet been perpetrated to the system. As such, the space system has insufficient evidence nor reason to trigger the React process. During this period of time the cyber terrorist threat actor is deemed to be collecting intelligence about their intended target and method of attack to achieve their overarching objectives, as determined in Table 11. This includes scanning, target identification, and preliminary assessments and decisions to weaponise in preparation to achieve their final objectives against the intended target. At the same time the defending space system utilises proactive threat detection techniques as part of the Anticipate function of the resilience framework. This initial period of time, including the processes of both the cyber terrorist threat actor and the defending space system, has been deemed the Scoping phase of the case study scenario.

The second phase of the case study scenario, Instigation, involves those initial post-Weaponisation pre–Adverse Event impact activities conducted by both the hypothetical cyber terrorist threat actor and the real-world space system, as detailed by the expert survey respondents. This includes activities by the threat actor to compromise the system, modelled using the Delivery, Exploitation, Installation, and Command & Control phases of the CKC, in order to pre-position themselves for their final action on objectives. This is the most critical phase for both the threat actor and defending space system to successfully achieve their objectives; those being, respectively, to cause a cyber-physical impact and to prevent a cyber-physical impact. An optimally resilient system is expected to detect the Delivery phase as early as possible in order to successfully circumvent the impact through activities in the React function of the resilience model. On failing to detect the Delivery phase, a resilient system should be able to detect Exploitation activities. On failing to do this, a resilient system should be able to detect Installation activities. The final opportunity for detection and impact circumvention occurs during the Command & Control phase. After successful execution of

Command & Control, the threat actor is perfectly positioned to strike. This could occur after an extended period of time, as would be the case for an APT, in which instance the space system should have mechanisms in place to detect ongoing covert threat activity. For the scenario of a cyber terrorist actor, there may be no political or legal reason to maintain persistence in the network after an opportunity for successful attack has been identified. As such, for the purposes of the case study, some aspects of the CKC model may be afforded less importance and so have been compressed according to the four phases outlined for the scenario.

The third phase, Adverse Event, occurs the moment the cyber terrorist threat actor begins delivering their action on objectives, causing a cyber-physical impact to the system and triggering the Survive and, later, Sustain response from the space system. It is in this phase of the scenario that the threat actor either achieves their goal of cyber-physical impact including any flow-on effects to the delivered services, or the space system proves resilient and survives the impact. Survival activities include defending against ongoing or concurrent adversities without losing the three fundamental features identified in the space security definition: control, services, and confidentiality. Additional factors were also considered at a high-level, such as societal impact, the Kessler effect, organisational impact, reputational damage, and financial or legal penalties. On successful survival, the system may experience damage yet maintain delivery of the critical services, or in the case of failure it may be substantially impaired and deemed unserviceable. A resilient space system should be able to withstand some impact whilst maintaining core operations. In this case, the system enters the Sustain phase of the resilience cycle where defenders have successfully curtailed ongoing impacts and have established a minimum baseline of operations despite the degraded state.

The fourth and final phase of the scenario, Remediation, refers to the remaining resilience phases of Recover and Adapt. This occurs after the successful defence and resiliency of the space system and includes activities to restore the system back to full operational capacity and improve the security and resilience posture based on findings made during the adverse event. This phase may occur over a long period of time, depending on the amount of received damage. The final state of the system should be different to the pre-event state, in that any lessons learned should be incorporated to improve the overall resiliency of the system given the new knowledge available. This phase was considered only briefly for the purposes of the case study scenario as it is not necessarily impacted by the threat actor and hence there is limited benefit

to further theoretical modelling besides what was already validated through the Delphi study process.

3.4 Summary of Methodology

The research detailed in this dissertation applies a mixed methodology approach utilising both quantitative (i.e., experimental) and qualitative (i.e., grounded theory and cases studies) methods with data obtained through extensive literature review and expert respondents. A clear perspective on the purpose of this body of research was established as follows:

1. Determine the scope of the space systems security domain through the identification and critical evaluation of research related to space systems security;
2. Establish a definition and taxonomy for space systems resilience; and
3. Develop a resilience assessment framework for determining the high-level resilience status of a space system to malicious cyber-physical threats.

These overarching research objectives were achieved by beginning with a comprehensive literature review of available and tangential research to core problem, and establishing some baseline definitions, models, and concepts to feed into the Delphi study methodology. The Delphi study presented these preliminary findings to two dozen space systems security experts globally, each with at least seven years of experience in the domain. The findings were iteratively improved based on expert feedback until a final consensus was achieved with complete agreement among respondents. These findings were then corroborated using an expert focus group to confirm the Delphi study findings and provide any further unstructured feedback. The final outcomes of the expert focus group were finally presented to case study participants in an open discussion forum. The framework was used to collect data from each respondent regarding security and resilience controls in place on the real-world operational space systems that they are responsible for. This data was fed through the case study methodology to theoretically test the resilience outcomes of each system against a cyber-physical terrorist threat scenario using the CKC model. The outcomes of all of the above research activities are detailed in the following chapter.

4 Study and Findings

The Study and Findings chapter presents the responses from expert participants and step-by-step analysis of feedback and outcomes gained through the study. The chapter commences with the Delphi study in section 4.1, where the preliminary concepts from the literature review are presented to expert participants for feedback and criticism. In this section, expert responses are solicited through an iterative survey process, analysed, and either rejected or incorporated into the novel framework. The outcomes from the Delphi study are then fed into the case study detailed in Section 4.2, where the final framework is validated and modified based on an experimental case study methodology and a final open-ended expert focus group discussion. Section 4.3 provides a summary of findings and outcomes from the Delphi study, case study, and expert focus group.

4.1 Delphi Study and Findings

4.1.1 Delphi Study Respondents

The respondents selected for the study were space security experts with more than seven years of work experience across academia, industry, or government. The organisational composition of the expert respondent base is approximately half from a background in Defence (including military and Defence industry), with the other half being an equal split between academic researchers and senior practicing engineers or cybersecurity consultants with space systems experience. The technical backgrounds of respondents are varied, with a majority of participants actively working in the area of space security or cyber security. Other technical backgrounds represented in the expert survey base include space system managers, aerospace engineers, military space personnel, electromagnetic security practitioners, and threat researchers. All responses were anonymised by the Survey Monkey platform prior to analysis by researchers to reduce bias and ensure the integrity of research outcomes.

4.1.2 Results of Delphi Study

4.1.2.1 Survey Round One

The Delphi Study Round 1 questions are described in Section 3.3.2.3 and should be referenced when interpreting the below responses and analysis.

A summary of all changes that were made as a result of the Delphi Study Round One survey responses is provided in the table below for ease of reference. All original responses and justifications behind the stated modifications are detailed in the remainder of this section.

Ref	Modifications
Question 1 Outcomes	
A001-1	Remove ‘external’ from the threat component of the definition.
A002-1	Remove “without interference” from the definition.
A003-1	Modify the definition to include the Ground Segment.
A005-1	Add supply chain to the definition.
A006-1	Modify the definition to cover the full life of system.
A006-2	Remove ‘interference’ from the definition.
A007-1	Remove “without damage or destruction” from the definition.
A012-1	Add confidentiality, integrity, and availability to the definition.
A014-1	Add ‘data’ to the definition.
A014-2	Add the Communications Segment to the definition.
Question 2 Outcomes	
A025-1	Change presentation of table for improved clarity.
A025-2	Add a supporting legend to assist with interpretation of terminology.
A025-3	Separate communications out into a separate segment.
A026-1	Add cyber security training and awareness to the cell corresponding to cyber threats to/by personnel.
A027-1	Add directed energy weapons to the supporting legend at A025-2.
A029-1	Add ‘Data’ to the supporting legend at A025-2.
A029-2	Add ‘Computing’ to the new column created at A025-3.
A030-1	Add key RF attacks to the supporting legend at A025-2.
A031-1	Replace ‘Military Space Ops’ with more descriptive sub-categories of counterspace operations.
A031-2	Add space debris to the supporting legend at A025-2.
A034-1	Add launch vehicle to the supporting legend at A025-2.
A035-1	Simplify the threat categories used for the rows in the table.
A036-1	Separate governance out into a separate segment.
A039-1	Add ‘Human Factors’ to the considerations for the space platform.
A039-2	Add manufacturing facilities to the supporting legend at A025-2.
A040-1	Include EMC alongside EMP in the table.
A044-1	Add ‘Physics’ as a consideration to kinetic-physical impacts in the supporting legend at A025-2.
Question 3 Outcomes	
A049-1	Add “sustaining core operations in a degraded state” to the definition.
A050-1	Provide more detailed taxonomical definitions for clarity.

A050-2	Replace ‘recurring ability’ with ‘continuously adapt’ in the definition.
A056-1	Remove ‘HILF’ from the definition.
A064-1	Change ‘Anticipate’ to ‘Prevent’ in the taxonomy and definition.
A065-1	Add ‘services’ to the scope of the definition.
Question 4 Outcomes	
A069-1	Redesign resilience model to appear less linear.
A071-1	Modify model so that ‘Adapt’ is clearly portrayed as the central continuous function.

Table 12 - Summary of modifications based on Round 1 responses

The Delphi Study Round 1 questions are described in Section 3.3.2.3 and should be referenced when interpreting the below responses and analysis.

4.1.2.1.1 Question 1 – Space Systems Security Definition

As demonstrated, to date there is no existing definition of ‘Space Systems Security’. Therefore, the first question in the survey sent to the two dozen space security experts attempted to build a contemporary definition for the first dimension of space security, using the Moltz (2011) definition as a starting point per the aforementioned Research Approach.

The question posed was: *Taking into account your own experiences and understanding of the domain, does Moltz’s definition adequately define ‘Space Systems Security’?*

4.1.2.1.1.1 Responses

Table 13 below provides the verbatim expert survey responses to Question 1 alongside a high-level yes or no assessment that summarises the respondents’ answer to the question as posed in the survey and summarised in Section 3.3.2.3.1. Note that spelling and grammatical errors have been included to avoid any inadvertent interference with the raw data.

The summary of response, analysis, and decision outcomes (i.e., changes made to the original definition) of each of the below responses are detailed in the following section.

ID	Response	Answer
R001	I think it is a strong definition, however using 'external' implies that threats can not originate from within. With the increase of social engineering and human influence campaigns (from a cyber threat perspective), along with the ever present insider threat (either malicious or	No

	non-malicious), I'd argue that this definition eliminates these threats from view. Due to the interconnected nature of security, I'd argue that external be dropped from the definition.	
R002	The definition seems to treat the concept of security with inadequate flexibility. It is implied, by this definition, that space systems security is either not present or has failed if an asset placed outside Earth's atmosphere were to become the target of interference by a third party. I would argue that security is underpinned by the ability to retain control over, and manage the conditions of, that which is meant to be secured for the purposes of maintaining/providing the desired state of security. With that in mind, I would propose the following modified version of Moltz's definition: "Space systems security is the ability to launch, place, operate and maintain control over assets outside Earth's atmosphere and the corresponding risk management capabilities designed to resist, prevent and/or mitigate external and internal threats of interference, damage, or destruction".	No
R003	It is adequate. A space asset is only valuable if you can communicate with it, so we need security on the ground side too - so it must be clear that this is included in the 'interference piece'.	Yes
R004	Seems fair	Yes
R005	The language is a little inconclusive as it appears to be solely focused on the space segment. What about the ground control segments and the supply chain assurance. Furthermore, Moltz lists external interference and overlooks the insider threat aspect too. Furthermore, I'm wondering if the concept of recovery/resilience and continuity of service aspects are covered appropriately, i.e. perhaps this should read to 'maintain operations, despite external interference or deliberate damage'.	No
R006	No, I don't believe it does. Operation of an asset sits in the context of a time frame, perhaps 20+ years. Operation in this context requires 'tasking' through command and control, i.e. cybernetics. 'External interference' is a designed function of the asset, a feature. The quote above needs to qualify 'good' from 'bad' and/or redraw the trust boundary. You'd do well to review Stafford Beer's Viable System Model as an cybernetic framework.	No
R007	False, I think that the reason why we put things in space is the knowing of the slight chance the Space asset will be lost, damaged, or partial use. That is the whole reason for resiliece and proliferation. I use an acronym D4P2, that I am willing to share.	No
R008	Yes	Yes
R009	It does adequately define it, but of course raises some questions, such as the impossibility of protection against eg physical degradation or destruction. It is difficult to encompass the complexities of space security in one short sentence! The table below illustrates this well.	Yes
R010	I agree with Moltz's definition. I would also like to see a brief explanation of the term 'external interference' so that we can understand that this may be human induced and non-human induced (eg environmental)	Yes
R011	Yes	Yes
R012	Security can refer to different things, but the definition offered conflates security with resilience and other functions in a hostile environment. For example is atmospheric	No

	interference considered external? I would argue security should relate to confidentiality, integrity and availability as it relates to specific threat actors.	
R013	for space it should involve degradation, denial and destruction. I also wonder if it should be expanded to place, operate, upgrade and de-orbit assets	No
R014	yes as long as this definition includes the services to and from space as part of the space eco system ie the data	Yes
R015	From a Defence perspective this is mostly adequate, however does 'external' apply to the natural space events/environment e.g. micro meteoroids, orbital debris, radiation?	Yes
R016	I think it's a good definition	Yes
R017	Use of the word 'external' is potentially problematic, mainly because its unclear what system boundary is between internal/external. E.g. Depending on how it is interpreted it might exclude issues relating to supply chain compromise, and insider threats (intentional and unintentional), as these are internal to the system. 'interference' is perhaps a bit imprecise - unclear if this would cover adversary intelligence collection which may not interfere with correct operation of the system, or other unauthorised use of the system which doesn't cause interference.	No
R018	That is not a bad definition overall. In some thinking it possibly does not communicate retaining positive control and retention of custody [i.e. operate assets 'as intended']. Some might also argue that this definition is a bit ambiguous in respect to "…operate… …without external interference, damage or destruction" – is the asset resilient to this, or not causing it? Some could argue that it should communicate some aspect of the wider environmental security too [e.g. asset/junk reflectivity impacts astronomy].	Yes
R019	I think that the biggest omission is passive interception of C&C and data that could be done outside of the above definition.	No
R020	Damage and destruction are potential outcomes of external interference. I'm not sure if this is an accurate definition.	No
R021	No - it is too narrow - for example, satellite systems require earth stations. Space cyber attacks may occur on earth. it should include the potential for other areas to "influence" space	No
R022	It is a great succinct defined. I would add degradation even though it is implied. It also doesn't cover privacy.	Yes

Table 13 - Delphi Study Round 1 Question 1 Survey Responses

In summary, the expert consensus on the suitability of the definition posed in Round 1 Question 1 of the Delphi Study was 11 votes for no and 11 votes for yes, leading to a 50% consensus rate. This is an inadequate rate of consensus and so analysis was conducted to improve on the proposed definition based on the issues and suggestions raised by the expert respondents, as detailed in the following section.

4.1.2.1.1.2 Analysis

Each of the responses recorded at Table 13 were analysed before being grouped and summarised by theme. All respondents' suggestions have been taken into account regardless of whether the respondent agreed or disagreed with the proposed definition in the original question. Decision outcomes were then documented in the final column of Table 14 for those expert responses that prompted a change or addition to be made for the Delphi Round 2 survey.

ID	Summary and interpretation	Analysis and comments	Decisions
A001	Issue with the word 'external' as it excludes threats that originate from within the system. Suggests that external be removed from the definition.	Agree that the definition of space systems security should include internal threats such as Trusted Insiders.	1. Remove 'external' from the threat component of the definition.
A002	Issue with the word 'external' as it excludes internal threats. Issue with the use of "without interference" as it implies that space systems security will have failed if the system were to become the target of interference by a third party. Suggests including regaining control of the system once interfered with.	The exclusion of internal threats from the definition has been addressed as per Decision 1 documented at A001. Agree that "without interference" should be removed from the definition. Regaining control of the system post-incident includes functions such as incident response, crisis management, disaster recovery, and business continuity planning. These are functions that operate after a security breach to get the space system and its associated security features back online and manage any impacts of the incident. These functions are resilience features that enable the ongoing security of the space system, even after breach.	1. Remove "without interference" from the definition.
A003	The proposed definition is adequate as long as the ground segment is included as part of the 'interference' piece.	This response indicates an issue with Moltz's inclusion of "outside the Earth's atmosphere" in the definition. To ensure the security of space systems the ground segment is an	1. Modify the definition to include the Ground Segment.

		essential component that must be considered.	
A004	The proposed definition is adequate.	No analysis required.	No changes made.
A005	Issue with the focus on the space segment, suggests including ground control segment and supply chain assurance. Issue with the word 'external' as it excludes insider threat.	This response indicates an issue with Moltz's inclusion of "outside the Earth's atmosphere" in the definition, an issue which has been addressed as per Decision 1 documented at A003. They also suggest that the supply chain should form part of the defined space system. The issue with 'external' threat is consistent with other expert responses and has been addressed as per Decision 1 documented at A001.	1. Add supply chain to the definition
A006	Issue with the use of "without interference" in the definition as it can be a designed feature of the asset. Issue with a lack of reference to a timeframe or lifecycle in definition as the operation of a space asset can occur over 20 years or more. Suggests that the definition should qualify good interference from bad interference based on trust.	The issue with "without interference" is consistent with other expert responses and has been addressed as per Decision 1 documented at A002. Agree that the security of a space system is ongoing and should occur across life of system. The security of a space system should remain intact regardless of the type of threat it faces. In this case, a 'good interference' would not be considered a threat as it does not lead to negative impacts to the system or its security. The definition should remain agnostic to threat and interference definitions.	1. Modify the definition to cover the full life of system. 2. Remove 'interference' from the definition.
A007	Issue with the use of "without damage or destruction" in the definition as loss or damage is a known and unavoidable risk that must be accepted when deploying space systems. It is often impossible to protect systems against physical impacts. Suggests referring to resilience and proliferation in the definition.	Agree with the respondent's concern. The line "without damage or destruction" should be removed from the definition. As per the analysis documented at A012, the suggestion to refer to resilience and proliferation in this Space Systems Security definition can be disregarded.	1. Remove "without damage or destruction" from the definition.

A008	Proposed definition is adequate.	No analysis required.	No changes made.
A009	Proposed definition is adequate, but it highlights the impossibility to protect against physical impacts.	The respondent's issue with the inability to protect against physical impacts is consistent with other expert responses and has been addressed as per Decision 1 documented at A007.	No changes made.
A010	Proposed definition is adequate but should be expanded on to include both human-induced and non-human induced threats.	Concern regarding the scope of the threat definition is consistent with other expert responses and has been addressed as per Decision 2 documented at A006.	No changes made.
A011	The proposed definition is adequate.	No analysis required.	No changes made.
A012	The proposed definition conflates security with resilience. Suggest that security should relate to confidentiality, integrity and availability. Issue with 'external' interference as it is too broad.	This answer conflicts with the response at A007, which states that resilience should be explicitly referred to. There is an abundance of literature that seeks to distinguish between security and resilience, claiming them to be two distinct concepts. In line with existing literature the definition of Space Systems Security should indeed remain separate and distinct from the definition for Space Systems Resilience.	1. Add confidentiality, integrity, and availability to the definition.
A013	The definition should include degradation and denial in addition to destruction. The definition should be expanded to place, operate, upgrade and de-orbit assets.	Destruction was removed from the definition as per Decision 1 documented at A007. The first suggestion can therefore be disregarded. The lack of reference to the entire lifecycle of the space system has been raised in other expert responses and has been addressed as per Decision 1 documented at A006.	No changes made.
A014	The definition is adequate so long as it encompasses the space system's data and services to and from space.	The definition's exclusion of terrestrial system components has been addressed as per Decision 1 documented at A003.	1. Add 'data' to the definition. 2. Add the Communications

		Agree that data should be included in the definition. The communications segment should also be explicitly mentioned as the mechanism for transferring value to and from space.	Segment to the definition.
A015	The definition is mostly adequate but should include further clarification on whether security includes security against natural space threats such as orbital debris or radiation.	The issue with 'external' interference wording is consistent with other expert responses and has been addressed as per Decision 1 documented at A001.	No changes made.
A016	The proposed definition is adequate.	No analysis required.	No changes made.
A017	Issue with the word 'external' as it excludes internal threats. Issue with the use of "without interference" as it is unclear whether this would cover passive adversary operations such as intelligence gathering.	The issue with 'external' interference wording is consistent with other expert responses and has been addressed as per Decision 1 documented at A001. The issue with "without interference" is consistent with other expert responses, albeit from a different perspective, and has been addressed as per Decision 1 documented at A002.	No changes made.
A018	Issue with the use of "without interference, damage or destruction" as it is too ambiguous. Suggest including natural events in the scope of the definition. Suggest including "operate assets as intended" in the definition.	The issue with "without interference, damage or destruction" is consistent with other expert responses and has been addressed as per Decision 1 documented at A002. Concern regarding the scope of the threat definition is consistent with other expert responses and has been addressed as per Decision 2 documented at A006. Operating an asset as intended still fails to consider passive attacks, such as eavesdropping (as raised in R017). By assuring the confidentiality, integrity, and availability of a space system (as per Decision 1 of A012), it can also be assured that the asset will	No changes made.

		operate as intended (insofar as security is concerned).	
A019	The definition is missing passive threats, communications, and data.	Concern regarding the scope of the threat definition is consistent with other expert responses and has been addressed as per Decision 2 documented at A006. The suggestion to include the communications segment is consistent with other expert responses and has been addressed as per Decision 2 documented at A014. The suggestion to include data in scope of the definition is consistent with other expert responses and has been addressed as per Decision 1 documented at A014.	No changes made.
A020	Issue with the use of "without interference, damage or destruction" as it is too ambiguous.	The issue with "without interference, damage or destruction" is consistent with other expert responses and has been addressed as per Decision 1 documented at A002.	No changes made.
A021	The proposed definition is too narrow as it neglects the interaction of the Space Segment with Earth.	The definition's exclusion of terrestrial system components has been addressed as per Decision 1 documented at A003.	No changes made.
A022	The definition is adequate but does not explicitly include privacy or degradation.	The concern surrounding privacy falls under an issue with the scope of the threat definition. This is consistent with other expert responses and has been addressed as per Decision 2 documented at A006. Damage and destruction were removed from the definition as per Decision 1 documented at A007. The suggestion regarding the addition of 'degradation' to the definition can therefore be disregarded.	No changes made.

Table 14 – Analysis of Delphi Study Round 1 Question 1 Survey Responses

In the analysis above there were a number of key themes that arose from the collective expert responses:

- Most respondents that answered ‘no’ had an issue with the explicitly specified ‘external’ interference in the definition, which neglects internal threats.
- Issues with the phrase "interference, damage or destruction" in the definition was the second most common reason that respondents answered ‘no’, primarily due to the inevitability of incurring such impacts over the lifecycle of many space systems.
- Issue with “outside Earth’s atmosphere”, which neglects Earth-based components and threats.
- Issue with the lack of reference to a timeframe or lifecycle for the space system in the definition.

4.1.2.1.1.3 Outcomes

In response to Moltz’s definition, as applied to space systems security, approximately half the respondents stated that the definition was adequate, some qualifying their support with possible improvements. The other half stated that Moltz’s definition is not adequate for defining space systems security, each raising one or more reasons to support their opinion.

Of the respondents that provided comments suggesting that Moltz’s definition should be modified, most raised an issue with the word ‘external’. The general agreement was that modern threats often originate internal to the system, such as an Insider Threat or coding flaw. A significant proportion of respondents also raised concern with the phrase ‘outside Earth’s atmosphere’, arguing that critical segments such as ground, control, and supply chains exist terrestrially. Additionally, a number of expert respondents took issue to the limitations of the terms ‘interference, damage, or destruction’, stating that it is not possible to avoid such outcomes in the space environment, given the non-malicious threat context (for example, radiation and space junk). Some respondents also mentioned the need for the definition to include a timeframe or sense of lifecycle, given the short pre-defined lifespan of most space systems.

The table below captures a summary of the changes made to the proposed definition based on the analysis of the expert opinions provided in the responses:

Ref	Modifications
A001-1	Remove ‘external’ from the threat component of the definition.

A002-1	Remove “without interference” from the definition.
A003-1	Modify the definition to include the Ground Segment.
A005-1	Add supply chain to the definition.
A006-1	Modify the definition to cover the full life of system.
A006-2	Remove ‘interference’ from the definition.
A007-1	Remove “without damage or destruction” from the definition.
A012-1	Add confidentiality, integrity, and availability to the definition.
A014-1	Add ‘data’ to the definition.
A014-2	Add the Communications Segment to the definition.

Table 15 - Summary of post-analysis changes to the Delphi Study Round 1 Question 1 proposal

Given the modifications noted above, and taking into account other less significant or unified comments, the resulting definition came to be:

“Space Systems Security is the ability to assure 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”.

4.1.2.1.2 Question 2 – Space Systems Security Domain

With an understanding of the criticality of space infrastructure, its deepening vulnerability issues, and the unpredictable threat environment within which it is situated, it is easy to see the importance of space security. Unfortunately, up until now there has been little recognition or structure afforded to the complex domain of space systems security.

The kind of efficiency needed to compete in the volatile arena of this new space race is only made possible through a better understanding of space systems security as a specialist interdisciplinary domain, where each contributing field has a valid voice for enhanced collaboration. The second question in the expert survey attempts to define the scope of the space systems security domain.

The initial model of the knowledge domain, constructed in Table 3, was provided to the expert respondents as per section 3.3.2.3.2, to which the respondents stated whether they believed anything was missing or inaccurate.

The question posed was: *Based on your experiences working with space technologies, do you believe anything is missing or inaccurate in Table 3?*

4.1.2.1.2.1 Responses

Table 16 below provides the verbatim expert survey responses to Question 2 alongside a high-level yes or no assessment that summarises the respondents' answer to the question as posed in the survey and summarised in Section 3.3.2.3.2. Note that spelling and grammatical errors have been included to avoid any inadvertent interference with the raw data.

The summary of response, analysis, and decision outcomes (i.e. changes made to the original knowledge domain table) of each of the below responses are detailed in the following section.

ID	Response	Answer
R023	No.	No
R024	The table seems valid and comprehensive from my perspective. I have a few suggestions for consideration that, if deemed valid and not yet covered by an existing category, I would recommend including. 1. Malicious Insider Threats/espionage – the threat could be as severe as hijacking an asset in space or on the ground. 2. Information warfare – I am thinking here of impersonation and the distribution of disinformation for the purposes of manipulating/corrupting operation of space or ground assets. 3. This is not a threat vector or an attack surface, but I think that physical mobility of some assets, particularly ground-based control systems, can dramatically increase their survivability and decrease the viability of some threats. 4. Similarly, a space or ground asset equipped with a suitable retaliatory capability (be it kinetic or otherwise) introduces the various advantages afforded by deterrence as an element of space systems security.	No
R025	I like the table from source to entry-point. Not sure what each internal box represents though (i.e. is that the method to mitigate)? We should capture optical comm interference somewhere. What about non-direct like GPS-jamming or losing NORAD TLE or taking out external ground tracking like radars? On the space side- im not sure what internal comms encapsulates? optical comm should be added. Should also add the Spacecraft mechanical ie the bus and power systems as a new column.	Yes
R026	This looks comprehensive but not detailed. IAM should be complimented with awareness etc	Yes
R027	Personnel Security is not mentioned? Insider is a major threat vector. Quantum encryption, Directed Energy (laser), Co-orbital ops (i.e, block view) Perhaps the concept of maneuvering for protection from deliberate action or space junk etc?? Is this all now just a 'military space ops' domain? Should not all users respond to threats?	Yes

R028	this is useful as a high-level taxonomy but it's level of abstraction hides important detail. e.g. cryptographic key material generation and handling.	No
R029	There need to be a section under Ground and Space Platforms for "Data". For example encryption, zero trust, obfuscation, RF, etc. Please reach out for more details and inquiry if interested.	Yes
R030	I'm not sure where it fits but the malicious addition of hidden electronic components should be included somewhere. Maybe that's covered in 3PP but it's not obvious to me. Also, I guess that GNSS spoofing/jamming is included under RF/Electronics, but it could be made more obvious.	No
R031	I don't know what is encompassed with the concept of military space ops, so it is difficult to comment.I think that the risk of harm from space debris should be noted (it might be malicious or non-malicious in context) Would kinetic engagement always necessitate "Military Space Ops"? Would there be occasion when a cyber attack or electronic attack may implicate a military response? This may require greater nuance.	Yes
R032	Very good. No changes suggested.	No
R033	the table is adequate	No
R034	I can’t see how non-malicious actions relate to security. I don’t fully understand the axis and labels of the table. If this is about security should it depict risks? How were these categories developed? You’ve got launchpad - what about launch vehicle?	Yes
R035	Todd Harrison has a simpler but possible more effective taxonomy in Defence against the Dark Arts in Space	Yes
R036	this covers most of the obvious technical ways to disrupt the space eco system. The less technical challenges are the regulatory, political and even legal, social, moral and ethical challenges which could impact system eco system. As an example, failure to enfore constellation regulatory framework and compliance could result in collisions which could render whole orbits inoperable with space debris.	Yes
R037	Not sure what the difference is between payloads and onboard sensors? The Space Platforms does not include propulsion, nor software. Impacts by debris or meteoroids are kinetic - physical so not Military SpaceOps. Where would non-RF directed energy fit - electronic? May need more than Telecom/Materials Engineering to protect.	Yes
R038	I think anything that denies operations is a threat, so there are some more basic things missing like disruption to human resources, power system attacks and distractive actions	Yes
R039	I wonder if 'information/data' should exist as a column in its own right? It is potentially a target of theft, manipulation, denial (eg. ransomware), damage and destruction - through non-malicious means, cyber means and physical means. This includes all the valuable information about the system itself (design schematics, other intellectual property) as well data/information relating to operations, and data/information collected by the space platform's sensors. 'Supply Chain' is a bit imprecise - does this cover all design and build/assembly (even where you are doing this in house)? Also, does it cover supply chain only of the space platform, or also supply chain of all the ground elements? The Ground	Yes

	Segment will have rocket/space platform assembly facilities - this is missing. The Ground Segment will have comms infrastructure that links ground stations, and launchpads and the like - this is missing. The Ground Segment will be dependent on critical infrastructure (power, water, telecommunications, etc) - this is missing. The Ground Station will have OT (electricity generators, motors driving dishes/antennas, etc.) and needs OT security. It also has IT and networks and will need cyber security. Not sure what you mean by 'cyber operations' here - Defence has a particular definition of cyber ops, as distinct from cyber security, but this may not carry across to the civil world. Also, cyber ops would seem to be applicable across more elements. For Personnel, there are other means beyond Cyber IAM to address cyber issues - culture, training, etc. We broadly group this as 'human aspects of cyber'. The Space Platforms seems to assume uncrewed space platforms. If humans on board then 'personnel' will present in both ground segment and space platform, and space platforms will have life support systems, and quality-of-life (e.g. entertainment) systems. The Space Platforms will have propulsion and power systems - this is missing. The electronic protection of space platform may draw on the EW discipline - e.g. for signature management (to defeat targeting), electronic self protection, countermeasures. EW also has relevance to defeating Kinetic Physical and Non-Kinetic physical.	
R040	That is a reasonable definition set, but the table may be a bit broadly quantised. Kinetic physical SV impacts are not entirely attributable to MIL Space Ops – they can be purely unintentional/accidental [Non-Malicous Threats], and this is becoming much more relevant. Supply chain factors can also be relevant entries to the SV [e.g. through parts qualifications/reliability, LEO COTS firmwares etc] that needs particular domain expertise to address. Non-Kinetic Physical might be expanded to include Electromagnetic Compatibility (EMC) which is arguably a much more likely threat than EMP.	Yes
R041	This is very focused on physical type threats, as opposed to passive based risks and also there are numerous legal issues.	Yes
R042	The terms in each cell are very broad so it is difficult to determine if this is an accurate reflection of the technical discipline. Is the intent to decompose/compartmentalise the problem to a series of disciplines?	Yes
R043	no	No
R044	There are two missing segments: control and terminal. Terminal is likely only applicable for space services (GPS and SATCOM). The threat of high altitude nuclear detonation isn't covered off (atmospheric scintillation). This is probably a Physics field. Atmospheric effects impact communications links -> meteorological.	Yes

Table 16 - Delphi Study Round 1 Question 2 Survey Responses

In summary, the expert consensus on the suitability of the definition posed in Round 1 Question 2 of the Delphi Study was 15 votes for yes and 7 votes for no, leading to a 68% consensus rate. This is an inadequate rate of consensus and so analysis was conducted to improve on the

proposed knowledge domain based on the issues and suggestions raised by the expert respondents, as detailed in the following section.

4.1.2.1.2.2 Analysis

Each of the responses recorded at Table 16 were analysed before being grouped and summarised by theme. All respondents' suggestions have been taken into account regardless of whether the respondent agreed or disagreed with the proposed definition in the original question. Decision outcomes were then documented in the final column of Table 17 for those expert responses that prompted a change or addition to be made for the Delphi Round 2 survey.

ID	Summary and interpretation	Analysis and comments	Decisions
A023	The proposed knowledge domain table is adequate.	No analysis required.	No changes made.
A024	The proposed knowledge domain table is adequate but ensure that insider threat, espionage, and information warfare is covered off. Suggest inclusion of retaliatory capabilities for deterrence.	Malicious insider threat and espionage is covered under 'Protective Security' and 'Personnel'. Information warfare is covered under the cyber threat category. Interesting note about physical mobility as a countermeasure against some threats. However, for the purposes of the knowledge domain table this would be considered a potential mitigation that may be implemented by someone in the field of, say, Electronics or Robotics engineering as already captured in the table under 'Space Platforms'. This category is intended to be broad to allow for flexibility as the sector continues to advance. Weaponised space systems may be another suitable countermeasure depending on the use case. This would most likely be implemented under the 'Military SpaceOps' cell in the table.	No changes made.
A025	The knowledge domain table is not easy to understand. The table is	Agree that the proposed table is awkward to interpret without	1. Change presentation of

	missing the following: optical communications interference, non-direct attacks such as jamming, and mechanical components such as the power system. It is unclear what 'internal communications' encompasses.	supporting text. The table could be improved with a small amount of text to describe the purpose of each cell. Optical communications interference would be considered a non-kinetic physical attack and is covered under 'Telecommunications Engineering'. Agree that this can be made more clear. Bus and power requirements are part of the internal communications category and so are already covered. This can also be made more clear in the table.	table for improved clarity. 2. Add a supporting legend to assist with interpretation of terminology. 3. Separate communications out into a separate segment.
A026	The knowledge domain table is comprehensive but not detailed enough. Suggest adding awareness training to complement 'Cyber IAM' in the cell corresponding to cyber threats to/by personnel.	The indication that there is insufficient detail in the proposed table is consistent with other expert responses and has been addressed as per Decision 2 documented at A025. Agree that cyber security training and awareness should be included in the table as indicated.	1. Add cyber security training and awareness to the cell corresponding to cyber threats to/by personnel.
A027	'Personnel Security' is not mentioned. Insider is a major threat vector. Suggest adding quantum encryption, directed energy, co-orbital operations, and manoeuvrability.	Personnel security comes under the 'Personnel' column as well as under 'Protective Security'. The table is intentionally kept at a high-level to avoid specifying technologies or platforms that could reduce the longevity of the model. Although the indication that there is insufficient detail to make this aspect self-explanatory is consistent with other expert responses and has been addressed as per Decision 2 documented at A025. Agree that directed energy threats, such as lasers, should be explicitly mentioned in the table.	1. Add directed energy weapons to the supporting legend at A025 Decision 2.
A028	The knowledge domain table is comprehensive but not detailed enough.	The indication that there is insufficient detail in the proposed table is consistent with other expert	No changes made.

		responses and has been addressed as per Decision 2 documented at A025. Agree that cyber security training and awareness should be included in the table as indicated.	
A029	The knowledge domain should mention data more explicitly and include relevant data security technologies.	Agree that data and computing should be given more weight in the table.	1. Add 'Data' to the supporting legend at A025 Decision 2. 2. Add 'Computing' to the new column created at A025 Decision 3.
A030	The malicious addition of hidden electronic components and spoofing/jamming could be made more clear in the table.	The malicious addition of hidden electronic components is covered by 'Supply Chain Security' in the table. Agree that RF attacks such as spoofing, and jamming could be made more clear.	1. Add key RF attacks to the supporting legend at A025 Decision 2.
A031	'Military Space Ops' requires further elaboration as it is too broad and can apply to other areas outside kinetic-physical. The table is missing space debris aspects, both incidental and malicious.	Agree that 'Military Space Ops' is unclear and ambiguous. Agree that space debris requires greater emphasis in the model.	1. Replace 'Military Space Ops' with more descriptive sub-categories of counterspace operations. 2. Add space debris to the supporting legend at A025 Decision 2.
A032	The proposed knowledge domain table is adequate.	No analysis required.	No changes made.
A033	The proposed knowledge domain table is adequate.	No analysis required.	No changes made.
A034	The knowledge domain table is not easy to understand. Non-malicious actions should be out of scope for security considerations. Launch vehicle is missing from the table.	The issue with the clarity of interpreting the knowledge domain table is consistent with other expert responses and has been addressed as per Decision 1 and 2 documented at A025. Non-malicious actions must be captured by the knowledge domain as	1. Add launch vehicle to the supporting legend at A025 Decision 2.

		there are aspects that should be considered by security and resilience efforts. For example, incidents caused by non-malicious insider threats or availability requirements. Launch vehicle is covered under payload but agree that this can be made more clear.	
A035	Todd Harrison has a simpler but more effective taxonomy.	The row categories in this proposed knowledge domain table were taken from the taxonomy proposed in the paper 'Defence against the Dark Arts' (Todd Harrison et al. 2021) and the 'Space Threat Assessment' (Todd Harrison et al. 2020; Todd Harrison et al. 2022), as published by CSIS. Todd Harrison's space threat taxonomy achieves a different objective than what is trying to be achieved in this table. The goal of this table is to identify the different areas that contribute to the field of Space Systems Security, of which the threat types play only one part.	1. Simplify the threat categories used for the rows in the table.
A036	The proposed knowledge domain table is missing the legal, social, moral, and ethical challenges that can impact the system.	Agree that the non-technical aspects of the space system does not have sufficient emphasis in the proposed table. Legal, social, moral, and ethical challenges affect all aspects of the space system; space, ground, and communications and computing. Therefore a new column should be added to the knowledge domain that covers governance aspects associated with operating a space system.	1. Separate governance out into a separate segment.
A037	The tables requires greater clarity on payloads, onboard sensors, and non-kinetic physical impacts. Missing onboard software and propulsion.	Non-malicious kinetic physical impacts, such as debris and meteoroids, are covered in the table but the indication that there is insufficient detail to make this aspect	No changes made.

		self-explanatory is consistent with other expert responses and has been addressed as per Decision 2 documented at A025. The lack of emphasis on software and propulsion has been noted in other expert responses and has been addressed as per Decision 1 and 2 documented at A025 as well as the decisions documented at A029.	
A038	The table is missing disruption to human resources, power system attacks, and distractive actions.	Disruption to human resources is covered by 'Protective Security' and has been made more clear for the Round 2 survey by Decision 2 documented at A025. Power system considerations were noted in R025 and have been addressed by Decision 2 documented at A025. Three considerations were noted in R025 and have been addressed by The lack of explanatory information about the threats has been noted in other expert responses and has been addressed as per Decision 2 documented at A025.	No changes made.
A039	The knowledge domain should mention data and information more explicitly. The following terms require further explanation in the table: supply chain and cyber operations. The following considerations are missing from the table or require greater emphasis: manufacturing facilities, communications infrastructure, training and culture, propulsion and power systems.	The lack of emphasis on data and information has been noted in other expert responses and has been addressed as per Decision 1 and 2 documented at A029. The indication that there is insufficient detail in the proposed table is consistent with other expert responses and has been addressed as per Decision 2 documented at A025. Propulsion and power system considerations were noted in R025	1. Add 'Human Factors' to the considerations for the space platform. 2. Add manufacturing facilities to the supporting legend at A025 Decision 2.

	The ground station should include OT security. The space platform may include personnel.	and have been addressed by Decision 2 documented at A025. Agree that manufacturing and personnel considerations should be given more emphasis in the table.	
A040	The knowledge domain table is comprehensive but not detailed enough. Non-malicious threats are becoming more relevant for kinetic physical impacts. Supply chain threats should apply to space vehicle as well. Non-Kinetic Physical should be expanded to include Electromagnetic Compatibility (EMC).	The indication that there is insufficient detail in the proposed table is consistent with other expert responses and has been addressed as per Decision 2 documented at A025. The comment regarding non-malicious threats contradicts the comment at R034 but supports the decision made at A034. The indication that supply chain should be considered across both ground and space segments is consistent with other expert responses and has been addressed as per Decision 1 documented at A036.	1. Include EMC alongside EMP in the table.
A041	The knowledge domain is missing legal aspects and non-physical risks.	The opinion that the knowledge domain is lacking consideration of legal and other governance aspects is consistent with other expert responses and has been addressed as per Decision 1 documented at A036. Non-physical risks are covered by cyber, electronic, and non-kinetic physical threats in the rows. However, the indication that there is insufficient detail to make this aspect self-explanatory is consistent with other expert responses and has been addressed as per Decision 2 documented at A025.	No changes made.
A042	The knowledge domain table is comprehensive but not detailed enough.	The issue with the clarity of interpreting the knowledge domain table is consistent with other expert responses and has been addressed as	No changes made.

	The knowledge domain table is not easy to understand.	per Decision 1 and 2 documented at A025.	
A043	The proposed knowledge domain table is adequate.	No analysis required.	No changes made.
A044	The proposed knowledge domain is missing the following considerations: control segment, terminal segment, and atmospheric scintillation (i.e. 'Physics').	The control segment is captured under 'Computing' / 'Personnel' and the terminal segment is captured under 'Computing' / 'Radio Link & Telemetry'. However, the indication that there is insufficient detail in the proposed table is consistent with other expert responses and has been addressed as per Decision 2 documented at A025.	1. Add 'Physics' as a consideration to kinetic-physical impacts

Table 17 – Analysis of Delphi Study Round 1 Question 2 Survey Responses

In the analysis above there were a number of key themes that arose from the collective expert responses:

- The knowledge domain table is comprehensive but has insufficient detail for self-evident clarity and interpretability.
- The presentation of the knowledge domain table could be simplified.
- Lack of emphasis on mechanical aspects of the space system such as propulsion and the power system.
- Missing governance aspects such as legal, regulatory, and social.
- Communications and computing, including data, requires greater emphasis.

4.1.2.1.2.3 Outcomes

Approximately two thirds of the respondents proposed at least one addition or modification to the initial model. These proposed changes were then incorporated into the modified knowledge domain table, as presented in Table 4 and further detailed in Table 5 and Table 6.

In Table 4 key threat types (rows) are correlated against key system segments (columns) that may be targeted. The resulting cells represent the 16 core functions of space systems security—ultimately, that is to fulfil the above definition of space systems security.

The segments detailed in Table 5 form the four key components of any space system:

- Governance segment;

- Ground segment;
- Space segment; and
- Communications, control, and computing (C3) segment.

In this model, the governance segment includes any people, policies, and processes in place to design, build, launch, operate, maintain, and decommission a space system. The ground segment includes any terrestrial technologies or subsystems that form part of the overall space system, while the space segment represents the same but for technologies and subsystems deployed outside Earth's atmosphere. Finally, the C3 segment includes anything that exists in or serves exclusively interacts with cyberspace, such as computing infrastructure, control signals, radio links, and data itself.

The threats to space systems detailed in Table 6 are an adaptation of the counter-space threats proposed by Harrison et al. (2022). The categories of Electronic and Non-Kinetic threats were combined, as per common feedback from the respondents. This change was also noted to align with the commonly used military terms 'cyber warfare' and 'electronic warfare'.

The table below captures a summary of the changes made based on the expert opinions:

Reference	Modifications
A025-1	Change presentation of table for improved clarity.
A025-2	Add a supporting legend to assist with interpretation of terminology.
A025-3	Separate communications out into a separate segment.
A026-1	Add cyber security training and awareness to the cell corresponding to cyber threats to/by personnel.
A027-1	Add directed energy weapons to the supporting legend at A025-2.
A029-1	Add 'Data' to the supporting legend at A025-2.
A029-2	Add 'Computing' to the new column created at A025-3.
A030-1	Add key RF attacks to the supporting legend at A025-2.
A031-1	Replace 'Military Space Ops' with more descriptive sub-categories of counterspace operations.
A031-2	Add space debris to the supporting legend at A025-2.
A034-1	Add launch vehicle to the supporting legend at A025-2.
A035-1	Simplify the threat categories used for the rows in the table.
A036-1	Separate governance out into a separate segment.
A039-1	Add 'Human Factors' to the considerations for the space platform.
A039-2	Add manufacturing facilities to the supporting legend at A025-2.
A040-1	Include EMC alongside EMP in the table.

A044-1	Add ‘Physics’ as a consideration to kinetic-physical impacts in the supporting legend at A025-2.

Table 18 - Summary of post-analysis changes to the Delphi Study Round 1 Question 2 proposal

4.1.2.1.3 Question 3 – Space Systems Resilience Definition and Taxonomy

As demonstrated, to date there is no existing definition of ‘Space Systems Resilience’. Therefore, the third question in the survey sent to the two dozen space security experts attempted to build a contemporary taxonomy and definition for space systems resilience. The definition and taxonomy utilised for the first round of the Delphi study is as described in Section 3.3.2.3.3.

The question posed was: *In your opinion, does the proposed definition and taxonomy (as at Figure 25) adequately capture the concept of Space Resilience?*

4.1.2.1.3.1 Responses

Table 19 below provides the verbatim expert survey responses to Question 3 alongside a high-level yes or no assessment that summarises the respondents’ answer to the question as posed in the survey and summarised in Section 3.3.2.3.3. Note that spelling and grammatical errors have been included to avoid any inadvertent interference with the raw data.

The summary of response, analysis, and decision outcomes (i.e. changes made to the original knowledge domain table) of each of the below responses are detailed in the following section.

ID	Response	Answer
R045	It looks good yes.	Yes
R046	Yes - this covers it well.	Yes
R047	Yes.	Yes
R048	I believe the definition and taxonomy presented here is comprehensive and suitably captures the concept of space resilience.	Yes
R049	yes, i think its adequate. However, is there really any difference between Survive and Sustain? Perhaps the sustain could be something like sustain system critical functionality. ie have a tiered approach to resilience and a graceful degradation under an attack where the priority is on mission critical functionality of the spacecraft. Is the adapt intended to be autonomous or is that a longer term user-in-the-loop?	Yes
R050	I would put it in terms of maintaining function in an increasingly contested environment. The assumption of a consistent baseline of activity seems optimistic.	No
R051	This is a sound, succinct list, which captures the key requirements well.	Yes

R052	Yes, it does, in the sense that it represents a Darwinian evolutionary approach.	Yes
R053	D4P2 -- Disaggregation — Separating missions that have different purposes, so that a single satellite is not carrying both conventional and nuclear systems, for example, or surveillance and communication systems. Diversity — Using multiple systems to achieve the same goal, such as having U.S. equipment that can use both GPS and Europe's Galileo navigation system. That way if an adversary disrupts GPS, U.S. forces could still use allied assets. Distribution — Spreading out capabilities across multiple satellites, so that no one satellite is fundamental to the system working. Loverro again used the example of GPS, where several satellites could be destroyed but the system would keep working. Deception — Not letting adversaries know which satellites are carrying which systems, or other means of misleading an enemy. Protection — Hardening satellites to defend against threats, or giving them ways to avoid incoming threats. Proliferation — Deploying multiple satellites to conduct the same mission. It's slightly different than distribution in that a single satellite can carry out the complete capability, but the other satellites are providing redundancy and back-ups if the first one is destroyed.	Yes
R054	Yes	Yes
R055	Yes it appears to capture it.	Yes
R056	I wonder about the concentration on HILF. What about other events along the frequency and impact spectrum? In my role as Co-Chair of the Space Trusted Information Sharing Network of the Critical Infrastructure Advisory Council, Department of Home Affairs, I am helping oversight a process that is examining the vulnerability of Australia's critical infrastructure to disruptions to the space services on which this CI relies. The formal analysis that is being undertaken is utilising the ISO 31,000:2018 Risk Management standard. Risk and resilience go hand in hand and some recognition of this relationship would be beneficial.	No
R057	Yes it captures most of the issues in the critical infrastructure literature	Yes
R058	I'm not sure why high impact and low frequency is more relevant than any other type of event. Surely any event can impact resilience, regardless of frequency?	No
R059	Not sure the HILF inclusion adds anything - if the system needs to deal wth a low impact high frequency event surely the same outcome is sought.	No
R060	Again, this is a very technical construct, as long as things like sustain include the moral/ethical and legal implications to maintian the will to continue this is a good framewlrk.	Yes
R061	Not sure I agree with the restriction to HILF events. In a contested space domain, the frequency may be high or even constant.	No
R062	The taxonomy assumes that system needs to be resilient, it could, equally be invisible (or more practically, unobserved) to threats	Yes
R063	This seems pretty good to me. However, it seems counterproductive to limit it to HILF events only though - the intent should be for the system to be resilient to any adverse event.	Yes
R064	Yes, that taxonomy and definition makes a great deal of sense. I know that it is just a literal taxonomic label, but I am a little uncomfortable with the word 'Anticipate'. We can anticipate events in intrinsic design that build resilience, but we cannot realistically	Yes

	'anticipate' true Black Swan [HILF] events. A true Black Swan [HILF] event is by definition practically impossible to 'anticipate' [or 'prevent'], but it is usually easy to 'detect'. The definition provided for 'Anticipate' does encompass 'detect' [which is the real-world action on a HILF] so I'm not that fussed really. That said, I like the taxonomy in that it contemplates more than detection for resilience – as it should. 'Adapt' is described in terms of "processes and procedures" that reflect on "lessons learned" to adopt new mechanisms for response. I don't disagree with this but was expecting the idea of 'building knowledge' to appear – especially in the context of autonomous systems.	
R065	This model appears to be developed with a focus on the actual infrastructure rather than the services delivered.	No
R066	Similarities with NIST (identify, protect, detect, response and recover). Is there a danger of confusion with the NIST taxonomy? Aligning these terms with a traditional 'bow tie' model for cyber security also causes some confusion...redundant terms (particularly Survive and Sustain). May require more context. ?	No
R067	why is Space Systems Resilience limited to HILF events? Space systems should have resilience to non-HILF events also	No

Table 19 - Delphi Study Round 1 Question 3 Survey Responses

In summary, the expert consensus on the suitability of the definition posed in Round 1 Question 3 of the Delphi Study was 15 votes for yes and 8 votes for no, leading to a 65% consensus rate. Although the results fair better than the previous questions, this is still an inadequate rate of consensus. As such analysis was conducted on the expert responses to improve on the proposed definition based on the issues and suggestions raised, as detailed in the following section.

4.1.2.1.3.2 Analysis

Each of the responses recorded at Table 19 were analysed before being grouped and summarised by theme. All respondents' suggestions have been taken into account regardless of whether the respondent agreed or disagreed with the proposed definition in the original question. Decision outcomes were then documented in the final column of Table 20 for those expert responses that prompted a change or addition to be made for the Delphi Round 2 survey.

ID	Summary and interpretation	Analysis and comments	Decisions
A045	The proposed definition and taxonomy are adequate.	No analysis required.	No changes made.
A046	The proposed definition and taxonomy are adequate.	No analysis required.	No changes made.

A047	The proposed definition and taxonomy are adequate.	No analysis required.	No changes made.
A048	The proposed definition and taxonomy are adequate.	No analysis required.	No changes made.
A049	The proposed definition and taxonomy are adequate although there is confusion about the definition of 'Survive' versus 'Sustain'.	Expert respondents were not issued with the full paper describing the taxonomy and how to interpret it so there appears to be some misinterpretation. 'Survive' refers to the resilience enhancing mechanisms in place to survive and respond to the immediate impacts of an incident, whereas 'Sustain' refers to the resilience enhancing mechanisms in place to sustain operations and services in a degraded state. The definition should be self-evident and interpretable without supporting documentation.	1. Add "sustaining core operations in a degraded state" to the definition.
A050	Issue with the definition's implication of a consistent resilience baseline over time. Suggest to reference maintaining system functions in an increasingly contested environment.	This concern is covered by inclusion of the word 'recurring ability' in the definition; however it is apparent that this wording is unclear. The evolving threat environment requires a time aspect in the definition and taxonomy, but perhaps can be better represented. The definition of the 'Adapt' function in the Space Systems Resilience Taxonomy can be updated for clarity.	1. Provide more detailed taxonomical definitions for clarity. 2. Replace 'recurring ability' with 'continuously adapt' in the definition.
A051	The proposed definition and taxonomy are adequate.	No analysis required.	No changes made.
A052	The proposed definition and taxonomy are adequate.	No analysis required.	No changes made.
A053	The proposed definition and taxonomy should align with the D4P2 resilience framework: Disaggregation, Diversity, Distribution, Deception, Protection and Proliferation.	Followed up with this respondent (they identified themselves by email) to gain further clarification and it was concluded that D4P2 (United States Department of Defense 2015) is in fact complementary to the 5-phase	No changes made.

		resilience cycle proposed. The proposed resilience taxonomy provides an overarching view of the goal of resilience, whereas D4P2 provides a taxonomy of the implementation methods available to achieve resilience in satellite constellations.	
A054	The proposed definition and taxonomy are adequate.	No analysis required.	No changes made.
A055	The proposed definition and taxonomy are adequate.	No analysis required.	No changes made.
A056	Issue with the exclusive focus on HILF events. Suggest to recognise the relationship between risk and resilience.	Expert respondents were not issued with the full paper describing the taxonomy and how to interpret it so there appears to be a misunderstanding. HILF events, as opposed to LIHF events, are what distinguishes resilience from other concepts such as reliability. Regardless, the definition should be self-evident and interpretable without supporting documentation, and at the broad level of a definition it is not necessary to make such a specific distinction such as HILF. Risk assessment and management aspects of the taxonomy and definition are covered by 'Anticipate'. The lack of clarity regarding the verbatim taxonomy usage in the definition is consistent with other expert responses and has been addressed as per A051 Decision 1.	1. Remove 'HILF' from the definition.
A057	The proposed definition and taxonomy are adequate.	No analysis required.	No changes made.
A058	Issue with the exclusive focus on HILF events.	The issue with specifying 'HILF' in the definition is consistent with other	No changes made.

		expert responses and has been addressed as per A057 Decision 1.	
A059	Issue with the exclusive focus on HILF events.	The issue with specifying 'HILF' in the definition is consistent with other expert responses and has been addressed as per A057 Decision 1.	No changes made.
A060	The space systems resilience definition should include ethical, moral, and legal aspects.	One of the supporting functions to a system is the people and organisation that keeps it operating, as well as the legal aspects to which the system must comply, and which will ultimately allow for activities such as forensics and prosecution post-event. Ethical, moral, and legal aspects of operating a space system affect every aspect of resilience activities and so are covered under "including all sub-components and supporting functions" in the definition. They are also emphasised in the supporting knowledge domain after the modifications made at A036-1 in Table 18.	No changes made.
A061	Issue with the exclusive focus on HILF events.	The issue with specifying 'HILF' in the definition is consistent with other expert responses and has been addressed as per A057 Decision 1.	No changes made.
A062	The definition and taxonomy assumes that a system needs to be resilient. It should allow for avoidant countermeasures (i.e. avoid threats through stealth measures).	Any countermeasure that makes a system invisible to threats would be considered an implementation to achieve resilience. So this comment is not in disagreement with the existing definition. The 'Anticipate' category of the taxonomy explicitly includes the ability to avoid events.	No changes made.
A063	Issue with the exclusive focus on HILF events.	The issue with specifying 'HILF' in the definition is consistent with other expert responses and has been addressed as per A057 Decision 1.	No changes made.

A064	Issue with word 'Anticipate' due to the inability to anticipate black swan events. "Building knowledge" should be a function of resilience.	Although it may not be possible to anticipate a black swan event, with an anticipation approach the system should expect a security breach and be prepared to respond, regardless of the cause. This can be likened to defending against a zero day attack. However, perhaps this is better described as 'preventing' an incident rather than 'anticipating' one. This decision is reinforced by the analysis of expert responses to Delphi round 1 Question 4. Building knowledge and resilience post-attack is part of the 'Adapt' function.	1. Change 'Anticipate' to 'Prevent' in the taxonomy and definition.
A065	There is a lack of focus on the delivered services in the proposed definition.	Valid observation, services are a vital function of space infrastructure and should be explicitly mentioned in the definition.	1. Add 'services' to the scope of the definition.
A066	Confusion about the definition of 'Survive' versus 'Sustain'. Issue with similarity to NIST and alignment to the bow tie model, suggest providing further context.	The lack of clarity regarding the verbatim taxonomy usage and lack of clarity in the definition is consistent with other expert responses and has been addressed as per A049 Decision 1 and A051 Decision 1. The NIST (2018) cybersecurity framework is an input into this model and so is intended to be complementary. Future research may work to align this model with existing frameworks such as NIST.	No changes made.
A067	Issue with the exclusive focus on HILF events.	The issue with specifying 'HILF' in the definition is consistent with other expert responses and has been addressed as per A057 Decision 1.	No changes made.

Table 20 – Analysis of Delphi Study Round 1 Question 3 Survey Responses

In the analysis above the following key themes arose from the collective expert responses:

- Most respondents that answered ‘no’ to the question had an issue with the exclusive focus on HILF events in the definition.
- General confusion surrounding the scope of activity included under each taxonomical function.

4.1.2.1.3.3 Outcomes

A 65% expert consensus on the suitability of the initial proposed space systems resilience definition and taxonomy lead to a distinct lack of variety in suggestions for improvement compared to the previous questions’ analyses. The table below captures a summary of the changes made based on the expert opinions:

Ref	Modifications
A049-1	Add “sustaining core operations in a degraded state” to the definition.
A050-1	Provide more detailed taxonomical definitions for clarity.
A050-2	Replace ‘recurring ability’ with ‘continuously adapt’ in the definition.
A056-1	Remove ‘HILF’ from the definition.
A064-1	Change ‘Anticipate’ to ‘Prevent’ in the taxonomy and definition.
A065-1	Add ‘services’ to the scope of the definition.

Table 21 - Summary of post-analysis changes to the Delphi Study Round 1 Question 3 proposal

Most respondents that raised an issue or concern with the definition and taxonomy referred primarily to the use of ‘HILF’ in the definition, which was rectified for the Delphi Study survey round 2 as per A056-1 in Table 21 above.

Given the modifications noted above, and taking into account other less significant or unified comments, the resulting definition came to be:

“Space Systems Resilience is the ability of a space system, including its services, sub-components, and supporting functions to continuously adapt in order to prevent, survive, and recover from threat events whilst sustaining core operations”.

4.1.2.1.4 Question 4 – Space Systems Resilience Model

The fourth and final question posed to the expert respondents presented a model that aims to visually communicate the space systems resilience taxonomy and definition as defined in Question 3 of the round 1 Delphi Study survey.

The question posed was: *In your opinion, does the model at Figure 26 adequately explain the space resilience cycle?*

4.1.2.1.4.1 Responses

Table 22 below provides the verbatim expert survey responses to Question 4 alongside a high-level yes or no assessment that summarises the respondents' answer to the question as posed in the survey and summarised in Section 3.3.2.3.4. Note that spelling and grammatical errors have been included to avoid any inadvertent interference with the raw data.

The summary of response, analysis, and decision outcomes (i.e. changes made to the original knowledge domain table) of each of the below responses are detailed in the following section.

ID	Response	Answer
R068	Seems excellent.	Yes
R069	Unsure - it's certainly possible to be in the "Survive" state and then transition directly back to "Anticipate" but I don't think the question is asking this. It's also possible to permanently stay in the "Survive" state (ie constant communications jamming that degrades performance but you can ride through it).	No
R070	Yes.	Yes
R071	I believe that the model at figure 2 is just as suitable as the preceding definition and taxonomy, but the possibility of ongoing effects associated with a HILF, as indicated at the 'residual impact' phase of the process diagram, might be cause to consider the inclusion of an extension to the definition of 'sustain' or the inclusion of another component to the taxonomy. Specifically, the ability of a space system to repel an attacker, cleanse itself of corruption and otherwise terminate a persistent threat is essential. This relates back to my earlier comment about retaliatory capabilities. In essence, a space system's resilience could be viewed as compromised or inadequate if it does not have the ability to terminate the space resilience cycle should the need arise. A system has not truly adapted to a threat if it cannot break free of the space resilience cycle	No
R072	this is ok. but i ask what the intent is? This is the natural flow, but what is the information to extract from this?	Yes
R073	Its not likely to be a black Swann event. Its a slow escalation with increasingly contested space.	No
R074	It might just be my reading of the diagram but does the return arrow on residual impact cover system upgrade/changes post HILF? It might be covered by 'ancitipate' but I'd think there should be a clearer indication of how survival of one event, informs future designs and may	Yes

	change current operations to minimise/mitigate the HILF on different platforms i.e. pre-emptive changes on system B after observing the HILF on system A.	
R075	What this doesn't show is the environmental cyclic rate of change. Put a different way 'What is the minimum safe planning horizon?' (There is no point monitoring for an anticipated risk materialising that informs you that this particular risk is 1 month away from having a 100% chance of destroying your asset if you need eight months to react to it).	No
R076	Systems Resilience in a OODA Loop would be better. With HILF Even feeding the OODA Loop, the same. Then Residual Impact same, yet not feeding the OODA Loop.	No
R077	Yes.	Yes
R078	What if it cannot recover and creates a hazard in itself eg space debris?	Yes
R079	This is a good high level framework. A similar framework is FEMA's (and Australia's); prevention, protection, mitigation, response and recovery.	Yes
R080	I think it should have a analysis component, i mean we have to understand and learn from previous attacks, this requires cyber analytics	Yes
R081	Is there a difference between adapt and respond? Don’t understand the utility of HILF vs other event types.	No
R082	Does this include adapting to the current threat?	Yes
R083	only comment is this seems to indicate a similar weighting to all components. By nature HILF means Low Frequency so adapting to respond may not be worth the effort ie massive solar flare once in a million year event maybe adaption is not worth it whereas recovery may be only priority. .	No
R084	In the future, I would say that a linear process will be inadequate to counter and survive the space threats. So a more agile and iterative model may be required? Also how does this apply to a single space system (a satellite) to a space constellation system (multiple satellites)?	No
R085	I think it is one of many possible operational architectures that might be effective	Yes
R086	As described, the model seems too linear to me, too reactive, and as mentioned in the last question shouldn't be initiated only by HILF events. I don't see resilience as a linear lifecycle or finite-state machine with discrete phases. Rather, I see it as a range of mechanisms that can be employed in an adaptive/flexible fashion as the situation dictates. Some mechanisms will be used almost continuously, some may be used in parallel, some may be used proactively, and some may be used in a different order depending on the event and hence response needed. This is key when dealing with threats (which are intentional, with malice, thinking and hence adaptive) - as opposed to hazards. It's worth pointing out that in the cyber domain at least, system are typically under near continuous attack. Hence at any given time, one or more of these resilience mechanisms are likely be being used. Ideally, anticipate should be a continuous actvity, not one that is triggered by an adverse event (as the diagram makes it appear). In fact, I would have thought this should be one of the mechanisms for identifying an adverse event has occurred or is about to occur. This then allows the system to preemptively prepare and respond. Your text indicates something along these lines, but the diagram appears contrary. Similarly, continuous adaptation is a threat agnostic self-	No

	defence mechanism in its own right (hence the area of 'moving target defence'). I wonder if this model is missing an assess/decide mechanism? Regardless of whether this model is conceived as a state machine or something more adaptive, some sort of situational assess/decide is necessary to make a conditional decision to transition states.	
R087	That diagram is OK, but it may be a bit simple. I don't see space resilience necessarily cycles as a simple linear state-driven process through all the taxonomic steps. For example, Survive/Sustain might feed straight back to Anticipate if there were hardening in the design sufficient to contain events with no impacts to recover from or no adaptation required – indeed these would seem to be desirable paths [demonstrating intrinsic resilience to events or action based on prior knowledge/design]. I suppose this also reflects my view of 'Anticipate' in that it encompasses prevention and avoidance, in addition to HILF detection. I presume that the feedback shown of Residual Impact is simply building the internal knowledge or depicting a resilience degradation [from the Residual Impact] – the reason for this feedback is not outwardly clear and is not articulated.	No
R088	Model too linear, and Adaption function should be earlier and/or in multiple stages of the lifecycle	No
R089	Refer to 'bow tie' comment above.	No
R090	What about for non-HILF events? What about "retaliate" or "defeat actor" after Adapt to eliminate the possibility of an attack.	No

Table 22 - Delphi Study Round 1 Question 4 Survey Responses

In summary, the expert consensus on the suitability of the definition posed in Round 1 Question 4 of the Delphi Study was 10 votes for yes and 13 votes for no, leading to a 43% consensus rate. This is an inadequate rate of consensus and so analysis was conducted to improve on the proposed definition based on the issues and suggestions raised by the expert respondents, as detailed in the following section.

4.1.2.1.4.2 Analysis

Each of the responses recorded at Table 22 were analysed before being grouped and summarised by theme. All respondents' suggestions have been taken into account regardless of whether the respondent agreed or disagreed with the proposed definition in the original question. Decision outcomes were then documented in the final column of Table 23 for those expert responses that prompted a change or addition to be made for the Delphi Round 2 survey.

ID	Summary and interpretation	Analysis and comments	Decisions
A068	The proposed space systems resilience model is adequate.	No analysis required.	No changes made.

A069	The model is too linear and does not account for variability in the phase sequencing.	Agree that the proposed model incorrectly implies a linear relationship between the timeline of a HILF event and the corresponding system resilience phase. Events can also occur concurrently.	1. Redesign resilience model to appear less linear.
A070	The proposed space systems resilience model is adequate.	No analysis required.	No changes made.
A071	The model is missing an aspect to retaliate or disable threats.	Although already addressed in the taxonomy and definition, any retaliatory (e.g. offensive security) aspect of a system (i.e. part of the 'Survive' or 'Sustain' function) could be made more explicitly clear in the model. By changing 'Anticipate' to 'Prevent' as documented at A064-1 in Table 21, the adaptation function would then become the default continuous state, with prevention being triggered by a known threat and survival being triggered by an attack. 'Sustain' would be the active state during an attack (post initial survival response) and recovery would be completed as soon as possible to return to continuous adaptation.	1. Modify model so that 'Adapt' is clearly portrayed as the central continuous function.
A072	The proposed space systems resilience model is adequate but it is unclear what it is trying to achieve.	The intent of the model is to functionally demonstrate how the resilience taxonomy works in practice.	No changes made.
A073	The model is too linear and does not account for black swan events.	The issue with the linearity of the proposed model is consistent with other expert responses and has been addressed as per A069 Decision 1.	No changes made.
A074	Confusion around 'Adapt' function and how post-incident learning and evolution is captured in the model.	System upgrades and informing of future designs would be an activity covered by the 'Adapt' phase of the cycle. The lack of clarity regarding the taxonomy usage is consistent with other expert responses and has been	No changes made.

		addressed as per A049 Decision 1 and A051 Decision 1.	
A075	Timing aspects are not covered by the model.	This concern is a function of the perceived linearity of the proposed model and is consistent with other expert responses, addressed as per A069 Decision 1.	No changes made.
A076	The proposed model is missing an assess or decide function to enable transitioning between states.	This concern is a function of the perceived linearity of the proposed model and is consistent with other expert responses, addressed as per A069 Decision 1.	No changes made.
A077	The proposed space systems resilience model is adequate.	No analysis required.	No changes made.
A078	Ensure the resilience model encompasses a failed state where the space system becomes space debris.	If the system cannot recover and becomes space debris then this would be part of the residual impact to the environment (arrow on left hand side of the proposed model).	No changes made.
A079	The proposed space systems resilience model is adequate.	No analysis required.	No changes made.
A080	The model is lacking a component for analysis to learn from previous incidents.	Incorporating 'lessons learned' after incident analysis is an activity that is already covered by the 'Adapt' phase of the cycle. However, the lack of clarity regarding the taxonomy usage is consistent with other expert responses and has been addressed as per A049 Decision 1 and A051 Decision 1.	No changes made.
A081	Issue with the exclusive focus on HILF events. Confusion surrounding taxonomical components.	The issue with specifying 'HILF' in the definition is consistent with other expert responses and has been addressed as per A057 Decision 1. The lack of clarity regarding the taxonomy usage is consistent with other expert responses and has been addressed as per A049 Decision 1 and A051 Decision 1.	No changes made.

A082	Ensure that adapting to the current threat environment is included in the model.	The 'Adapt' and 'Anticipate' functions help to adapt to the current threat environment. Adapt helps post-event (on the system in question) and Anticipate helps pre-event (based on threat intelligence regarding other events or near-misses on other space systems). The lack of clarity regarding the taxonomy usage is consistent with other expert responses and has been addressed as per A049 Decision 1 and A051 Decision 1.	No changes made.
A083	The proposed model seems to assume equal importance of each phase, which is not valid for HILF (e.g. adapt is less important for very rare events).	The issue with specifying 'HILF' in the definition is consistent with other expert responses and has been addressed as per A057 Decision 1. The concern regarding equal importance of phases is a function of the perceived linearity of the proposed model and has been addressed as per A069 Decision 1.	No changes made.
A084	The model is too linear to respond to continuously evolving space threats. The proposed model does not capture the difference in approach between a single space system versus a constellation system.	This concern is a function of the perceived linearity of the proposed model and is consistent with other expert responses, addressed as per A069 Decision 1. The model is intended to remain agnostic in its usage across different types of space systems. Hence, the model can apply to both single and constellation systems in the same manner, just at a differing scale and perhaps with differing mitigation methods – particularly in the governance segment.	No changes made.
A085	The proposed space systems resilience model is adequate. The taxonomy could be adequately communicated using various different models.	No analysis required.	No changes made.

A086	The proposed model is too linear and reactive to respond to continuously evolving space threats. The model is also missing an assess or decide function to enable transitioning between states. Issue with the exclusive focus on HILF events. Anticipate appears to be triggered by the HILF event when it should in fact be continuous.	The concern regarding the perceived linearity of the proposed model is consistent with other expert responses and has been addressed as per A069 Decision 1. The issue with specifying 'HILF' in the definition is consistent with other expert responses and has been addressed as per A057 Decision 1. The lack of a continuous improvement focus is consistent with other expert responses and has been addressed as per A071 Decision 1.	No changes made.
A087	The proposed model is too linear and reactive to respond to continuously evolving space threats. Prevention should have more emphasis in the model.	The concern regarding the perceived linearity of the proposed model is consistent with other expert responses and has been addressed as per A069 Decision 1. The concern regarding the lack of emphasis given to prevention is consistent with other expert responses and has been addressed as per A064 Decision 1.	No changes made.
A088	Confusion about the definition of 'Survive' versus 'Sustain'. Issue with similarity to NIST and alignment to the bow tie model, suggest providing further context.	The lack of clarity regarding the verbatim taxonomy usage and lack of clarity in the definition is consistent with other expert responses and has been addressed as per A049 Decision 1 and A051 Decision 1. The NIST (2018) cybersecurity framework is an input into this model and so is intended to be complementary. Future research may work to align this model with existing frameworks such as NIST.	No changes made.
A089	Issue with the exclusive focus on HILF events. There should be a phase to retaliate to or disable threats.	The issue with specifying 'HILF' in the definition is consistent with other expert responses and has been addressed as per A057 Decision 1.	No changes made.

		The concern regarding the lack of emphasis given to prevention (i.e., retaliating against or disabling threats) is consistent with other expert responses and has been addressed as per A064 Decision 1.	

Table 23 – Analysis of Delphi Study Round 1 Question 4 Survey Responses

In the analysis above there were a number of key themes that arose from the collective expert responses:

- Most respondents that answered 'no' to Question 4 of the survey indicated that the proposed model is too linear and so does not adequately capture the flexibility of approach required for resilience activities, as well as introduces interpretability issues.
- The 'Adapt' function should be represented to be more of a continuous approach.
- All other comments were related to the underlying definition or taxonomy and have been captured in the analysis of Question 3 in Section 4.1.2.1.3.2.

4.1.2.1.4.3 Outcomes

The table below captures a summary of the changes made based on the expert opinions:

Ref	Modifications
A069-1	Redesign resilience model to appear less linear.
A071-1	Modify model so that 'Adapt' is clearly portrayed as the central continuous function.

Table 24 - Summary of post-analysis changes to the Delphi Study Round 1 Question 4 proposal

Although only two changes were documented in response to the expert opinions provided for Question 4, a number of further changes were required based on the changes implemented to the underlying taxonomy and definition, as described in Table 21. Additionally, the two modifications recorded in Table 24 above represent significant changes and require the complete redesign of the model. As such the resulting modified model, as shown in Figure 27, appears vastly different to the originally proposed model, as shown at Figure 26.

4.1.2.2 Survey Round Two

After completing the Delphi Study Round 1 analysis and implementing changes based on the expert responses, as described in Section 4.1.2.1, a second round of surveys were sent out to the participants that responded to the Round 1 survey. This section recounts the responses

received in response to the survey as well as the ensuing analysis that identifies modifications or additions that were made to the originally proposed question.

A summary of all changes that were made as a result of the Delphi Study Round Two survey responses is provided in the table below for ease of reference. All original responses and justifications behind the stated modifications are detailed in the remainder of this section.

Ref	Modifications
Question 1 Outcomes	
A090-1	Replaced 'support' with 'enable' in the definition.
A091-1	‘People’ added to the definition.
A093-1	Replaced 'availability' with 'services' in the definition.
A096-1	Replaced 'integrity' with 'control' in the definition.
A108-1	Replaced 'ability to assure' with 'assurance of' in the definition.
Question 2 Outcomes	
A110-1	‘Honeypot/trap’ added to address cyber threats to the space segment.
A111-1	‘Identity and access management’ added to address cyber threats to the human segment.
A111-2	‘Facility Compartmentalisation’ added to address kinetic threats to the governance segment.
A111-3	‘Internal scanning’ added to address kinetic threats to the space segment.
A111-4	‘Directed Energy Weapons’ added to the electromagnetic adversities definition in the supporting table.
A111-5	Add ‘Data Preservation’ to the C3 Segment.
A113-1	Add ‘Human Segment’ to the knowledge domain.
A114-1	Add to threat table based on the counterspace continuum (Defense Intelligence Agency 2022).
A114-2	‘Mission Control’ added to the Ground Segment definition in the supporting table.
A115-1	Add Spectrum Regulation (e.g. ITU) to the knowledge domain.
A116-1	‘Dazzling/Blinding’ added to the electromagnetic threat description in the supporting table.
A120-1	Add supporting figure to communicate segmental interrelationships (see Figure 28).
A124-1	Change ‘threat’ to ‘adversities’
A124-2	Change ‘electronic’ to ‘electromagnetic’
A124-3	Add ‘protective security’ to address related kinetic threats to the governance segment.
A124-4	Add ‘LPI/LPD waveforms’ to the electromagnetic threat description in the supporting table.
A124-5	Add ‘Advanced signals processing’ and ‘signature management’ to address related electromagnetic threats to the C3 segment.
A126-1	Change ‘legal’ to ‘legal and regulatory’ to address related non-malicious threats to the governance segment.
A127-1	Add ‘quality and product assurance’ to address related non-malicious threats to the governance segment.

A129-1	Add ‘Spacecraft Hardening’ to address related kinetic threats to the space segment.
Question 3 Outcomes	
A140-1	Add ‘Anticipate’ to the taxonomy and definition.
A144-1	Reduce emphasis on continuous adaptation in the definition.
A145-1	Add the ability to operate in a degraded state to the definition.
A148-1	Develop a chart that demonstrates system function over time throughout the incident lifecycle with annotated taxonomical resilience phases.
Question 4 Outcomes	
A153-1	Add conditions for what must occur to transition between phases of the model.
A153-2	Modify resilience time graph (see A148-1) to demonstrate how each resilience phase aligns with system impact and annotate phase transition requirements.
A164-1	Rename ‘Prevent’ to ‘React’.
A164-2	Remove ‘Adapt’ from centre of diagram.

Table 25 - Summary of modifications based on Round 2 responses

The Delphi Study Round 2 questions are described in Section 3.3.2.4 and should be referenced when interpreting the below responses and analysis.

4.1.2.2.1 Question 1 – Space Systems Security Definition

The Delphi Study Round 1 survey sought to build on Moltz’s 2011 definition of the first dimension of space security, namely: “[Space systems security is] the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction”.

The question posed in the Delphi Study Round 2 survey was:
*The resulting definition based on your collective responses is: “**Space Systems Security is the ability to assure 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.**” Does this new definition adequately define Space Systems Security?*

4.1.2.2.1.1 Responses

Table 13 below provides the verbatim expert survey responses to Question 1 alongside a high-level yes or no assessment that summarises the respondents’ answer to the question as posed in the survey and summarised in Section 3.3.2.3.1. Note that spelling and grammatical errors have been included to avoid any inadvertent interference with the raw data.

The summary of response, analysis, and decision outcomes (i.e. changes made to the original definition) of each of the below responses are detailed in the following section.

ID	Response	Answer
R090	Yes. Although, consider update from "that support it" to "that enables it" - for improved alignment to "enabling system" term in systems engineering, covering ("its lifecycle" of) both acquisition and support.	Yes
R091	This definition will adequately define space systems security once the category of 'humans' or 'people' are suitably integrated as core components. I would propose that this might be achieved by inserting the word 'people' into the definition prior to the end of the sentence. I.e., "…including all ground communications, and space segments as well as the *people*, data processes, and supply chains that support it".	No
R092	Yes	Yes
R093	Whilst this is a reasonable / serviceable definitio of space system security, I think it could be improved by adding a focus on the protection of the services a space system provides. Space systems have value due to the services they provide to the terrestial users of the services rather than the space system has value in and of itself. Therefore, the security focus of a space system should be protection of the services it provides,since the orginal value / purpose of the space system is based on these services. Note that the term services includes communiucations, PNT services, ISR services, etc.	Yes
R094	Yes	Yes
R095	Yes	Yes
R096	The definition is reasonable. Personally, I would like to see more explicit emphasis on retaining positive "control" captured rather than rely on the implication coming from integrity/availability as is stated – but this is possibly just my preference. The other aspect I think is a bit awkward is that the words "…including all ground communications, and space segments…" does not really capture the full gambit of communications involved [terrestrial, ground station to/from satellite, and between satellites].	Yes
R097	Yes, the definition is good.	Yes
R098	Could include during design and testing	Yes
R099	Yes	Yes
R100	The definition still doesn't clearly cover 'full functionality and control'. what if you only lose a payload or subsystem? The terms 'integrity' and 'availability' are too ambiguous for me. What does an available spacecraft with integrity actually mean?	No
R101	Should the definition be expanded to include the protection from space systems as well as for space systems? Particularly in the sense that threats can come from space (other space systems) as well and from terra firma?	No
R102	I believe that it is a solid definition	Yes

R103	Yes.	Yes
R104	Definition seems to omit people. This means you have narrowed to just the technical aspects of the systems, rather than the full socio-technical system. Is this intentional? This means your subsequent consideration of resilience largely omits the human aspects, which can undermine or support system resilience.	No
R105	Yes	Yes
R106	Yes	Yes
R107	Yes, I think the definition is good.	Yes
R108	no = "Space Systems Security is the ability to assure..." it is not the "ability" to assure; it is the assurance... or the provision of…	No
R109	Yes	Yes

Table 26 - Delphi Study Round 2 Question 1 Survey Responses

In summary, the expert consensus on the suitability of the definition posed in Round 2 Question 1 of the Delphi Study was 15 votes for yes and 5 votes for no, leading to a 75% consensus rate. Although it could be argued that this rate of consensus is adequate, the expert responses provide yet additional opportunities to improve on the proposed definition. The analysis and outcomes regarding these improvements are detailed in the following section.

4.1.2.2.1.2 Analysis

Each of the responses recorded at Table 13 were analysed before being grouped and summarised by theme. All respondents' suggestions have been taken into account regardless of whether the respondent agreed or disagreed with the proposed definition in the original question. Decision outcomes were then documented in the final column of Table 14 for those expert responses that prompted a change or addition to be made for the Delphi Round 2 survey.

ID	Summary and interpretation	Analysis and comments	Decisions
A090	The proposed definition is adequate, however consider changing the phrase "that support it" to "that enables it" for improved alignment to systems engineering terminology.	Agree, suggested change has been implemented according to the respondent's proposal.	1. Replaced 'support' with 'enable' in the definition.
A091	The proposed definition will be adequate once the people aspect is added to it.	Agree, change to be made to insert the word 'people' into the definition prior to the end of the sentence, for example "…including all ground communications, and space segments	1. 'People' added to the definition.

		as well as the *people*, data processes, and supply chains that support it".	
A092	The proposed definition is adequate.	No analysis required.	No changes made.
A093	The proposed definition is adequate; however it could be improved with more emphasis on protecting the space system's services.	Agree, space hardware and software have no intrinsic value without the services that they are designed to provide. Although this is somewhat captured by the inclusion of 'availability' in the definition, perhaps availability is cybersecurity lingo where the meaning is not widely obvious to space professionals in general. In the context of space systems, availability is required insofar as the availability of services, hence the word 'availability' may reasonably be replaced with 'services'.	1. Replaced 'availability' with 'services' in the definition.
A094	The proposed definition is adequate.	No analysis required.	No changes made.
A095	The proposed definition is adequate.	No analysis required.	No changes made.
A096	The proposed definition is adequate; however 'integrity' is ambiguous in a space systems context and should be replaced with 'control'. Communications is not adequately captured in the definition.	Agree that 'integrity' is an ambiguous term to include in a definition such as this one. Perhaps integrity is cybersecurity lingo where the meaning is not widely obvious to space professionals in general. In the context of space systems, 'control' is a more useful term to include in the definition. The respondent's verbatim response at R096 indicates a potential misunderstanding of the word 'communications' to be 'ground communications. There is in fact a comma that separates 'ground' from 'communications' in the definition. As such, 'communications' is to be interpreted as encompassing all communications, including terrestrial,	1. Replaced 'integrity' with 'control' in the definition.

		ground station to/from space systems (i.e. satellites), and between space systems.	
A097	The proposed definition is adequate.	No analysis required.	No changes made.
A098	The proposed definition is adequate; however it could be improved with the inclusion of ‘during design and testing’.	Design and testing are already accounted for in the statement of “throughout its lifecycle”.	No changes made.
A099	The proposed definition is adequate.	No analysis required.	No changes made.
A100	The proposed definition is missing the ‘control’ aspect. The terms 'integrity' and 'availability' are too ambiguous.	The suggestion to include ‘control’ in the definition is consistent with other expert responses and has been addressed as per A096 Decision 1. The issue with the words ‘integrity’ and ‘availability’ is consistent with other expert responses and has been addressed as per A093 Decision 1 and A096 Decision 1.	No changes made, reinforces A093 Decision 1 and A096 Decision 1.
A101	The proposed definition is adequate; however it could be improved by referencing the protection from space threats as well as ground-based threats.	The definition must be threat agnostic and as such it must not explicitly define the threat. The threat could be another space system, asteroid, space junk, cyber-attack, or otherwise; all of these are valid under the current definition.	No changes made.
A102	The proposed definition is adequate.	No analysis required.	No changes made.
A103	The proposed definition is adequate.	No analysis required.	No changes made.
A104	The proposed definition will be adequate once the people aspect is added to it.	The observation that the definition currently omits ‘people’ is consistent with other expert responses and has been addressed as per A089 Decision 1.	No changes made, reinforces A089 Decision 1.
A105	The proposed definition is adequate.	No analysis required.	No changes made.
A106	The proposed definition is adequate.	No analysis required.	No changes made.
A107	The proposed definition is adequate.	No analysis required.	No changes made.
A108	Space systems security is not “the ability to assure”, it is rather “the assurance of”.	Agree, the wording should be made to read as per the respondent’s suggestion at R108.	1. Replaced 'ability to assure' with 'assurance of' in the definition.
A109	The proposed definition is adequate.	No analysis required.	No changes made.

Table 27 – Analysis of Delphi Study Round 2 Question 1 Survey Responses

In the analysis above there were a number of key themes that arose from the collective expert responses:

- ‘Control’ is missing from the definition
- ‘Services’ is missing from the definition
- ‘People’ is missing from the definition
- The terms ‘integrity’ and ‘availability’ are ambiguous.

4.1.2.2.1.3 Outcomes

The table below captures a summary of the changes made based on the expert opinions:

Ref	Modifications
A090-1	Replaced 'support' with 'enable' in the definition.
A091-1	‘People’ added to the definition.
A093-1	Replaced 'availability' with 'services' in the definition.
A096-1	Replaced 'integrity' with 'control' in the definition.
A108-1	Replaced 'ability to assure' with 'assurance of' in the definition.

Table 28 - Summary of post-analysis changes to the Delphi Study Round 2 Question 1 proposal

4.1.2.2.2 Question 2 – Space Systems Security Domain

The second question in the expert survey attempts to define the scope of the space systems security knowledge domain. The revised model of the knowledge domain, as shown in Table 4, was provided to the expert respondents as per section 3.3.2.4.2, to which the respondents stated whether they believed anything was missing or inaccurate.

The question posed was: *Does this new table adequately cover the important high-level disciplines that are required to effectively protect the confidentiality, integrity, and availability of space systems?*

4.1.2.2.2.1 Responses

Table 29 below provides the verbatim expert survey responses to Question 2 alongside a high-level yes or no assessment that summarises the respondents’ answer to the question as posed in the survey and summarised in Section 3.3.2.4.2. Note that spelling and grammatical errors have been included to avoid any inadvertent interference with the raw data.

The summary of response, analysis, and decision outcomes (i.e. changes made to the original knowledge domain table) of each of the below responses are detailed in the following section.

ID	Response	Answer
R110	Yes. Although, consider including "Vulnerability Management" to address Cyber threats in Governance Segment; and "Honeypot/trap" to address Cyber threats in Ground Space and C3 Segments.	Yes
R111	Governance Segment & Cyber: “Access Management” must delineate and include both identity and access management. This will also further clarify this section’s controls for social engineering attacks. Governance Segment & Electronic: Protection from electronic threats in this domain could also be extended to include facility compartmentalization (physical air gaps), the use of backups (offsite). Ground Segment & Cyber: Protection from cyber threats should also explicitly accommodate for insider threats and social engineering – I would recommend including reference to ‘access management’ in the extended format previously suggested: “Access Management” must delineate and include both identity and access management. This will also further clarify this section’s controls for social engineering attacks. Space Segment & Kinetic: To this I would suggest including defensive infrastructure designed to protect against damage caused by failures to a space systems kinetic threat countermeasure systems caused by corruption or tampering by a malicious actor. This could be controlled by running regular system scans, tests, and performing other activities that have previously been referred to as “cyber assurance testing”. C3 Segment & Electronic: Also requires physical hardening specifically suitable for resisting, deflecting and/or absorbing DEWs. Additionally, the asset should be able to scan its internal systems and exterior for transmitters or receivers that are not native to the space asset (i.e., malicious EW equipment). Last, an EW countermeasure suite dedicated to the protection of the C3 segment would be ideal. C3 Segment & Kinetic: Consider including kinetic threat countermeasures such as reactive armor.	No
R112	Yes	Yes
R113	In general, this is a good breakdown / coverage of space systems security domain. There are two areas that should be considered for the structing of the table. The first is the threat categorisation should be aligned with the categorisation used by the CSIS. The second is that it may be worth treating the users / user terminals has a seprate segment to the ground segment.	Yes
R114	Maybe, yet I would add more fields. C3 should be C5ISR. And look at the space systems continnum attached in my reply, page 3..	No
R115	No - Governance should include regulatory (ITU) aspects. The concept of competitive space comes from scarcity of spectrum and how the international community competes for access to space	No

R116	I think that the refinement is pretty good. There could be some further refinement of the cell description details but that would be minor. One thing that you might want to consider is widening the "Kinetic" Threat Type to instead use "Energy" - that would capture things like Laser/Maser attacks in addition to the narrower view of Kinetic (physical) energy and also capture things like sensor dazzling/blinding that can be seen to be somewhat abstracted from "Electronic". This last point is possibly more pertinant to military applications than others.	Yes
R117	Yes, at a high-level.	Yes
R118	Yes	Yes
R119	Yes	Yes
R120	Software is now in C3. Does that mean the ground and space segments are only hardware?	Yes
R121	Where does human factors fit in? Or is it assumed? I see there is cyber training under cyber, but what about human error?	Yes
R122	Not sold on the term "non-malicious threats", but cant quite think of a term that suitably groups this thread	Yes
R123	Yes.	Yes
R124	Seems to conflate faults, hazards, threats and vulnerabilities – calling all of these things threats. Other resilient systems literature makes the distinction between adverse events and adverse conditions, and collectively refers to these as ‘adversities’. I tend to think this is a better word than ‘threats’, and avoids overloading the meaning of ‘threat’. • It is unclear if the C3 segment only relates to the space vehicle, or if it also relates to the computers/comms/etc of the ground segment. • Omits the threat category of human Influence, which has the potential to impact all segments. Presumably this omission flows from the narrow definition, as discussed in question 1. • 'Electronic threats' would be better named ‘Electromagnetic threats’ for consistency with more recent US and Australian military terminology. I.e. EW is now ‘Electromagnetic Warfare’, rather than the old ‘Electronic Warfare’. • Business Continuity Management/Planning should be included, relevant to all threat categories. • For kinetic threats against governance – physical security is relevant (e.g. to protect R&D and supply chain from theft, espionage, insiders) • For electromagnetic threats against C3 – LPI/LPD waveforms, anti-jam, advanced signals processing, signature management are additional domains that are relevant	No
R125	Yes	Yes
R126	Government policy is not covered by the table. I think it sits alongside legal (which I assume also includes regulatory)	Yes
R127	I think that as long as 'reliability engineering' is broadly enough defined to include quality assurance and product assurance.	Yes
R128	Yes	Yes
R129	"For the Ground Segment, Non-Malicious Threat, you state “Protecting ground components from non-malicious threats through Debris / Celestial Monitoring and Reliability Engineering (Telecomm, Software, Aerospace, ICT)”. I’m not sure what debris means in this context e.g. are you meaning dust storms, cyclone debris, etc? I would have thought	Yes

	debris and probably celestial monitoring is more important for the space components as that is where one of the biggest threat lies i.e. space junk. Also a key non-malicious threat in space is radiation/high energy particles which is more than 'just' materials, it is hardening and spacecraft design. Does counterspace include manoeuvre?	

Table 29 - Delphi Study Round 2 Question 2 Survey Responses

In summary, the expert consensus on the suitability of the definition posed in Round 2 Question 2 of the Delphi Study was 16 votes for yes and 4 votes for no, leading to a 80% consensus rate. Although it could be argued that this rate of consensus is adequate, the expert responses provide yet additional opportunities to improve on the proposed definition. The analysis and outcomes regarding these improvements are detailed in the following section.

4.1.2.2.2.2 Analysis

Each of the responses recorded at Table 29 were analysed before being grouped and summarised by theme. All respondents' suggestions have been taken into account regardless of whether the respondent agreed or disagreed with the proposed definition in the original question. Decision outcomes were then documented in the final column of Table 30 for those expert responses that prompted a change or addition to be made for the Delphi Round 3 survey.

ID	Summary and interpretation	Analysis and comments	Decisions
A110	The proposed knowledge domain is adequate, however suggest to include 'vulnerability management' to address Cyber threats in Governance Segment. Add "honeypot/trap" to address Cyber threats in Ground, Space, and C3 Segments.	Vulnerability management is covered under 'Cyber Assurance/Testing'. Honeypot/trap added to space segment, not as relevant to ground and C3 because active monitoring can take place instead. This is more of a specific tactic rather than a discipline or area of security.	1. 'Honeypot/trap' added to address cyber threats to the space segment.
A111	Recommend adding the following to the knowledge domain: access management, facility compartmentalisation, backup procedures, personnel vetting, internal scanning, and directed-energy weapons (DEW).	Agree that the following should be explicitly represented in the knowledge domain: access management, facility compartmentalisation, personnel vetting, internal scanning, and directed-energy weapons (DEW). Backup procedures relate to a	1. 'Identity and access management' added to address cyber threats to the human segment. 2. 'Facility Compartmentalisation' added to address

		specific risk-mitigating control and would be better captured as 'Data Preservation' for the purposes of the knowledge domain.	kinetic threats to the governance segment. 3. 'Internal scanning' added to address kinetic threats to the space segment. 4. 'Directed Energy Weapons' added to the electromagnetic adversities definition in the supporting table. 5. Add 'Data Preservation' to the C3 Segment.
A112	The proposed knowledge domain is adequate.	No analysis required.	No changes made.
A113	The proposed knowledge domain is adequate; however the threat categorisation should align to the original CSIS threat categories. The users should be considered separate to the ground segment.	This respondent appears to make a similar suggestion to what was raised at R035 in Round 1 of the Delphi Study. This concern has been addressed at A035, in that the CSIS space threat taxonomy achieves a different objective than what is trying to be achieved by this space systems security knowledge domain. Agree that users should be given distinct emphasis in the knowledge domain, especially given the fact that a large proportion of cyber incidents have a root cause that can be traced back to humans. Additionally, there are specific human challenges that should be explicitly considered as the industry progresses towards further human space travel innovations and business drivers.	1. Add 'Human Segment' to the knowledge domain.
A114	The proposed knowledge domain is adequate, however C3 should be	Intelligence, surveillance, and reconnaissance (ISR) is more of an	1. Add to threat table based on the space

	C5ISR. The attached space systems continuum (Defense Intelligence Agency 2022) provides further discourse on space systems technologies and fields.	activity than a system segment, with a lot of those activities falling across various cells in the knowledge domain table. Of the 'C5' three are already covered, the other two are: 'Command' and 'Cyber'. Cyber is already covered across the cyber row. Command is not a threat vector, but it has not been covered in the table and should be. One aspect of Command, Personnel, is covered by Governance segment. Mission Control should be added to the Ground Segment definition.	continuum (Defense Intelligence Agency 2022). 2. 'Mission Control' added to the Ground Segment definition in the supporting table.
A115	Governance should include regulatory (ITU) aspects.	Agree, spectrum regulation should be explicitly identified in the knowledge domain table.	1. Add Spectrum Regulation (e.g. ITU) to the knowledge domain.
A116	The proposed knowledge domain is adequate, however suggest to change 'kinetic' to 'energy'.	Energy and light attacks would now be considered under the Electromagnetic category as per the changes documented at A124 Decision 2. However agree that it is worth adding some energy attack examples to the supporting definition table.	1. 'Dazzling/Blinding' added to the electromagnetic threat description in the supporting table.
A117	The proposed knowledge domain is adequate.	No analysis required.	No changes made.
A118	The proposed knowledge domain is adequate.	No analysis required.	No changes made.
A119	The proposed knowledge domain is adequate.	No analysis required.	No changes made.
A120	Respondent demonstrated some confusion regarding the addition of the C3 segment and its intent.	The C3 segment is intended to interact across all other segments in the space systems security knowledge domain. The confusion can be clarified with a diagram that demonstrates the interrelationship of each segment in the knowledge domain.	1. Add supporting figure to communicate segmental interrelationships (see Figure 28).

A121	The proposed knowledge domain is adequate, however the human factors should be more explicitly mentioned.	The suggestion to make human factors more prominent in the knowledge domain is consistent with other expert responses and has been addressed as per A113 Decision 1.	No changes made.
A122	The proposed knowledge domain is adequate, however 'Non-Malicious' terminology could be improved.	Agree that the term 'non-malicious' could be modified or improved however no alternate wording is provided consistently in the literature and no other words have been proven to be more appropriate.	No changes made.
A123	The proposed knowledge domain is adequate.	No analysis required.	No changes made.
A124	Suggest to make the following changes: change 'threat' to 'adversities', clarify how the C3 segment relates to the others, make human influence more prominent, change 'electronic' to 'electromagnetic', add physical security to Governance Kinetic. Add the following to the knowledge domain: LPI/LPD waveforms, anti-jamming, advanced signals processing, and signature management to electromagnetic threats against C3.	Agree with all proposed changes and additions at R124, except for the suggestion to include anti-jamming as this is already covered by LPI/LPD waveforms and ECM. The suggestion to make human influence more prominent in the knowledge domain is consistent with other expert responses and has been addressed as per A113 Decision 1. The request for further clarification on segmental interrelationships within the proposed knowledge domain is consistent with other expert responses and has been addressed as per A120 Decision 1.	1. Change 'threat' to 'adversities' 2. Change 'electronic' to 'electromagnetic' 3. Add 'protective security' to address related kinetic threats to the governance segment. 4. Add 'LPI/LPD waveforms' to the electromagnetic threat description in the supporting table. 5. Add 'Advanced signals processing' and 'signature management' to address related electromagnetic threats to the C3 segment.
A125	The proposed knowledge domain is adequate.	No analysis required.	No changes made.
A126	Government policy is not covered by the knowledge domain table.	Government policy is account for under 'legal compliance' in the cells	1. Change 'legal' to 'legal and regulatory'

		that addresses non-malicious threats to the governance segment. For clarity this can be expanded to include 'legal and regulatory compliance'.	to address related non-malicious threats to the governance segment.
A127	The proposed knowledge domain is adequate as long as 'reliability engineering' includes quality assurance and product assurance.	Agree that quality and product assurance should be addressed in the knowledge domain.	1. Add 'quality and product assurance' to address related non-malicious threats to the governance segment.
A128	The proposed knowledge domain is adequate.	No analysis required.	No changes made.
A129	Radiation / high energy particles is a non-malicious threat that requires hardening and spacecraft design.	Agree that spacecraft design and hardening should be addressed in the knowledge domain.	1. Add 'Spacecraft Hardening' to address related kinetic threats to the space segment.

Table 30 – Analysis of Delphi Study Round 2 Question 2 Survey Responses

In the analysis above there were a number of key themes that arose from the collective expert responses:

- The knowledge domain does not adequately emphasise the human aspects of space systems security
- The interrelationship of segments in the knowledge domain should be explained as part of the model
- 'Electronic' threat is outdated terminology and should be updated to be 'Electromagnetic'.

4.1.2.2.2.3 Outcomes

The table below captures a summary of the changes made based on the expert opinions:

Ref	Modifications
A110-1	'Honeypot/trap' added to address cyber threats to the space segment.
A111-1	'Identity and access management' added to address cyber threats to the human segment.
A111-2	'Facility Compartmentalisation' added to address kinetic threats to the governance segment.
A111-3	'Internal scanning' added to address kinetic threats to the space segment.
A111-4	'Directed Energy Weapons' added to the electromagnetic adversities definition in the supporting table.
A111-5	Add 'Data Preservation' to the C3 Segment.

A113-1	Add ‘Human Segment’ to the knowledge domain.
A114-1	Add to threat table based on the counterspace continuum (Defense Intelligence Agency 2022).
A114-2	‘Mission Control’ added to the Ground Segment definition in the supporting table.
A115-1	Add Spectrum Regulation (e.g. ITU) to the knowledge domain.
A116-1	‘Dazzling/Blinding’ added to the electromagnetic threat description in the supporting table.
A120-1	Add supporting figure to communicate segmental interrelationships (see Figure 28).
A124-1	Change ‘threat’ to ‘adversities’
A124-2	Change ‘electronic’ to ‘electromagnetic’
A124-3	Add ‘protective security’ to address related kinetic threats to the governance segment.
A124-4	Add ‘LPI/LPD waveforms’ to the electromagnetic threat description in the supporting table.
A124-5	Add ‘Advanced signals processing’ and ‘signature management’ to address related electromagnetic threats to the C3 segment.
A126-1	Change ‘legal’ to ‘legal and regulatory’ to address related non-malicious threats to the governance segment.
A127-1	Add ‘quality and product assurance’ to address related non-malicious threats to the governance segment.
A129-1	Add ‘Spacecraft Hardening’ to address related kinetic threats to the space segment.

Table 31 - Summary of post-analysis changes to the Delphi Study Round 2 Question 2 proposal

4.1.2.2.3 Question 3 – Space Systems Resilience Definition and Taxonomy

The third question in the survey sent to the two dozen space security experts attempted to build a contemporary taxonomy and definition for space systems resilience. The definition and taxonomy utilised for the second round of the Delphi study is as described in Section 3.3.2.4.3.

The question posed was: *Does the modified definition adequately define Space Systems Resilience?*

4.1.2.2.3.1 Responses

Table 32 below provides the verbatim expert survey responses to Question 3 alongside a high-level yes or no assessment that summarises the respondents’ answer to the question as posed in the survey and summarised in Section 3.3.2.3.3. Note that spelling and grammatical errors have been included to avoid any inadvertent interference with the raw data.

The summary of response, analysis, and decision outcomes (i.e. changes made to the original knowledge domain table) of each of the below responses are detailed in the following section.

ID	Response	Answer
R130	Yes. Refer to response to item 2: "Vulnerability Management" linked to Adapt, and "Honeypot/trap" linked to Prevent.	Yes
R131	I argue that this new definition adequately defines Space Systems Resilience.	Yes
R132	Yes	Yes
R133	I think this is an acceptable / useable definition. Note that it is different to the "Space Domain Mission Assurance: A Resilience Taxonomy" issuesd by US DoD, but not markedly so. This as been referenced in a current programs.	Yes
R134	Yes	Yes
R135	Yes	Yes
R136	This is a pretty good higher-echelon definition… though it could be argued that a significant resilience contribution is achievable with just Prevention, Survival, Sustainment and Recovery aspects - without continuous evolution with Adaptation. Of course, adaptation is needed to capture the unanticipated/HILF-type threats but most threats would not fall into this category. As worded, the definition is possibly giving too much emphasis on "..to continuously adapt in order to…" when many responses to real run-of-the-mill threats really do not need to rely on this.	Yes
R137	Yes, it does.	Yes
R138	yes	Yes
R139	Yes	Yes
R140	This is good. But what is still missing for me here, and is hidden in Adapt, is the necessity to 'detect' and have 'intelligence' that you are under threat. I think this is a necessary piece to be resilient by ultimately adapting and recovering	No
R141	I am comfortable with this definition	Yes
R142	Does 'services' cover the human element?	Yes
R143	Yes.	Yes
R144	The 5 taxonomical aspects are okish. I tend to think that 'resilience' and 'adaptation' are subtly different things. Use of the term 'prevent' is slightly problematic, especially if it is considered to include 'avoid'. Avoiding a threat/adversity doesn't make a system more resilient, it simply decreases the need for resilience. • The subsequent definition of space system resilience is inaccurate. The definition implies that prevent, survive, recover and sustain are the result of continuously adapting. However, a system can have resilience even in the absence of adaptation, and adaptation does not necessarily lead to a more resilient system. • Suggest the following rewording "Space systems resilience is the ability of a space system, including its services, sub-components, and supporting functions to prevent, survive, recover, and adapt to adversities, whilst sustaining its core capabilities".	No
R145	No - survive, sustain, recover phases need to explicitly mention operation in a degraded state potentionally at the expense of some capability/services	No
R146	You may wish to consider including the word 'improve' in Adapt	Yes

R147	Yes	Yes
R148	yes but Sustain and Survive are essentially the same thing	Yes
R149	There's a significant difference in resilience depending on what your space system is? For example if you have a single, exquisite satellite as your space system then the resilience for this is different to a constellation of smaller satellites that may be less capable for each individual satellite but work together to provide a space system that is perhaps "inherently" more resilient. However I think your taxonomy is valid for both cases – but note the following Q4 comment.	No

Table 32 - Delphi Study Round 2 Question 3 Survey Responses

In summary, the expert consensus on the suitability of the definition posed in Round 2 Question 3 of the Delphi Study was 16 votes for yes and 4 votes for no, leading to a 80% consensus rate. Although it could be argued that this rate of consensus is adequate, the expert responses provide yet additional opportunities to improve on the proposed definition. The analysis and outcomes regarding these improvements are detailed in the following section.

4.1.2.2.3.2 Analysis

Each of the responses recorded at Table 32 were analysed before being grouped and summarised by theme. All respondents' suggestions have been taken into account regardless of whether the respondent agreed or disagreed with the proposed definition in the original question. Decision outcomes were then documented in the final column of Table 33 for those expert responses that prompted a change or addition to be made for the Delphi Round 3 survey.

ID	Summary and interpretation	Analysis and comments	Decisions
A130	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A131	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A132	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A133	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A134	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A135	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.

A136	The definition is possibly giving too much emphasis on "..to continuously adapt in order to…" when many responses to real run-of-the-mill threats really do not need to rely on this.	The continuous adaptation component of resilience is crucial to remain resilient over time, with 'continuous' needed in order to combat constantly evolving cyber threats. This is the function where something like Threat Intelligence would sit.	No changes made.
A137	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A138	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A139	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A140	Detection is hidden under 'Adapt' and requires greater emphasis in the taxonomy and definition.	One outcome of the Delphi Study Round 1 analysis was to change 'Anticipate' to 'Prevent' (see A064-1), however in doing so the fundamental requirement to monitor and detect threats and aversities lost its prevalence. The first approach to address this issue was to introduce extra wording around monitoring and detecting threats in the taxonomical category definitions. However after completing analysis it was discovered that the lack of monitoring and detecting was a commonly raised concern and as such 'Anticipate' was added back into the taxonomy, albeit as an addition to 'Prevent'. So, in essence, the prevention aspects of the initially proposed 'Anticipate' function of resilience have now been separated out into their own separate function.	1. Add 'Anticipate' to the taxonomy and definition.
A141	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A142	Does 'services' cover the human element?	No, 'supporting functions' encompasses human element.	No changes made.

A143	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.
A144	'Adapt' not a function of resilience. 'Prevent' should not include 'avoid'. Avoiding a threat is not 'resilience', it simply reduces the need for resilience.	Although adaptation and resiliency are indeed two differing concepts, an increase in a system's adaptive capabilities will in fact improve its resiliency. As such, even though the respondent's statement is true, it does not negate the need to include 'Adapt' as a core feature of space systems resilience. However, given this confusion and those from prior responses, it is pragmatic to slightly revise the definition to reduce emphasis on 'continuous adaptation'. Possessing the inherent ability to actively reduce your need for resilience in response to identified threats is still a resilience enhancing feature. For, without it, the system may experience more adverse events, ultimately impacting resiliency and delivery of core functionality.	1. Reduce emphasis on continuous adaptation in the definition.
A145	The definition and taxonomy should explicitly mention operation in a degraded state.	'Survive' is the function that describes operating in a degraded state. Agree however that this is obvious in the taxonomy but not clear in the definition. Definition to be updated.	1. Add the ability to operate in a degraded state to the definition.
A146	The proposed taxonomy and definition are adequate, however consider including the word 'improve' in the 'Adapt' function of the taxonomy.	Adapt is defined as "the system's mechanisms in place to continuously evolve based on threat events and intelligence to increase resilience to threats." This definition includes the phrase 'continuously evolve', which implies continuous improvement. No change is required.	No changes made.
A147	The proposed taxonomy and definition are adequate.	No analysis required.	No changes made.

A148	Confusion about the definition of 'Survive' versus 'Sustain'.	The lack of clarity regarding the definition of 'Survive' versus 'Sustain' was raised in Round 1 under responses R049 and R051. There are very distinct differences between the 'Survive' and 'Sustain' functions, however it appears this is still not clear in the provided materials. The distinction between the two is most apparent when demonstrated in a time sequence that clearly distinguishes between the reactionary 'Survive' phase, which is concerned with immediate incident response / triage, and the 'Sustain' phase, which is focused on maintaining operations in a degraded state.	1. Develop a chart that demonstrates system function over time throughout the incident lifecycle with annotated taxonomical resilience phases.
A149	Awareness should be considered as a function in its own right and not effectively part of 'Prevent'.	The suggestion to increase the importance of awareness in the taxonomy and resulting definition is consistent with other expert responses and has been addressed as per A140 Decision 1.	No changes made, reinforces A140 Decision 1.

Table 33 – Analysis of Delphi Study Round 2 Question 3 Survey Responses

In the analysis above each response was more or less unique, with most responses not requesting any changes. The only repeat theme that arose from the expert responses was that awareness should be considered as a function in its own right and not effectively part of 'Prevent'. This response is particularly interesting as an outcome of the Delphi Study Round 1 analysis was to change 'Anticipate' to 'Prevent' (see A064-1), however in doing so the fundamental requirement to monitor and detect threats and aversities seems to have lost its prevalence. The approach to address this issue was to add 'Anticipate' back into the taxonomy, but this time as an addition to 'Prevent'. So, in essence, the prevention aspects of the initially proposed 'Anticipate' function of resilience have now been separated out into their own separate function. In this way, although this round of responses indicates a required emphasis on awareness, detection, and general anticipation of threats and adverse events (i.e. 'Anticipate'), taking into consideration past responses the actual functionality that was

originally missing was the ‘Prevent’ function. This make sense in the context of the original taxonomy usage being developed for electric grids rather than space systems, where prevention is less of an option than on a spacecraft.

4.1.2.2.3.3 Outcomes

The table below captures a summary of the changes made based on the expert opinions:

Ref	Modifications
A140-1	Add ‘Anticipate’ to the taxonomy and definition.
A144-1	Reduce emphasis on continuous adaptation in the definition.
A145-1	Add the ability to operate in a degraded state to the definition.
A148-1	Develop a chart that demonstrates system function over time throughout the incident lifecycle with annotated taxonomical resilience phases.

Table 34 - Summary of post-analysis changes to the Delphi Study Round 2 Question 3 proposal

4.1.2.2.4 Question 4 – Space Systems Resilience Model

The fourth and final question in the Round 2 survey presented a representative model of space systems resilience, built on the taxonomy defined in the previous subsection. The model presented to the expert respondents for the second round of the Delphi study is as described in Section 3.3.2.4.4.

The question posed was: *Does this new model adequately represent the Space Systems Resilience cycle?*

4.1.2.2.4.1 Responses

Table 35 below provides the verbatim expert survey responses to Question 4 alongside a high-level yes or no assessment that summarises the respondents’ answer to the question as posed in the survey and summarised above. Note that spelling and grammatical errors have been included to avoid any inadvertent interference with the raw data.

The summary of response, analysis, and decision outcomes (i.e. changes made to the original knowledge domain table) of each of the below responses are detailed in the following section.

ID	Response	Answer
R150	Yes. Although, consider rotate diagram left by 45 degree for a tear-shaped outline with "Threat Event" at the top. Somehow it seems aligned to "bowtie" risk management methodology.	Yes

R151	I argue that this new model adequately represents the Space Systems Resilience cycle.	Yes
R152	Yes	Yes
R153	I think this is OK in terms of the topology. I think a more detailed desciption of the types of transitions that occur to move between the different nodes in the diagram. I.e. not aal arrows in the diagram are the same or mean the smae types of actions.	Yes
R154	The threat box should be between Sustain and Recover. I would lable the whole OODA Loop as "Space Systems Recilience Threat Event" and then change the box to "Incident."	No
R155	This diagram is not that clear as to how you transition between entities - is this supposed to be a state diagram? It might be better represented as a state diagram showing how the system moves between states in response to a known or unknown threat	No
R156	I think the model depiction has been improved quite a bit, and I like it. "Threat Event" might be better pluralised to “Threat Event/s”, or perhaps depicted with a small cascade of overlying events. Possibly the outer arrows should be larger in width than the inner arrows to/from Adapt – that I do not see this as a particular weakness.	Yes
R157	Yes, it does.	Yes
R158	yes	Yes
R159	Yes	Yes
R160	what is the arrow from prevent to threat event represent? as above, it doesnt capture any information/knowledge/sensing of the threat	No
R161	This model is OK, although it assumes the threats are always external. Mistakes during any one of these facets pose a threat in and of themselves (and not only from insider threats)	Yes
R162	Not convinced yet. I've been working to a model provided by DNV GL in which resilience is defined as the systems ability to respond and recover following a successful attack.	No
R163	Yes.	Yes
R164	To my mind, sustaining the core capabilities is the outcome of system resilience, rather than a discrete state in a process model. • Prevent is where the taxonomical description (slide 4) includes the detect function. Logically detection can only follow occurrence of an adverse event. However Prevent also includes the avoid and deter functions, which are relevant when a threat is known but an adverse event has not yet occurred. Thus it is ambiguous where Prevent should be placed in the process model, which would suggest this taxonomical grouping is wrong. Perhaps Detect should be standalone, not part of Prevent. • Adapt is different to the others. In effect it produces changes to each of the other processes, rather than being a resilience control that is applied in the process of returning a system to normal operations. The relationship should be shown differently in the diagram, otherwise it confuses things.	No
R165	Yes	Yes
R166	Yes	Yes
R167	Yes	Yes
R168	yes but Sustain and Survive are essentially the same thing	Yes

R169	I'm not sure that the model work for me, and perhaps this goes back to the taxonomy? I think the fundamental requirement for resilience is "awareness" of the environment, the threat, the ability to sense and characterise, etc. If we do not have this then all the other elements of the taxonomy breakdown i.e. you can't prevent, adapt, survive, etc. . I think that it is worthwhile considering awareness as a function in its own right and not effectively part of prevent.	No

Table 35 - Delphi Study Round 2 Question 4 Survey Responses

In summary, the expert consensus on the suitability of the definition posed in Round 2 Question 4 of the Delphi Study was 14 votes for yes and 6 votes for no, leading to a 70% consensus rate. This is an inadequate rate of consensus and so analysis was conducted to improve on the proposed model based on the issues and suggestions raised by the expert respondents, as detailed in the following section.

4.1.2.2.4.2 Analysis

Each of the responses recorded at Table 35 were analysed before being grouped and summarised by theme. All respondents' suggestions have been taken into account regardless of whether the respondent agreed or disagreed with the proposed model in the original question. Decision outcomes were then documented in the final column of Table 36 for those expert responses that prompted a change or addition to be made for the Delphi Round 3 survey.

ID	Summary and interpretation	Analysis and comments	Decisions
A150	The proposed model is adequate, however consider centring the model around the 'Threat Event'.	In order to address other feedback in the below responses, the model was modified to the point that this comment was no longer applicable.	No changes made.
A151	The proposed model is adequate.	No analysis required.	No changes made.
A152	The proposed model is adequate.	No analysis required.	No changes made.
A153	The proposed model is adequate, however consider describing what must occur to transition between states.	This is a common response to this question in the survey. Although not intended as a state diagram, the model should indeed describe what must occur to transition between states.	1. Add conditions for what must occur to transition between phases of the model. 2. Modify resilience time graph (see A148-1) to demonstrate how each resilience

			phase aligns with system impact and annotate phase transition requirements.
A154	The ‘Threat Event’ should occur between ‘Sustain’ and ‘Recover’.	This comment arises from a misunderstanding of the resilience taxonomy. The resilience taxonomy should be separated out of Question 3 and listed as a separate (fifth) outcome of this research to make its intention clear. For the third round, the time function graph developed as a result of outcome A148 Decision 1 will help clarify how each phase is represented against the lifecycle of an adverse event, such as a cybersecurity incident. It would not make sense for the incident to occur after the Sustain phase because the Sustain phase is itself triggered by an incident and involves maintaining critical operations at a reduced capacity.	No changes made.
A155	The proposed model should describe what must occur to transition between phases.	The suggestion to add phase transition conditions to the model is consistent with other expert responses and has been addressed as per A153 Decision 1 and 2.	No changes made, reinforces A153 Decision 1 and 2.
A156	The proposed model is adequate.	No analysis required.	No changes made.
A157	The proposed model is adequate.	No analysis required.	No changes made.
A158	The proposed model is adequate.	No analysis required.	No changes made.
A159	The proposed model is adequate.	No analysis required.	No changes made.
A160	The proposed model should describe what must occur to transition between phases. The model does not capture sensing of the threat.	The suggestion to add phase transition conditions to the model is consistent with other expert responses and has been addressed as per A153 Decision 1 and 2. The lack of system anticipation of threats is addressed in the taxonomical analysis of Question 3	No changes made, reinforces A153 Decision 1 and 2 and A140 Decision 1.

		responses and the outcome is recorded at A140 Decision 1.	
A161	The model assumes threats are external.	This is not correct. The 'Threat Event' in the model may be an insider or other internal threat. The proposed model is designed to apply to both internal and external threats and adversities.	No changes made.
A162	The proposed model does not align to the respondent's organisation's internal processes. No improvement suggestions were offered.	No analysis required.	No changes made.
A163	The proposed model is adequate.	No analysis required.	No changes made.
A164	Sustaining the core capabilities of a space system is the outcome of system resilience rather than a discrete phase. The 'Prevent' phase of the taxonomy is problematic as it contains functions that occur both before and after an adverse event occurs (i.e. detect versus deter/avoid). Suggest make 'Detect' a standalone function in the taxonomy and not part of 'Prevent'. 'Adapt' should be shown differently in the diagram.	'Sustain' refers specifically to the ability to sustain services and operations *in a degraded state.* This has been made more explicit in the third round of the Delphi Study by way of changes made at A145 Decision 1. The observation that 'Prevent' occurs both before and after the 'Threat Event' in the model is astute and does in fact indicate an issue with the taxonomy. This point also intersects with the responses to Question 3 that indicate a lack of system awareness in the taxonomy, resulting in 'Anticipate' being reintroduced into the taxonomy at A140 Decision 1. Although the reintroduction of 'Anticipate' addresses the primary concern of this response, the word 'Prevent' could be renamed to 'React' to make this relationship clearer. The suggestion to include 'Detect' as a separate taxonomical function is address in A140 Decision 1, where 'Anticipate' fulfils the	1. Rename 'Prevent' to 'React'. 2. Remove 'Adapt' from centre of diagram.

		function of scanning and threat detection. Agree that centring 'Adapt' in the model can place an unintended focus on that one function over the others. This concern is congruent with that in R136.	
A165	The proposed model is adequate.	No analysis required.	No changes made.
A166	The proposed model is adequate.	No analysis required.	No changes made.
A167	The proposed model is adequate.	No analysis required.	No changes made.
A168	Confusion about the definition of 'Survive' versus 'Sustain'.	The lack of clarity regarding the definition of 'Survive' versus 'Sustain' was raised in Round 1 under responses R049 and R051. There are very distinct differences between the 'Survive' and 'Sustain' functions, however it appears this is still not clear in the provided materials. This concern was addressed by developing a chart that demonstrates system function over time throughout the incident lifecycle with annotated taxonomical resilience phases, as detailed at A148 Decision 1.	No changes made, reinforces A148 Decision 1.
A169	Awareness should be a function in its own right and not part of 'Prevent'.	The lack of system awareness of threats is addressed in the taxonomical analysis of Question 3 responses and the outcome is recorded at A140 Decision 1.	No changes made, reinforces A140 Decision 1.

Table 36 – Analysis of Delphi Study Round 2 Question 4 Survey Responses

In the analysis above there were a couple of key themes that arose from the collective expert responses:

- The proposed model should describe what must occur to transition between phases.
- Awareness should be considered as a function in its own right and not effectively part of 'Prevent'. This feedback was also raised in Question 3 responses and is addressed in Section 4.1.2.2.3.3.
- Centring 'Adapt' in the model places too much importance on it.

4.1.2.2.4.3 Outcomes

The table below captures a summary of the changes made based on the expert opinions:

Ref	Modifications
A153-1	Add conditions for what must occur to transition between phases of the model.
A153-2	Modify resilience time graph (see A148-1) to demonstrate how each resilience phase aligns with system impact and annotate phase transition requirements.
A164-1	Rename 'Prevent' to 'React'.
A164-2	Remove 'Adapt' from centre of diagram.

Table 37 - Summary of post-analysis changes to the Delphi Study Round 2 Question 4 proposal

4.1.2.3 Survey Round Three

The Delphi Study Round 3 questions are described in Section 3.3.2.5 and should be referenced when interpreting the below analysis.

The approach to Round 3 of the Delphi Study was slightly different to those of previous rounds, in that the participants were requested to provide optional feedback. The following was communicated to participants and accompanied the release of the Delphi Study Round 3 survey: "No response will be taken as no major objections to the attached outcomes." After 3 months, a communication was released to notify participants of the conclusion of the study and to thank them for their participation.

A summary of all changes that were made as a result of the Delphi Study Round Three survey responses is provided in the table below for ease of reference. All original responses and justifications behind the stated modifications are detailed in the remainder of this section.

Ref	Modifications
Question 1 Outcomes	
N/A	No changes made.
Question 2 Outcomes	
A170-1	Add 'Onboard Physical Security and Self-Protection Equipment' to address kinetic threats to the Human Segment when in space.
A170-2	Add 'Security Culture' to the supporting definition of 'Human Segment' in the space systems security knowledge domain.
Question 3 Outcomes	
N/A	No changes made.
Question 4 Outcomes	

A170-3	Add ‘to better anticipate, react, survive, sustain and recover from future adverse events’ to the definition of ‘Adapt’.
Question 5 Outcomes	
N/A	No changes made.

4.1.2.3.1.1 Responses

No objections to the proposed definitions and models were raised throughout this period, with several respondents replying to affirm the positive results of the study. One respondent provided further comments and suggestions by email, which is provided verbatim in the table below. Note that spelling and grammatical errors have been included to avoid any inadvertent interference with the raw data.

ID	Response	Objections
R170	Outstanding work, and my most sincere congratulations on the outcomes of this project. My first piece of final feedback is that the space systems security definition is robust, but also an incredibly important piece of work, from or by which I am sure countless further endeavours will be launched or at least inspired. The rest of my final feedback is largely inconsequential, but still, in for penny in for a pound! • “Space systems security is the assurance of the availability of the services, control, ~~and~~ integrity, and confidentiality of a space system throughout its lifecycle, including all ground, communications, and space components, as well as the people, data, processes, and supply chains ~~that~~ by which it is enabled.” o Strikethrough and red text used to indicate some minor adjustments to the definition of SSS to align more closely with the language of the all-mighty (but admittedly widely recognised, understood and followed) ‘CIA triad’, and to get rid of ending the sentence on a proposition (that’s just annoying). • Outcome 2, Human Segment, Kinetic – Protection from kinetic threats of the kind listed could also be provided by various types of personal armour and certain types of shielding. Similarly, it might be a conversation in and of itself, but I would say that astronauts operating in or on a space asset that’s likely to encounter kinetic adversaries would likely stand to benefit from being armed and/or trained in self-defence. I will give you a call and we can discuss that one and hopefully I can communicate what I mean a bit more clearly. Another term that might be more palatable could be ‘active defence systems’. • Outcome 2, Ground segment, assurance of ground components against cyber adversities: I would add to this reference to “security culture” in a manner similar to that featured in the preceding column. • Outcome 3: **Adapt**, which refers to the system’s ability to evolve based on threat intelligence and lessons learned from adverse events so that the Space System can better *anticipate, react, survive, sustain* and *recover* from future events.	No

	○ Just a suggestion for how it might be phrased, but I think you get the idea here – It should be made inescapably clear that he evolution to which you refer is connected to the preceding elements of SSR, and it's cool to create a link to previously established concepts within the taxonomy. Otherwise and overall, I think this is excellent, I am thrilled with the outcomes, and I feel privileged to have been offered the opportunity to contribute to this work.	

Table 38 - Delphi Study Round 3 Survey Responses

4.1.2.3.1.2 Analysis

The response provided in the previous subsection was analysed and the proposed definitions and models were modified according to the outcomes recorded in the table below.

ID	Summary and interpretation	Analysis and comments	Decisions
A170	The proposed definitions, knowledge domain, and resilience model are adequate, however some minor grammatical aspects can be improved. Consider re-aligning to the widely recognised 'CIA Triad'. The Human Segment should consider kinetic threats. 'Security culture' should be added to the knowledge domain. Suggest to add "so that the system can better anticipate, react, survive, sustain and recover from future adversities" to the definition of 'Adapt'.	Respondents to the Delphi Study Round 1 analysis noted issues with the ambiguity of the CIA Triad and requested that the definition be modified to be intelligible by space professionals more broadly. The outcomes of these responses were to remove the terms 'availability' and 'integrity', as recorded in A093 Decision 1 and A096 Decision 1. Agree that the Human Segment should consider kinetic threats in space, particularly as human spaceflight becomes more viable. The need for physical security for space tourists and astronauts will inevitably arise as human traffic to space increases. This could be considered a form of insider threat, whereby an authorised party is deployed to space, and one becomes aggressive towards the others for whatever reason. These elements must be considered in the knowledge domain. Agree that 'Security culture' should be added to the knowledge domain.	1. Add 'Onboard Physical Security and Self-Protection Equipment' to address kinetic threats to the Human Segment when in space. 2. Add 'Security Culture' to the supporting definition of 'Human Segment' in the space systems security knowledge domain. 3. Add 'to better anticipate, react, survive, sustain and recover from future adverse events' to the definition of 'Adapt'.

		Agree that the taxonomical definitions would be enhanced with the cyclical reference under the 'Adapt' definition.	

Table 39 - Analysis of Delphi Study Round 3 Survey Responses

4.1.2.3.1.3 Outcomes

The table below captures a summary of the changes made based on the expert opinion analysed in the previous section:

Ref	Modifications
A170-1	Add 'Onboard Physical Security and Self-Protection Equipment' to address kinetic threats to the Human Segment when in space.
A170-2	Add 'Security Culture' to the supporting definition of 'Human Segment' in the space systems security knowledge domain.
A170-3	Add "to better anticipate, react, survive, sustain and recover from future adverse events" to the definition of 'Adapt'.

Table 40 - Summary of post-analysis changes to the Delphi Study Round 3 proposal

4.1.3 Expert Focus Group

A virtual focus group session was held with respondents who replied to the Round 3 results in order to discuss the final outcomes of the study. The meeting was brief given that there were no major objections to the Delphi Study outcomes presented in the Round 3 survey pack.

4.1.3.1.1.1 Comments

ID	Comment
R171	The system function time chart from Outcome 5 should have t2 and t3 swapped. The threat must be contained before the system can be stabilised.

Table 41 - Delphi Study Focus Group Comments

4.1.3.1.1.2 Analysis

ID	Summary and interpretation	Analysis and comments	Decisions
A171	The threat must be contained before the system can be stabilised. Suggest swapping t2 and t3 labels.	Agree, a system cannot be rendered stable until it is no longer experiencing immediate impacts from an ongoing threat event or adversity. The stabilised state is likely to be at a reduced operational capacity, which	1. Switch 'System Stabilised' and 'Threat Contained' in the time graph of Outcome 5.

		is already captured in the presented graph.	

Table 42 - Delphi Study Focus Group Analysis

4.1.3.1.1.3 Outcomes

Overall, the consensus was that major improvements have been made to the original definitions and models presented in Round 1 compared to the modified ones presented in Round 3. Some discussion took place regarding the role of space systems security as human spaceflight continues to advance. However most comments made revolved around issues which have already been addressed in the analysis presented in Section 4.1.2.3.1.3, and so only one minor modification was required, as detailed below:

Ref	Modifications
A171-1	Switch 'System Stabilised' and 'Threat Contained' in both resilience models of Outcome 5.

Table 43 - Delphi Study Focus Group Outcomes

The general findings of the Delphi Study Focus Group were that the proposed definitions, knowledge domain, and model are adequate and the outcomes of the study were positive.

4.1.4 Summary of Delphi Study Outcomes

This section provides a summary of the overall Delphi Study findings across all three rounds. The following subsections provide a summary of the initially proposed definition or model in Round 1 and compares it to the modified outcome after taking into consideration expert feedback on the survey questions post Round 3 analysis.

4.1.4.1 Outcome 1 – Space Systems Security Definition

The Delphi study commenced with the Moltz (2011) definition below:
"Space security is the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction"

The new definition based on iterative expert feedback is:
"Space systems security is the assurance of the services, control, and confidentiality of a space system throughout its lifecycle, including all ground, communications, and space components, as well as the people, data, processes, and supply chains that enable it."

4.1.4.2 Outcome 2 – Space Systems Security Domain

The Delphi study commenced with a preliminary knowledge domain mapping shown in Table 3 (reiterated below for clarity):

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

Table 3 – Originally Proposed Space Systems Security Knowledge Domain

The new knowledge domain based on iterative expert feedback is provided in the below tables, with Table 45 and Table 46 providing further clarification to the knowledge domain presented in Table 44.

	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, Data Preservation
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, Onboard Physical Security and Self-Protection Equipment.	**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.

Table 44 - Final Delphi Outcome: Space Systems Security Knowledge Domain

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

Table 45 - Final Delphi Outcome: Space systems segments

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

Table 46 - Final Delphi Outcome: Space systems adversities

The segments described in Table 45 can be understood to interact, at a high-level, as shown in Figure 33 below.

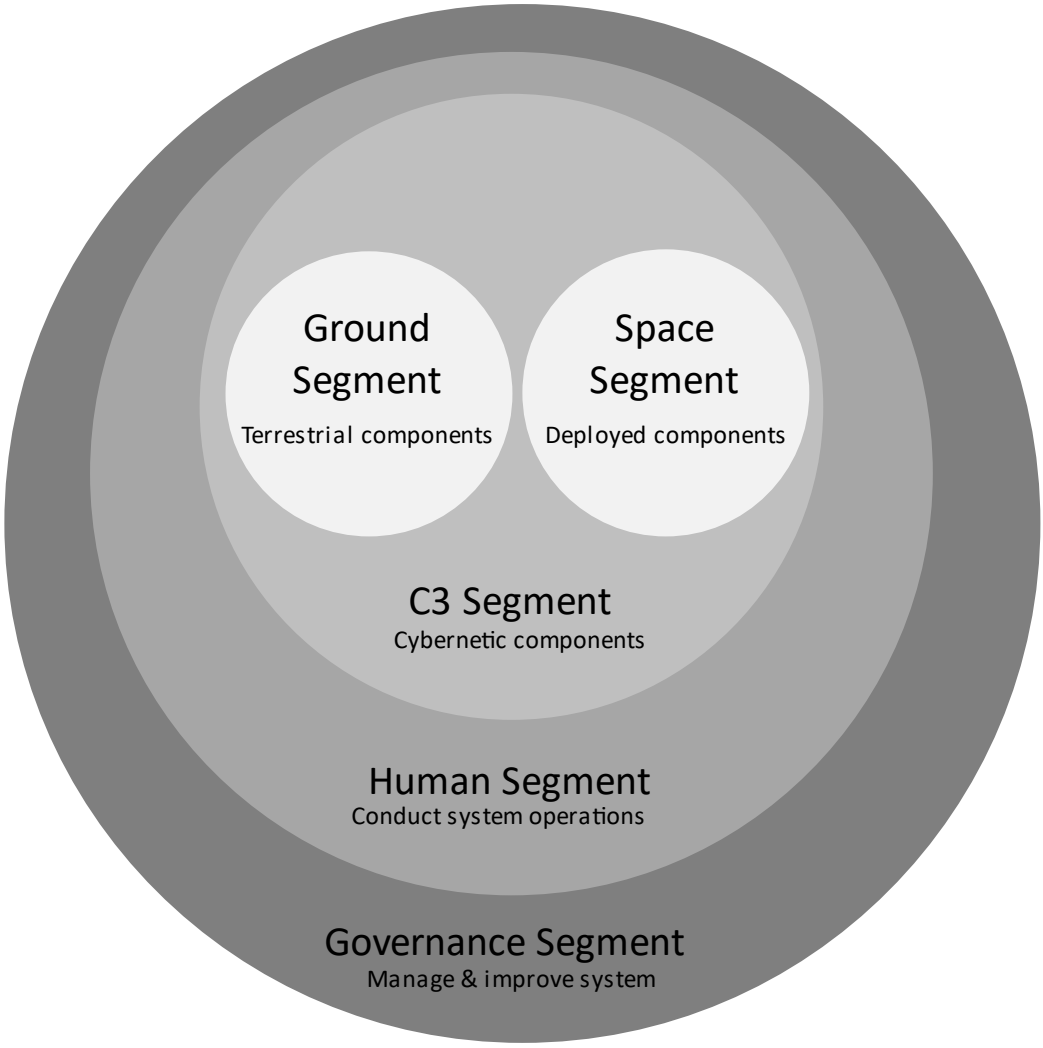

Figure 33 - Final Outcome: Space System Segment Interactions

The figure above demonstrates how each segment interrelates with one another, as well as providing a brief summary of the key functions each segment encompasses. These summary definitions are intended for additional clarity and should not be interpreted strictly. They are provided below:

- Governance Segment: Manage and improve the system.
- Human segment: Conduct system operations.
- C3 Segment: Cybernetic components.
- Ground Segment: Terrestrial components.
- Space Segment: Launched components.

As recounted above and in the examples provided at Table 45, each segment consists of individual processes and operations that interact with other layers.

The ‘Governance Segment’ provides the organisational structures, policies, processes, and other management systems that underpin the entire space system. This is represented as a circle that encompasses the other segments because it controls how the other segments operate throughout the space system’s full lifecycle.

The ‘Human Segment’ provides the human resources, users, astronauts/cosmonauts, and other people-oriented aspects that sustain the space system. It does not include end-users of the space system’s offered services, unless those end-users are within the boundaries of the Governance Segment’s scope. The Human Segment is depicted to sit within the Governance Segment and surrounding the other three segments; C3, Ground, and Space. This indicates that the Human Segment controls how the C3, Ground, and Space segments operate throughout the space system’s full lifecycle.

The ‘C3 Segment’ provides cybernetic components to the space system such as data, computing, and software, as well as the radio-links and antennae that provide the communications. This segment encompasses the Ground Segment and Space Segment because it controls equipment in both those segments and processes any data passing through them.

The ‘Ground Segment’ and the ‘Space Segment’ are both represented in Figure 33 as mutually exclusive circles contained within the other segments. They are mutually exclusive due to geographical barriers, with the Ground Segment being exclusively terrestrial and the Space Segment being exclusively non-terrestrial. The two segments are connected to each other via the C3 Segment, which contains both of them in the diagram.

4.1.4.3 Outcome 3 – Space Systems Resilience Taxonomy

The Delphi study commenced with a 5-stage taxonomy that had emerged out of critical infrastructure resilience literature:

- Anticipate refers to the system’s resilience enhancing mechanisms in place to prevent, detect, and avoid high impact low frequency (HILF) cyber events;
- Survive refers to the system’s resilience enhancing mechanisms in place to mitigate, absorb, and withstand the impacts of the HILF cyber event;
- Sustain refers to the system’s resilience enhancing mechanisms in place to contain any impacts and preserve core functions during a HILF cyber event;

- Recover refers to the system's resilience enhancing mechanisms in place to respond, restore operations, and 'bounce back' from a HILF cyber event; and
- Adapt refers to the processes and procedures in place to reflect on lessons learned and adopt new mechanisms to increase resilience for any similar cyber events in the future.

The new 6-phase Space Systems Resilience taxonomy based on iterative expert feedback is:

- **Anticipate**, which refers to the system's ability to maintain situational awareness and proactively detect potential threats;
- **React**, which refers to the system's ability to avoid, deter, or neutralise detected threats and respond to adverse events;
- **Survive**, which refers to the system's ability to mitigate, absorb, or withstand the impacts of an adverse event;
- **Sustain**, which refers to the system's ability to retain control and preserve core functions and services in a degraded state;
- **Recover**, which refers to the system's ability to respond, restore operations, and 'bounce back' from adverse events.
- **Adapt**, which refers to the system's ability to evolve based on threat intelligence and lessons learned to better anticipate, react, survive, sustain and recover from future adverse events.

4.1.4.4 Outcome 4 – Space Systems Resilience Definition

The Delphi study commenced with the definition below:
"Space systems resilience is the recurring ability of a space system, including all sub-components and supporting functions, to anticipate, survive, sustain, recover from, and adapt to high impact low frequency events."

The new definition based on iterative expert feedback is:
"Space systems resilience is the ability of a space system, including its services, sub-components, and supporting functions, to anticipate, react to, survive, recover from, and adapt to adverse events whilst maintaining control and sustaining core operations and services in a degraded state."

4.1.4.5 Outcome 5 – Space Systems Resilience Model

The Delphi Study commenced with a space-contextualised critical infrastructure resilience model shown in Figure 10 (reiterated below for clarity):

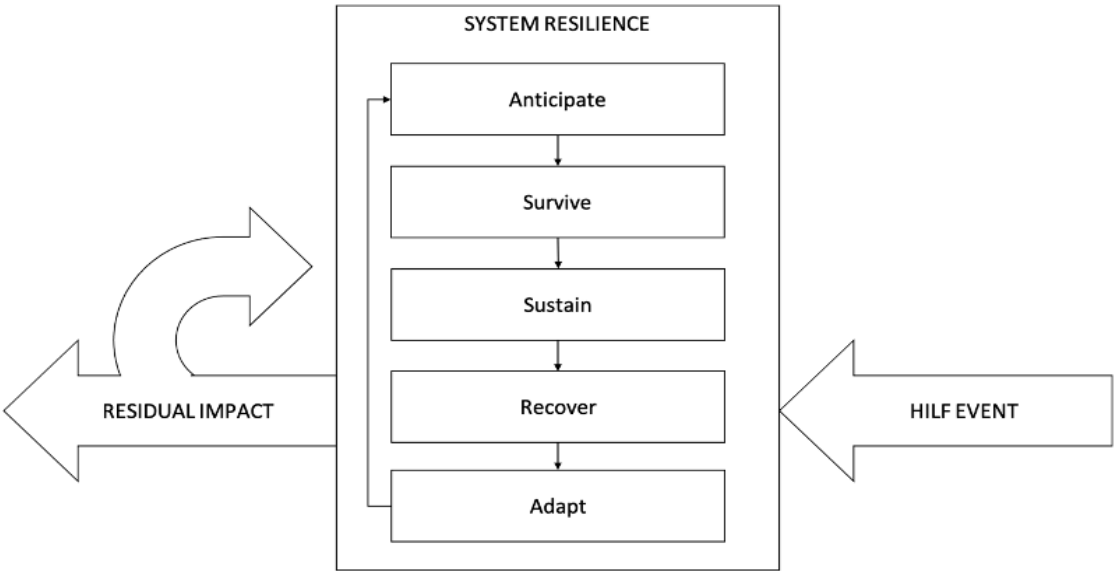

Figure 10 – Resilience cycle in response to High-Impact Low-Frequency (HILF) threats

Based on iterative expert feedback, the new resilience cycle is:

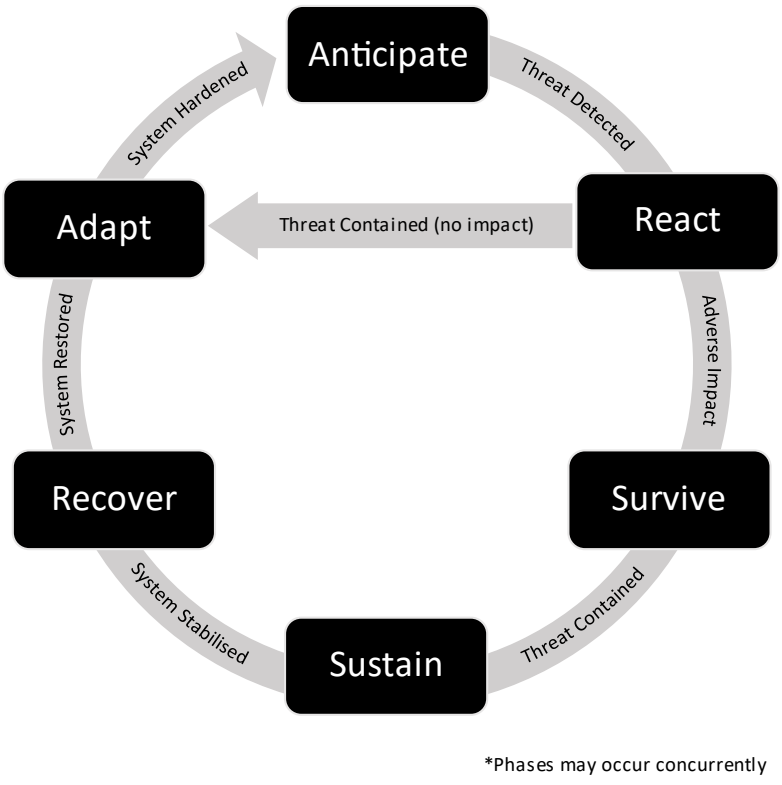

Figure 34 - Final Delphi Outcome: Space Systems Resilience Cycle

The model shown in Figure 34 can also be represented as a function of time, as shown below:

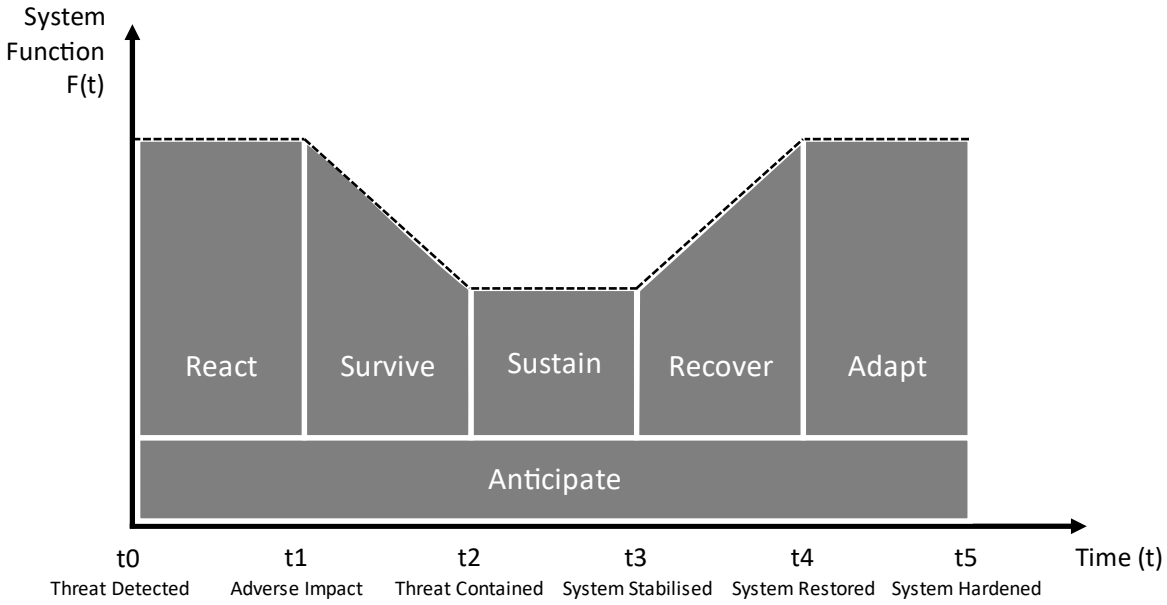

Figure 35 - Final Delphi Outcome: Space Systems Resilience Model

In the diagram shown at Figure 35, each resilience function in the taxonomy is represented on a time graph with t0 to t5 representing the phase transition condition to transition to the next phase in the cycle, as depicted in Figure 34. It is possible for a new threat to trigger a threat detection event (as shown at t0) while an existing adversity has already advanced to a later stage in the resilience cycle. In these cases there will be concurrent adversities and the system resilience cycle triggered by both events will occur concurrently albeit at different stages in the cycle. In some cases this may overwhelm the system, for example if a cyber attack occurs while treating an existing security breach the incident response team may be under resourced to complete the required activities within the required timeframe and the services may be impacted.

In Figure 35 above, 'Anticipate' forms a constant along the bottom of the chart. This ensures that the space system is always on alert for potential adversities and actively monitoring for threats. These activities occur concurrently to the other phases of resilience, so the system is able to 'React' to new threats even whilst dealing with an ongoing adverse event. A scenario such as this is common for cyber security incidents, for example, where one attack is often a precursor or distraction for other concurrent attacks to take place.

In the same figure, t0 marks the moment the system decides to react based on evidence gained in the 'Anticipate' phase. In a resilient system the 'React' phase occurs before any significant consequences have been realised. For example, it may simply involve the exceptional deployment of patches to a recently identified critical vulnerability in one of the core softwares installed in the ground segment. Or it may require a complex response to a high risk threat, such as manoeuvring the space vehicle to avoid, or indeed destroy, debris; whether incidental or malicious. The 'React' phase in the resilience cycle aims to curtail the threat before impact and is often brief but crucial in determining the system's overall resilience to adversities.

The moment a significant consequence from an adverse event is realised, the 'Survive' phase is entered, marked by t1 in the diagram at Figure 35. A significant consequence, or adverse impact, includes any impacts that affect the core mission of the space system; that is, to provide its services, maintain confidentiality, and to retain control over the system itself. Anytime one of these three aspects are impacted then the overall system functionality, represented by the Y-axis in the diagram, can be understood to decline. Activities that take place in the 'Survival' phase should be triggered by processes and procedures from the 'React' phase and continuously informed by the 'Anticipate' function. Such activities may include incident response (e.g. system triage, reverse malware engineering) and disaster management, informed by business continuity plans and the potential activation of emergency backup systems. The survival phase ends once the threat is contained, taking into account the governance segment such as reputation management and customer relations.

'Sustain' is marked on the diagram as commencing at t2 and represents the point in time where the threat causing the adversity has been contained (i.e. no longer an immediate threat). At this point the system has experienced a quantifiable reduction in performance and a plan can be put in place that allows for critical system operations to continue while less crucial functions are deprioritised, at least until full system functionality is regained. Whilst 'Survive' is concerned with addressing the immediate threat and containing any flow-on impacts, 'Sustain' is concerned with maintaining operations in a degraded state; particularly the critical core functions of the system. These two phases may often occur in parallel, with 'Sustain' always commencing after 'Survive' is already underway.

Once system survival is assured, the damage is known, and any impacts of the adverse event have been quantified, the system enters the 'Recover' phase. At this point incident response teams shift focus from threat-based activities, such as identification and containment, to recovery-based activities, such as restoring routine operations and functionality, as well as any necessary public relations and communications about the incident. The recovery phase is complete once the system has been fully restored to standard operations, as marked by t4 on the diagram.

The final phase, 'Adapt' takes into account any findings identified throughout the previous phases, including if no adverse event was realised. Adaptation activities may be triggered by preventative threat intelligence in the 'Anticipate' function (i.e. the horizontal arrow cutting through the cycle in Figure 34), or it may involve implementing system hardening and organisational improvements based on post-incident analysis. The end of the adaptation phase is marked by t5, where the system, including any governance and personnel aspects, is fully hardened against the threat identified at t0. At this point in time the system is considered to be at full functionality, including the security subsystems, and any resources allocated to response activities can be re-allocated back to the 'Anticipate' function.

4.2 Case Study and Findings

The methodology behind the case study, including the threat model and approach for the case study scenario, is detailed in section 3.3.2.6. This section details the data collection from the expert interviews and provides the detailed analysis of the case study scenario play-throughs.

The aim of the case study is to theoretically validate the research outcomes arising from the Delphi study by testing the framework against a real-world space system. This is achieved by using the threat model in section 3.3.3.3 as a reference to step through each phase of the CKC. This process was simplified in the Methodology chapter to include the below four stages and is detailed further in Figure 32:

1. **Scoping.** The first phase of the scenario covers all scoping activities conducted by both the threat actor and the defending space system. This includes scanning, target/threat identification, and preliminary assessments and decisions to both weaponise and prepare a response.
2. **Instigation.** The second phase of the scenario concerns the initial actions carried out by both the threat actor and the defending space system in the lead up to an attack. This

includes activities by the threat actor to compromise the system and pre-position themselves for their final action on objectives, as well as activities by the defenders to react to identified malicious activity, such as delivery of malicious code or unexpected privileged activity.

3. **Adverse Event.** In the third phase of the scenario, the cyber terrorist threat actor completes their action on objectives, causing a cyber-physical impact to the system and triggering the Survive and, later, Sustain response from the space system. It is in this critical phase that either the threat actor achieves their goal, or the space system proves resilient and successfully manages to contain the threat whilst maintaining baseline services and operations in a degraded state.
4. **Remediation.** The fourth and final phase of the scenario refers to the remaining resilience phases of Recover and Adapt, which take place after the threat actor has completed their attack, any cascading impacts have been contained, and the system is no longer under direct threat. Activities conducted in the phase include restoring the system back to its pre-event baseline and improving the resilience posture based on findings made during the adverse event.

At each of the four stages outline above, the threat actor's actions are theoretically simulated against the space system in question, as detailed by the case study expert participants, with potential outcomes being modelled based on gaps in resilience posture identified through the interviews. The outcomes of this experimental case study methodology are detailed in this section. For ease of reference, the threat model table defined in the Methodology chapter is repeated below:

Aspect	Case Study Definition
Actor	A state-sponsored terrorist organisation with high cyber capability
Motive	Pre-meditated political motivations stemming from ideological foundations
Intent	Damage trust in critical infrastructure organisations and generate instability
Means	Cyber attack
Effect	Availability of services reduced due to cyber-physical impact
Target	Space system (as defined in section 4.2.2 by the case study respondents)

Table 11 - Cyber terrorist threat model definition for the case study

4.2.1 Case Study Respondents

The respondents selected for the case study were space security experts with more than seven years of work experience in industry or government from reputable organisations internationally and with current security responsibilities for the space system in question. Each respondent was identified as responsible for different space systems at separate organisations, covering both domestic and international applications. The first respondent provided data surrounding resilience controls for a launchpad mission control system, whilst the second respondent provided data on the resilience measures in place for the ground stations they are responsible for. Both expert participants were also able to provide some complementary information surrounding the security and resilience controls in place on payloads and the broader space segment. This was utilised to develop a third case study on the space segment, in addition to the launchpad mission control system and ground station scenarios.

4.2.2 Interviews

The full transcripts of each case study interview as well as the tables containing all recorded data is provided in this section and the associated appendices. This data is used as input into the case steady threat scenario, with detailed analysis of each system's resilience assessment provided in the following section. All gathered data from the case study interviews have been filtered to avoid disclosure of personal or corporate information, or any other data which may compromise the confidentiality agreement made with participants. Categorical details of the expert respondents to the survey interviews are detailed in section 4.2.1. The methodology behind the interview process is examined in section 3.3.

Interviews were conducted in an Australian context, so it should be noted that a portion of the data collected refers to Australian standards and regulatory Acts. For example, when 'NV1' (i.e., Negative Vetting level 1) is mentioned the interviewer or expert respondent are making reference to the Australian Government personnel security vetting process run by the Australian Government Security Vetting Agency (AGSVA). The NV1 level of security clearance is obtained through a series of background and police checks as well as a psychological interview and provides a moderate level of assurance that the person is trustworthy in the context of national security. Additionally, IRAP, ISM, SOCI, and DISP are acronyms frequently used in the Australian Government and cyber security context, and refer to Australian security standards and programs that each seek to provide a level of security

assurance for the system. In short, the IRAP (Industry Registered Assessors Program) scheme produces Australian Government endorsed cyber security professionals who have proven competency in assessing controls related to the Australian Government ISM (Information Security Manual). The ISM is comprised of a comprehensive set of controls and guidelines that provide cyber security guidance on protecting sensitive and classified information and is often implemented on Australian systems across the Defence and Critical Infrastructure industries. SOCI refers to the Australian Security of Critical Infrastructure Act, which defines high-level obligations for critical infrastructure owners and operators across Australia, including those deemed Space Technology or Defence Industry. Finally, DISP is the Australian Defence Industry Security Program, which is a membership that private entities must be admitted to prior to handling national security related official or classified information. The DISP membership scheme requires that a minimum level of security controls be implemented across the four pillars of: Governance, Physical, Personnel, and Information & Cyber.

4.2.2.1 Launchpad Mission Control

The full transcript of the case study interview regarding the launchpad mission control system (MCS) security and resilience is provided in Appendix C. All audio was recorded during a video conversation with the knowledge domain table at Table 44 visible to both the interviewer and the expert respondent throughout the duration of the call. The data was recorded in a blank version of the knowledge domain table, which served to both guide the discussion as well as ensuring comprehensive coverage across all relevant aspects regarding the space system's security measures. The final state of the recorded data for the launchpad mission control system is provided in Table 47 below.

	Governance Segment	Human Segment	Ground Segment	Space Segment	C3 Segment
Non-Malicious	10% of workforce is focused on regulatory compliance. Some DRP, backups, redundancy for availability reqs. ASA licensing. Lack of assurance,	Good security culture, NV1 clearance, security briefing (physical/cyber/routine), container for MCS, WHS.	Collision and Avoidance monitoring for space-based assets to determine launch windows (COLA). Software reliability is lacking.	N/A	Telecom system reliability is robust (SAT, VOIP, mobile, UHF, etc) for redundancy. Confidentiality is specific to pre-launch.

	DISP compliance, risk registers.				
Cyber	IRAP, 3PP, centralised monitoring and auditing on IT systems, limited supply chain assurance, some threat intel but no dedicated function, media register, lacking cyber risk management.	Annual cyber training & awareness inc. for newstarts. Campaign-specific security briefings. 2FA, passwords, NV1 clearance for all staff.	No SOC, one-person on-site CIRT, incident reporting, secure-by-design practices in place in line with ISM PROTECTED level controls. No OT security.	N/A	No secure code review, MFA, authorised USBs for transfers, no monitoring on comms, no encryption, no CRC / integrity checking.
Electro-magnetic	ACMA licensing, spectrum analyser, spectrum licensing.	No bug sweeping.	No TEMPEST, remote range helps mitigate jamming.	N/A	Not much due to complexity, cost, and limited technologies available.
Kinetic	Nuclear inspection, insurance.	ID passes (staff/contractor) includes access restrictions, limited social engineering awareness.	20 security cameras across the range, swipe access, defence in depth for physical boundary security, locks but not SCEC-endorsed under the Australian Government scheme.	N/A	Not much due to complexity, cost, and limited technologies available.

Table 47 - Launchpad Mission Control Interview Data

4.2.2.2 Ground Station

The full transcript of the case study interview regarding the ground station security and resilience is provided in Appendix D. All audio was recorded during a video conversation with the knowledge domain table at Table 44 visible to both the interviewer and the expert respondent throughout the duration of the call. The data was recorded in a blank version of the knowledge domain table, which served to both guide the discussion as well as ensuring

comprehensive coverage across all relevant aspects regarding the ground station's security measures. The final state of the recorded data for the ground station system is provided in Table 48 below.

	Governance Segment	Human Segment	Ground Segment	Space Segment	C3 Segment (focused on ground)
Non-Malicious	Good controls for DRP, BCP, legal/reg compliance, high availability requirements, limited supply chain security, V&V in place, product assurance to MILSPEC/AUS standards. Strong data management.	Government security clearances, WHS, Security Training & Awareness, Legal / Regulatory Compliance, insurance, WHS, Human Factors Engineering, Safety Engineering, Strong non-malicious security culture.	Redundancy, backup systems, COTS in use. Reliability Engineering (Telecomm, Software, ICT). High availability mindset.	N/A	Inherited from Government ICT infrastructure and frameworks.
Cyber	Developing cyber strategy and cyber risk management. Good cyber requirements analysis (ISM / DSPF), OT Security in the works, dedicated threat intel function, dedicated GRC roles.	Growing cyber security culture, Cyber Training & Awareness, Good Identity and Access Management, Personnel Vetting, Developing Cyber Security Monitoring, Data Classification	Some secure code review but not comprehensive. Good Identity and Access Management, Developing Cyber Security Monitoring. Developing IT / OT Security Engineering, Security Monitoring. Solid Cyber Incident Response, dedicated roles (for all of the above).	N/A	Data Classification, IT Security, Secure Code Review, Cryptography, Security Monitoring (e.g. IDS/IPS), Anti Malware, Redundancy Engineering, Integrity Checks, Data Classification.
Electro-magnetic	Spectrum management, EM management, E3, dedicated threat intel function.	Perimeter, surveillance, Facility Compartmentalisation, Bug Sweeping, Cell Phone Lockers.	TEMPEST testing. No ECM for buildings/infrastructure. Remote operations for jamming reduction.	N/A	All COTS and Government inherited.
Kinetic	Physical security governance, strong controls, defence in depth, internal and external auditing, strong policies,	Physical Security (e.g. safes / locks, building, perimeter, surveillance), No dedicated Social Engineering Awareness Training	Fencing, restricted access to systems, swipe cards, ID badges, password protections, remote site, CCTV with alerting, site	N/A	Monitoring, Resilience / Redundancy Engineering, Physical Hardening.

	dedicated roles and functions.	(elements within security training)	monitoring, physical patrols. No MFA.		

Table 48 - Ground Station Interview Data

4.2.2.3 Space Vehicle and Payload

Although no individual interview was conducted with an expert participant regarding the space vehicle and payload system, enough data was gathered through the other respective interviews in order to build a theoretical picture of the security and resilience status for the purposes of the case study. Excerpts from the other interviews that shed light on the security status of the space vehicle are provided as samples in Appendix E. The final state of the recorded data for the ground station system is provided in Table 49 below.

	Governance Segment	**Human Segment**	**Ground Segment**	**Space Segment**	**C3 Segment**
Non-Malicious	Adherence to strict legal and regulatory requirements. Business continuity and disaster recovery differs depending on the services delivered by the payload. Poor product assurance and limited V&V for many payloads. Space DevOps being developed.	Inherited from the ground station system security.	Inherited from the ground station system security.	A lot done well to protect against environmental adversities such as space debris and radiation.	Inherited from the ground station system security.
Cyber	Little to no consideration of cyber security on the space vehicle post-launch.	Inherited from the ground station system security.	Inherited from the ground station system security.	IoT devices often sent up as part of payload without secure practices. No anti-malware or IDS/IPS. Inherited vulnerabilities from COTS.	Inherited from the ground station system security.

Electro-magnetic	Spectrum regulation and adherence to legal and regulatory requirements. Limited counter-EW technologies.	Inherited from the ground station system security.	Inherited from the ground station system security.	Nil.	Inherited from the ground station system security.
Kinetic	Nil.	Inherited from the ground station system security.	Inherited from the ground station system security.	Some hardening of space hardware but nothing that could withstand a malicious kinetic attack.	Inherited from the ground station system security.

Table 49 - Space Vehicle and Payload Interview Data

4.2.3 Scenario Analysis

The threat model and theoretical threat event scenario were determined through the literature review and subsequent methodology analysis. The case study methodology, including the detailed threat model and scenario, are described in section 3.3.2.6. This section provides the experimental analysis of the threat model and scenario when applied to the expert respondents' real-world systems using the resilience assessment framework produced by the Delphi study.

This process was simplified in the Methodology chapter to include the below four stages and is detailed further in Figure 32:

1. Scoping, including all scoping activities conducted by both the threat actor and the defending space system.
2. Instigation, including the initial actions carried out by both the threat actor and the defending space system in the lead up to an attack.
3. Adverse Event, including the cyber-physical impact caused by the threat actor and resulting survival and sustainment responses from the space system. It is in this phase that the space system either fails or succeeds in proving resilient to the adversity.
4. Remediation, including the activities conducted after the threat actor has completed their attack and any cascading impacts have been contained. This phase is given less emphasis in the experimental case study process.

At each of the four stages outlined above, the threat actor's actions are theoretically simulated against the space system in question, as detailed in each subsection below, with potential outcomes being modelled based on gaps in resilience posture identified in the interview data.

In preparation for each case study scenario, the data collected during the interviews was restructured according to resilience strengths and weaknesses of each system. This analysis was then further distilled into a critical chain of resilience posture vulnerabilities, which were finally used as a starting point for the threat scenario simulation.

4.2.3.1 Launchpad Mission Control

The launchpad mission control system is a space system designed to control all of the ground-based components of the spaceport. This includes controlling the technologies used to obtain both air and maritime situational awareness, as well as all the operational technologies related to the launchpad, such as water systems, drones, cameras, communications and telemetry equipment. These subsystems are primarily cyber-physical OT systems that could be targeted by a cyber threat actor to cause a physical impact to the system and affect its mission. Many of the functions that these cyber-physical systems (CPS) provide could have safety implications if interfered with. For example, if the radars or display feed for maintaining air situational awareness are interfered with there could be sizeable consequences. This section will simulate a cyber-physical attack against the launchpad mission control system by a remote cyber terrorist actor with the goal to interrupt a launch.

The data collected during the case study interview of the expert participant responsible for the launchpad mission control system, as captured in Table 47, was distilled into specific strengths and weaknesses in Table 50. This table provides a preliminary analysis of the space system's security and resilience posture. Without compensatory controls, specific weaknesses may be exploited by the threat actor in pursuit of their objectives (see Table 11 for further detail on the cyber terrorist threat actor's defining features and objectives for the case study).

	Governance Segment	Human Segment	Ground Segment	Space Segment	C3 Segment

Non-Malicious	**Strengths** 10% of workforce is focused on regulatory compliance. Backups, redundancy for availability reqs. ASA licensing, DISP compliance, risk registers. **Weaknesses** Lack of assurance, limited DRP.	**Strengths** Good security culture, NV1 clearance, security briefing (physical/cyber/routine), container for MCS, WHS. **Weaknesses** No specific weaknesses noted.	**Strengths** Collision and Avoidance monitoring for space-based assets to determine launch windows (COLA). **Weaknesses** Software reliability is lacking.	N/A	**Strengths** Telecom system reliability is robust (SAT, VOIP, mobile, UHF, etc) for redundancy. Confidentiality is specific to pre-launch. **Weaknesses** No specific weaknesses noted.
Cyber	**Strengths** IRAP, 3PP, centralised monitoring and auditing on IT systems, media register. **Weaknesses** Limited supply chain assurance, some threat intel but no dedicated function, lacking cyber risk management.	**Strengths** Annual cyber training & awareness including for newstarts. Campaign-specific security briefings. 2FA, passwords, NV1 clearance for all staff. **Weaknesses** No specific weaknesses noted.	**Strengths** Incident reporting, secure-by-design practices in place in line with ISM PROTECTED level controls. **Weaknesses** No SOC, one-person on-site CIRT, no OT security.	N/A	**Strengths** MFA, authorised USBs for data transfers. **Weaknesses** No secure code review, monitoring on comms, encryption, or CRC / integrity checking.
Electro-magnetic	**Strengths** ACMA licensing, spectrum analyser, spectrum licensing. **Weaknesses** No specific weaknesses noted.	**Strengths** No specific strengths noted. **Weaknesses** No bug sweeping.	**Strengths** Remote range helps mitigate jamming. **Weaknesses** No TEMPEST.	N/A	**Strengths** No specific strengths noted. **Weaknesses** No Redundancy Engineering, Integrity Checks, ECM / EW Protection, LPI/LPD waveforms, advanced signals

					processing, or signature management
Kinetic	**Strengths** Nuclear inspection, insurance. **Weaknesses** No specific weaknesses noted.	**Strengths** ID passes (staff/contractor) includes access restrictions. **Weaknesses** Limited social engineering awareness.	**Strengths** 20 security cameras across the range, swipe access, defence in depth for physical boundary security. **Weaknesses** Locks may have some vulnerabilities.	N/A	**Strengths** No specific strengths noted. **Weaknesses** No Redundancy Engineering or Physical Hardening.

Table 50 - Launchpad Mission Control Resilience Data

Resilience strengths that were identified through the interview process can be noted to assess aspects of the system that enhance its resilience to adversities. In reference to Table 50, the following high-level resilience strengths were identified in the interview data for the launchpad mission control system:

- General strengths in resilience:
    - Legal and regulatory compliance, including licensing
    - Backups and redundancy
    - Holistic security strategy in place (inferred through DISP compliance)
    - Good security culture, including training and briefings
    - Personnel vetting
    - Third party supply chain vetting
    - High redundancy communications systems
    - Insurance.
- Strengths in resilience specific to cyber adversities:
    - Limited requirement to protect data confidentiality post-launch
    - Documented and baselined security controls (inferred through IRAP)
    - Centralised monitoring and auditing on IT systems
    - Multi factor authentication with complex passphrases as the second factor
    - Secure-by-design practices are in place

    - Controlled and documented data transfers.
- Strengths in resilience specific to electromagnetic adversities:
    - Spectrum analysis and registration
    - Remoteness of the launchpad range.
- Strengths in resilience specific to kinetic adversities:
    - Collision avoidance through COLA
    - Remoteness of the launchpad range
    - Nuclear inspections
    - ID passes and physical access restrictions such as electronic swipe entry
    - Physical boundary security with monitored security cameras.

Resilience weaknesses that were identified through the interview process can be noted to assess aspects of the system that may be vulnerable to adversities. Vulnerabilities in resilience posture can be exploited by adversaries to cause greater, and perhaps irrecoverable, damage, such as the cyber-physical terrorist threat defined by the case study threat model. In reference to Table 50, the following weaknesses were identified in the resilience data for the launchpad mission control system:

- General weaknesses in resilience:
    - Lack of assurance activities, which may weaken the identified strengths
    - Limited disaster recovery processes
    - Software reliability and assurance is lacking
    - Inadequate incident response resourcing and planning, which may increase the impact of incidents.
- Weaknesses in resilience specific to cyber adversities:
    - Limited supply chain assurance
    - No system-specific threat intelligence
    - No cyber risk management processes
    - No OT security
    - No secure code review
    - No monitoring or integrity checking of communications links
    - No data encryption.
- Weaknesses in resilience specific to electromagnetic adversities:
    - No bug sweeping

    - No TEMPEST testing
    - No monitoring or integrity checks on electromagnetic frequencies
    - No electromagnetic countermeasures in place
    - No use of LPI/LPD waveforms or signature management.
- Weaknesses in resilience specific to kinetic adversities:
    - Limited social engineering awareness
    - Vulnerable locks
    - No physical hardening or communications link redundancies.

It should be noted that not all strengths and weaknesses are relevant to this case study scenario. For example, nuclear devices and many electromagnetic attacks require advanced equipment that are not readily available to non-state actors, such as the offensive cyber arm of a terrorist organisation. For this reason, only relevant aspects of the above-noted strengths and weakness are considered in the scenario analysis, as detailed in the following sections.

The identified strengths and weaknesses above can be rearranged into the taxonomical pillars of space systems resilience, as determined in section 4.1.4.3. Rearranging the strengths and weaknesses in this manner provides a resilience lens on the security controls identified through use of the space systems security knowledge domain table. For the purposes of this case study exercise, only the strengths and weaknesses identified to be relevant to the cyber terrorist scenario are represented in Table 51 below.

Resilience Function	**Strengths**	**Weaknesses**
Anticipate – the system's ability to maintain situational awareness and proactively detect potential threats.	• Good security culture, including training and briefings • Personnel vetting • Third party vetting • Centralised monitoring and auditing on IT systems • Controlled and documented data transfers	• Lack of assurance activities weakens existing controls • Software reliability and assurance is lacking • Limited supply chain assurance • No system-specific threat intelligence • No cyber risk management processes • No OT security

		• No monitoring or integrity checking of communications links • Limited social engineering awareness.
React – the system's ability to avoid, deter, or neutralise detected threats and respond to adverse events.	• MFA with complex passphrases.	• Inadequate incident response planning. • No OT security • No secure code review • No cyber risk management processes • No encryption.
Survive – the system's ability to mitigate, absorb, or withstand the impacts of an adverse event.	• High redundancy networks and systems.	• Inadequate incident response resourcing and planning • Lack of assurance activities weakens existing controls • Software reliability and assurance is lacking • No OT security.
Sustain – the system's ability to retain control and preserve core functions and services in a degraded state.	• High redundancy networks and systems.	• Lack of assurance activities weakens existing controls • Limited disaster recovery processes • Limited supply chain assurance • No OT security.
Recover – the system's ability to respond, restore operations, and 'bounce back' from adverse events.	• Data backups • Insurance • Documented and baselined system.	• Lack of assurance activities weakens existing controls • Limited disaster recovery processes • No OT security.
Adapt – the system's ability to evolve based on threat intelligence and lessons learned to better anticipate, react, survive, sustain and recover from future adverse events.	• Secure-by-design practices • Holistic security strategy • Good security culture, including training and briefings.	• Lack of assurance activities weakens existing controls • No system-specific threat intelligence • No cyber risk management processes • No OT security.

Table 51 - Launchpad Mission Control Resilience Strengths and Weaknesses

4.2.3.1.1 Scoping

The first phase of the case study threat scenario involves scoping activities conducted by both the cyber terrorist threat actor and the defending launchpad mission control system. In this phase the cyber terrorist actor conducts Reconnaissance and Weaponisation in line with the CKC model presented in section 3.3.3.4. At the same time, the launchpad mission control system carries out activities related to the Anticipate function of the space systems resilience model. In this scenario, the ultimate goal of the cyber terrorist is to cause a cyber-physical impact to the system.

Threat actor reconnaissance involves vulnerability scanning and social engineering techniques to identify weaknesses in the launchpad mission control system that could be exploited in pursuit of the final objective to impact the control and/or services of the system. During this period of time the cyber terrorist threat actor is collecting intelligence about their intended target and method of attack to achieve their overarching objectives, as determined in Table 11. As this occurs, the launchpad mission control system is conducting resilience activities to Anticipate the cyber terrorist's scoping activities, including both Reconnaissance and Weaponisation.

As determined through the Delphi Study process, Anticipate refers to the system's ability to maintain situational awareness and proactively detect potential threats. For the launchpad mission control system, the following weaknesses in the Anticipate function of resilience were identified:

- Lack of assurance activities weakens existing controls
- Software reliability and assurance is lacking
- Limited supply chain assurance
- No system-specific threat intelligence
- No cyber risk management processes
- No OT security
- No secure code review
- No monitoring or integrity checking of communications links
- Limited social engineering awareness.

Offsetting the above weaknesses, certain strengths in scoping were also identified for the defending launchpad mission control system. These strengths may be unknowingly weakened through the identified lack of assurance activities, however for the purposes of this case study they are deemed to be functioning effectively. Each identified strength can be said to limit the opportunities for the cyber threat actor to progress to more advanced stages of the CKC, and include:

- Good security culture, including training and briefings
- Personnel vetting
- Third party vetting
- Centralised monitoring and auditing on most IT systems
- Controlled and documented data transfers.

Taking into account both the strengths and weaknesses in resilience, the cyber terrorist threat actor has a few different options available for the successful completion of their scoping activities. Some strengths also offset some weaknesses to limit the adversary's options; for example, personnel and third-party vetting combined with a good security culture and regular security training can limit some of the insider threat opportunities that may arise due to a lack of social engineering awareness. The remaining weaknesses can be distilled into a few core vulnerabilities that the threat actor may exploit in pursuit of their goals.

Perhaps most notably, several weaknesses were identified regarding the security and assurance of software in the launchpad mission control system, including a lack of: software reliability testing, software assurance, secure code review, supply chain assurance, system-specific threat intelligence, and OT security. Software vulnerabilities are ideal for malicious cyber threat actors, such as the cyber terrorist defined for the case study threat model, because they provide a foothold for the Delivery phase of the CKC (i.e., the CKC phase that initiates the Instigation phase of the case study scenario). Software vulnerabilities may be identified by the threat actor through the initial Reconnaissance activities and will determine the approach taken for the Weaponisation phase of the CKC. The cyber terrorist may identify vulnerabilities through technical system scanning or social engineering techniques.

Vulnerability scanning conducted by the threat actor may be identified by the Launchpad Mission Control system through monitoring and auditing activities, however such activities are

notoriously complicated to differentiate between legitimate threats to the system and routine scanning activities conducted by botnets and other automated or partially automated processes. Taking into account the limited security personnel, as identified during the interview, it is plausible that scanning activities conducted by the threat actor may go undetected or unactioned.

Additionally, the OT systems are not being monitored or secured in any way, leaving the cyber-physical components of the system vulnerable to attack. Although many OT systems are designed to be mostly 'air gapped', it is still common that there may be some connectivity to other networks. For example, OT networks and devices are often connected in some way to the corporate IT network in order to collect monitoring data, such as through SCADA, or to enable a level of remote visibility for command and control management. Without adequate IT-OT segregation, OT networks may be exposed to the corporate network and any threats that exist within the IT environment. It is also increasingly common for OT systems to have some level of internet connectivity for remote administration and maintenance, especially where the site location is remote and difficult to routinely access. For these reasons, the case study scenario assumes that the OT network is accessible for some Reconnaissance activities by the threat actor.

It may be possible that other avenues for successful Reconnaissance and Weaponisation exist, however for the purposes of this case study the cyber terrorist actor need only a single viable path to progress to the Instigation stage. The Instigation stage commences once the threat actor is positioned to deliver the weaponised payload designed for the Launchpad Mission Control system in question and commences active Delivery of weapons and Exploitation of vulnerabilities.

4.2.3.1.2 Instigation

The second phase of the scenario concerns the initial actions carried out by both the threat actor and the defending launchpad mission control system in the lead up to an attack. For the cyber terrorist threat actor this includes activities to compromise the system and pre-position for the final Action on Objectives, including the Delivery, Exploitation, Installation, and Command & Control phases of the CKC, as presented in section 3.3.3.4. At the same time the defending Launchpad Mission Control system is in Anticipate mode and hence given the opportunity to React to identified malicious activity, such as delivery of malicious code or unexpected

privileged activity and attempt to contain the threat before any adverse event inflicts impact to the system. These aspects of the CKC are somewhat easier to detect and identify as malicious compared to Reconnaissance activities.

Upon the successful Delivery of cyber weapons developed by the terrorist in the previous stage, the system is deemed compromised and the threat actor is well positioned to escalate their attack through the phases of the CKC. Delivery may involve a complex combination of different threat vectors and attacks and often leads to the installation of malicious code on the system. This allows several opportunities for the threat actor to be detected by the system and the React phase initiated as part of the resilience cycle.

As determined through the Delphi Study process, React refers to the system's ability to avoid, deter, or neutralise detected threats and respond to adverse events. For the launchpad mission control system, the following weaknesses in the React function of resilience were identified:

- Inadequate incident response resourcing and planning
- No OT security
- No secure code review
- No cyber risk management processes
- No encryption.

Only one strength was identified in the React function of the defending launchpad mission control system, "MFA with complex passphrases". However, it should be noted that activities conducted as part of the Anticipate function are required until the threat has successfully been detected. As such, some strengths and weaknesses may carry over from the Scoping stage to the Instigation stage. Accordingly, the following strengths and weaknesses in the Launchpad Mission Control system's Anticipate function may be relevant to the successful deployment of React function activities in this case study scenario:

- Strengths
    - Good security culture, including training and briefings
    - Centralised monitoring and auditing on most IT systems.
- Weaknesses
    - Lack of assurance activities weakens existing controls
    - Limited supply chain assurance

- No system-specific threat intelligence
- No cyber risk management processes
- No monitoring or integrity checking of communications links
- Limited social engineering awareness.

In the case of the Launchpad Mission Control system, there are several weaknesses that the cyber terrorist threat actor may use to Deliver weapons to the system and Exploit available vulnerabilities to Install malicious payloads and attain Command and Control of the aspects of the system that are required for the final Action on Objectives. Most notably, the insecure OT systems, supply chain weaknesses, lack of encryption, and lack of assurance activities, together represent a collection of vulnerabilities that may be chained together to the threat actor's advantage. With the objective of causing a cyber-physical impact the OT systems are expected to be the primary target for attack, however it is likely that other systems will be compromised in the process. A lack of encryption also allows for easier manoeuvring for the threat actor inside the system. Another avenue for creating a cyber-physical impact would be to use the Launchpad Mission Control system to impact any payloads scheduled to be launched into orbit. The centralised logging and auditing activities are not conducted on the OT network and so it is likely that any pre-positioning of the threat actor will go unnoticed.

Even in the case of successful threat detection, the small security team and lack of incident response capabilities, particularly on the cyber-physical OT systems, may lead to inevitable compromise. If the threat actor is perceptive, they may notice that they have been detected and quickly move to cause any impact possible to the system before being triaged and losing access. With no pre-prepared incident response plan, any post-detection triage or incident response processes will be slowed down and potentially ineffective. Finally, without risk management processes in place, it is plausible that not all potential cyber-physical risks were considered and mitigated against, hence the impacts could be still significant depending on how early the threat is able to be detected and quarantined.

It should be noted that some attacks may serve as a distraction for system responders whilst another attack is coordinated to occur simultaneously. In small incident response teams this method of attack can be highly successful. The effectiveness of each of these methods of delivery depends on the system in question, including its vulnerabilities, critical functions, and any incorporated technologies. The interviews were kept at a high-level for security purposes,

meaning that specific vulnerabilities were not identified to do a low-level analysis such as a play-by-play simulation of specific attacks. Therefore, for the purposes of this case study, the scenario takes an agnostic approach to specific attacks and instead assumes the successful delivery of whichever method the hypothetical cyber terrorist actor might choose to lead to the next stage, the Adverse Event.

4.2.3.1.3 Adverse Event

In the third phase of the scenario, the cyber terrorist threat actor completes their Action on Objectives phase of the CKC, causing a cyber-physical impact to the system and triggering the Survive and, later, Sustain response from the launchpad mission control system. It is at this stage that the space system's resilience mechanisms that aim to contain the threat and maintain operations in a degraded state are tested.

For the launchpad mission control system to successfully defend against the cyber terrorist's Action on Objectives, it must be able to Survive (i.e., mitigate, absorb, or withstand the impacts of an adverse event) and Sustain operations (i.e., retain control and preserve core functions and services in a degraded state). In consideration of the analysis at Table 51, the following strengths and weaknesses were noted to be relevant to the Adverse Event stage of the case study scenario:

- Strengths
    - High redundancy networks and systems.
- Weaknesses
    - Inadequate incident response resourcing and planning
    - Lack of assurance activities weakens existing controls
    - Software reliability and assurance is lacking
    - No OT security
    - Limited disaster recovery processes
    - Limited supply chain assurance.

Although it was stated earlier that multiple attacks are common as part of a larger coordinated campaign, for the purposes of this case study only a single attack is considered. This simulates the system's Survive function without the added complexities of resilience cycles occurring simultaneously. An attack that aims to cause a cyber-physical impact to the launchpad would take place on the OT systems, for which there are no security controls in place to enhance its

resiliency. Logging and auditing activities are also not conducted on the OT network and so it is likely that any pre-positioning of the threat actor will go unnoticed unless it is detected through the IT network. However, as discovered in the Instigation phase, even if the threat is detected, it is likely that an impact will still occur to the system due to the limited response mechanisms in place. As such, the case study considers the following two scenarios:

1. The threat actor is successful in their Action on Objectives and the launchpad is rendered inoperable at the time of launch due to cyber attack, deeming the launch operation a failure.
2. The threat actor is detected before completing their Action on Objectives and the impact is delivered prior to the time of launch, allowing time for the launchpad to prove resilient and sustain operations in a degraded state.

In the first scenario, the launchpad is rendered inoperable and the launch is deemed a failure. In this situation the system has not proven resilient to cyber-physical attack because it has failed to maintain control and deliver its core services as required. Due to the lack of incident response and security assurance processes, the system may experience heightened impacts over extended periods of time. The system must enter the Remediation stage in order to Recover and Adapt to increase resilience against similar attacks in the future. In this case, and as discussed in section 2.2.2.3.2, social impacts should also be considered such as any flow on impacts of launch failure. For example, Liu et al. (2016) state that "a resilient system should assess whether social well-being has indeed been preserved after a critical event". The impacts of a cyber-physical attack on a launchpad system would likely depend on the nature of the payloads that were failed to be launched while the system remains unserviceable. In Table 11 the cyber terrorist's Intent is defined as to damage trust in critical infrastructure organisations and generate instability. Such impacts may include political, social, economic, or psychological impacts outside the system's boundary. A key function that is required to minimise this kind of impact is the communications and public relations function, which can serve to reduce any flow-on effects after an incident, particularly in relation to reputation management and maintaining a level of public and government trust.

The second scenario allows for further consideration of the launchpad mission control system's Survive and Sustain functions. In this scenario the threat actor is detected before completing their Action on Objectives and the impact is delivered prior to the time of launch. In this situation the threat actor may not have achieved their key Effect, as defined in Table 11,

however some impact is still delivered to the launchpad mission control system. Without the defined Effect on the system being achieved, the availability of the launchpad mission control services may not be directly reduced due to a cyber-physical impact. However, the system is yet in a degraded state and so its resiliency is still being tested. At this point a non-catastrophic adverse event is experienced and the system enters the Survive phase of the resilience cycle at Figure 34.

The launchpad mission control system was noted to have high redundancy networks and devices, so if any equipment was damaged in the attack, then it is probable that it would readily be able to be replaced. However, with no disaster recovery or incident response processes in place this activity may take longer than necessary, ultimately reducing the availability of the system for a longer period of time. Limited supply chain assurance also holds the potential to increase the length of system downtime after an availability compromise on non-swappable devices, especially for any PLCs or other industrial components. Finally, with no OT security controls in place, any impacts to the operational infrastructure of the Launchpad Mission Control system may render the system unserviceable for extended periods of time. Firstly, with no controls in place to help pinpoint the areas of compromise, the integrity of the entire OT system is at risk and so cannot be relied upon until after a full-scale investigation. The investigation will necessarily include the entire system due to the lack of logging, monitoring, or prevention techniques on the network. However, IT systems are routinely backed up and there is redundancy in communications channels. So, the IT and communications aspects of the Launchpad Mission Control system are likely to be able to withstand some impact, such as ransomware on the corporate network or a DDoS on a communications channel, for example.

4.2.3.1.4 Remediation

The fourth and final phase of the scenario refers to the remaining resilience functions of Recover and Adapt. Activities related to these functions are initiated once the immediate impacts have been contained and the system is no longer under direct threat, such as after triage and post-incident reporting. Activities conducted in this phase include restoring the system back to its pre-event baseline and improving the resilience posture based on findings made during the adverse event. The threat actor is no longer considered at this stage in the scenario.

For the launchpad mission control system, the following weaknesses in the Recover and Adapt functions of resilience were identified and are relevant to this scenario:

- Lack of assurance activities weakens existing controls
- Limited disaster recovery processes
- No OT security
- No cyber risk management processes.

By contrast, the following relevant strengths in the Recover and Adapt functions of resilience were identified for the launchpad mission control system:

- Data backups
- Insurance
- Documented and baselined system
- Holistic security strategy
- Good security culture.

In light of the above, the launchpad mission control system is likely to be able to be restored back to a previous state that was stored and documented prior to the adverse event. Depending on the level of insurance coverage, any economic impacts of the adverse event is also likely to be minimised. A good security culture will minimise social impacts to the Human Segment, in that there will be an increased emphasis on recovery rather than blame. Finally, as far as strengths are concerned, the existing security strategy can be updated as part of adaptation efforts.

However, remediation efforts may be hampered by a lack of recovery processes and risk management methodologies. Risk management allows for accurate communication and prioritisation of restoration and adaptation functions based on criticality. A lack of pre-existing processes and risk tolerance definition may hinder post-incident communication and slow the restoration process, thus extending the impact of the adverse event. Without recovery processes and procedures the full system restoration may also be slowed down with specific components or subsystems potentially deemed irrecoverable, particularly on OT subsystems.

4.2.3.2 Ground Station

The ground station is a space system designed to facilitate communication and control of space-based assets. This includes managing the operational technologies that enable communications as well as processing of any data being sent to or received from artificial satellites in orbit. The

subsystems controlled by the ground station are primarily cyber-physical OT systems that could be targeted by a cyber threat actor to cause a physical impact to the system and affect its availability. Many of the functions that these cyber-physical systems (CPS) provide could have severe implications if interfered with. For example, if the data being transmitted or received is interfered with, the space vehicle and payload itself could be at risk of cyber attack. This section will simulate a cyber-physical attack against the ground station by a remote cyber terrorist actor with the goal to disable the physical infrastructure and interrupt communications with the space asset.

The data collected during the case study interview of the expert participant responsible for the ground station system, as captured in Table 48, was distilled into specific strengths and weaknesses in Table 52. This table provides a preliminary analysis of the space system's security and resilience posture. Without compensatory controls, specific weaknesses may be exploited by the threat actor in pursuit of their objectives (see Table 11 for further detail on the cyber terrorist threat actor's defining features and objectives for the case study).

	Governance Segment	Human Segment	Ground Segment	Space Segment	C3 Segment (focused on ground)
Non-Malicious	**Strengths** Good controls for DRP, BCP, legal/reg compliance, high availability requirements, V&V, product assurance to MILSPEC/AUS standards. Strong data management practices. **Weaknesses** Limited supply chain security.	**Strengths** Government security clearances, WHS, Security Training & Awareness, Legal / Regulatory Compliance, Insurance, WHS, Human Factors Engineering, Safety Engineering, Strong non-malicious security culture. **Weaknesses** No specific weaknesses noted.	**Strengths** Redundancy, backup systems, COTS in use. Reliability Engineering (Telecomm, Software, ICT). High availability mindset. **Weaknesses** No specific weaknesses noted.	N/A	**Strengths** Inherited from Government ICT infrastructure and frameworks. **Weaknesses** Inherited from Government ICT infrastructure and frameworks with little visibility.
Cyber	**Strengths** Good cyber requirements analysis	**Strengths** Good Cyber Training & Awareness, Identity	**Strengths** Good Identity and Access Management,	N/A	**Strengths** Data Classification, IT Security, Secure

	(ISM / DSPF), dedicated threat intel function, dedicated GRC roles. **Weaknesses** Immature cyber security strategy, cyber risk management, and OT security.	and Access Management, Personnel Vetting, Data Classification. **Weaknesses** Immature cyber security culture.	Cyber Incident Response. Dedicated security roles and positions. **Weaknesses** Some secure code review but not comprehensive. Limited cyber security monitoring, IT / OT Security Engineering. No MFA in place.		Code Review, Cryptography, IDS/IPS, Anti Malware, Redundancy Engineering, Integrity Checks, Data Classification. **Weaknesses** No specific weaknesses noted.
Electro-magnetic	**Strengths** Spectrum management, EM management, E3, dedicated threat intel function. **Weaknesses** No specific weaknesses noted.	**Strengths** Perimeter, surveillance, Facility Compartmentalisation, Bug Sweeping, Cell Phone Lockers. **Weaknesses** No specific weaknesses noted.	**Strengths** TEMPEST testing. Remote operations for jamming reduction. **Weaknesses** No ECM for buildings/infrastructure.	N/A	**Strengths** Inherited from COTS and Government. **Weaknesses** Inherited from COTS and Government with limited visibility.
Kinetic	**Strengths** Physical security governance, strong security controls, defence in depth, internal and external auditing, strong policies, dedicated roles and functions. **Weaknesses** No specific weaknesses noted.	**Strengths** Physical Security (e.g. safes / locks, building, perimeter, surveillance). **Weaknesses** Limited Social Engineering Awareness Training.	**Strengths** Fencing, restricted access to systems, swipe cards, ID badges, password protections, remote site, CCTV with alerting, site monitoring, physical patrols. **Weaknesses** No specific weaknesses noted.	N/A	**Strengths** Monitoring, Resilience / Redundancy Engineering, Physical Hardening. **Weaknesses** No specific weaknesses noted.

Table 52 - Ground Station Resilience Data

Resilience strengths that were identified through the interview process can be noted to assess aspects of the system that enhance its resilience to adversities. In reference to Table 52, the following high-level resilience strengths were identified in the interview data for the ground station system:

- General strengths in resilience:

    - Disaster recovery and business continuity plans are in place
    - High availability systems
    - Verification and validation
    - Product assurance rated to Australian standards up to MILSPEC
    - Strong data management practices
    - Personnel vetting
    - Security Training & Awareness
    - Insurance
    - Human factors and safety engineering
    - Strong general security culture with a high availability mindset
    - Redundancy and backups in place for all systems
    - Reliability engineering
    - Inherited strengths from Government ICT infrastructure and frameworks
    - Internal and external auditing
    - Strong policies.
- Strengths in resilience specific to cyber adversities:
    - Extensive system security control requirements for IT (based on the ISM)
    - System-specific threat intelligence
    - Dedicated cyber security and governance roles
    - Cyber training and awareness
    - Strong identity and access management practices
    - Data classification in place
    - Dedicated cyber incident response
    - Secure code reviews
    - Cryptography in use
    - Intrusion detection and prevention technologies on IT infrastructure
    - Anti-malware in use
    - Redundancy engineering for IT and OT
    - Data integrity checks.
- Strengths in resilience specific to electromagnetic adversities:
    - Electromagnetic Environment Effects (E3) and TEMPEST testing
    - EW threat intelligence function
    - Perimeter surveillance

    - Facility compartmentalisation
    - Bug sweeping and cell phone lockers
    - Remote operations for jamming reduction.
- Strengths in resilience specific to kinetic adversities:
    - Physical security governance
    - Defence in depth approach (e.g. safes / locks, building, perimeter, surveillance)
    - Dedicated security roles and functions
    - Restricted access to systems
    - Swipe cards and ID badges
    - Remote site
    - CCTV with alerting
    - Active site monitoring and physical patrols
    - Physical hardening.

Resilience weaknesses that were identified through the interview process can be noted to assess aspects of the system that may be vulnerable to adversities. Vulnerabilities in resilience posture can be exploited by adversaries to cause greater, and perhaps irrecoverable, damage, such as the cyber-physical terrorist threat defined by the case study threat model. In reference to Table 52, the following weaknesses were identified in the resilience data for the launchpad mission control system:

- General weaknesses in resilience:
    - Limited supply chain security
    - Inherited connectivity to Government ICT infrastructure and frameworks with little visibility or control.
- Weaknesses in resilience specific to cyber adversities:
    - Immature cyber security strategy
    - Limited cyber risk management
    - No OT security
    - Immature cyber security culture
    - Some secure code review but not comprehensive
    - Limited cyber security monitoring
    - No MFA in place.
- Weaknesses in resilience specific to electromagnetic adversities:

    - No ECM for buildings/infrastructure
    - Inherited vulnerabilities from COTS and Government devices and networks with limited to no visibility.
- Weaknesses in resilience specific to kinetic adversities:
    - Limited social engineering awareness training.

It should be noted that not all strengths and weaknesses are relevant to this case study scenario. For example, to exploit the lack of ECM for buildings and infrastructure, the terrorist would require advanced equipment that are not readily available to non-state actors. For this reason, only relevant aspects of the above-noted strengths and weakness are considered in the scenario analysis, as detailed in the following subsections.

The identified strengths and weaknesses above can be rearranged into the taxonomical pillars of space systems resilience, as determined in section 4.1.4.3. Rearranging the strengths and weaknesses in this manner provides a resilience lens on the security controls identified through use of the space systems security knowledge domain table. For the purposes of this case study exercise, only the strengths and weaknesses identified to be relevant to the cyber terrorist scenario are represented in Table 53 below.

Resilience Function	Strengths	Weaknesses
Anticipate – the system's ability to maintain situational awareness and proactively detect potential threats.	• Verification and validation • Personnel vetting • Internal and external auditing • Intrusion detection system for IT • Secure code reviews • System-specific threat intelligence • Data integrity checks • CCTV with alerting • Active site monitoring.	• Limited supply chain security • Inherited ICT infrastructure and governance frameworks with little visibility or control • No OT security • Some software and devices are COTS and have not been security reviewed • Limited cyber security monitoring • Limited social engineering awareness training.
React – the system's ability to avoid, deter, or neutralise detected threats	• Human factors and safety engineering • Strong identity and access management practices	• No OT security • Inherited ICT infrastructure and governance frameworks with little visibility or control

and respond to adverse events.	• Dedicated cyber incident response • Cryptography • Intrusion prevention system for IT • Anti-malware • Physical security patrols.	• No MFA in place.
Survive – the system's ability to mitigate, absorb, or withstand the impacts of an adverse event.	• Disaster recovery and business continuity plans are in place • Physical hardening • High availability systems • Product assurance rated to Australian standards up to MILSPEC • Redundancy and backups in place for all systems.	• No OT security.
Sustain – the system's ability to retain control and preserve core functions and services in a degraded state.	• High availability systems • Reliability engineering • Redundancy and backups in place for all systems.	• Limited supply chain security • No OT security.
Recover – the system's ability to respond, restore operations, and 'bounce back' from adverse events.	• Insurance • Backups for all systems • Strong data management practices • Dedicated cyber security and governance roles.	• No OT security.
Adapt – the system's ability to evolve based on threat intelligence and lessons learned to better anticipate, react, survive, sustain and recover from future adverse events.	• System-specific threat intelligence • Security training & awareness • Strong general security culture with a high availability mindset • Internal and external auditing • Strong policies in place • Dedicated cyber security and governance roles.	• Immature cyber security strategy • Limited cyber risk management • No OT security • Immature cyber security culture • Inherited ICT infrastructure and governance frameworks with little visibility or control • Limited social engineering awareness training.

Table 53 – Ground Station Resilience Strengths and Weaknesses

4.2.3.2.1 Scoping

The first phase of the case study threat scenario involves scoping activities conducted by both the cyber terrorist threat actor and the defending ground station system. In this phase the cyber terrorist actor conducts Reconnaissance and Weaponisation in line with the CKC model presented in section 3.3.3.4. At the same time, the launchpad mission control system carries out activities related to the Anticipate function of the space systems resilience model. In this scenario, the ultimate goal of the cyber terrorist is to cause a cyber-physical impact to the system.

Threat actor reconnaissance involves vulnerability scanning and social engineering techniques to identify weaknesses in the launchpad mission control system that could be exploited in pursuit of the final objective to impact the control and/or services of the system. During this period of time the cyber terrorist threat actor is collecting intelligence about their intended target and method of attack to achieve their overarching objectives, as determined in Table 11. As this occurs, the ground station is conducting resilience activities to Anticipate the cyber terrorist's scoping activities, including both Reconnaissance and Weaponisation.

As determined through the Delphi Study process, Anticipate refers to the system's ability to maintain situational awareness and proactively detect potential threats. For the ground station, the following weaknesses in the Anticipate function of resilience were identified:

- Limited supply chain security
- Inherited ICT infrastructure and governance frameworks with little visibility or control
- No OT security
- Some software and devices are COTS and have not been security reviewed
- Limited cyber security monitoring
- Limited social engineering awareness training.

Offsetting the above weaknesses, certain strengths in scoping were also identified for the defending ground station. Each identified strength can be said to limit the opportunities for the cyber threat actor to progress to more advanced stages of the CKC, and include:

- Verification and validation
- Personnel vetting
- Internal and external auditing

- Intrusion detection system for IT
- Secure code reviews
- System-specific threat intelligence
- Data integrity checks
- CCTV with alerting
- Active site monitoring.

It should also be noted that some strengths offset specific weaknesses and hence may limit the adversary's attack options. For example, personnel vetting combined with a good security culture and regular security training can limit some of the insider threat opportunities that may arise due to a lack of social engineering awareness.

With limited cyber security monitoring and social engineering awareness training, the ground station system is especially vulnerable to scoping activities conducted by the terrorist threat actor. A lack of supply chain or OT security combined with the use of COTS and inherited infrastructure may also provide avenues for the threat actor to develop targeted cyber weaponry. Despite the other strengths noted for the Anticipate function, these two vulnerabilities may allow the threat actor to complete their scoping objectives and progress to the Instigation phase.

Although out of scope to this case study, the ground station's strengths listed above may provide resilience to other threats or potential adversities. As determined in section 2.2, resilience must be aligned to a specific threat and hence can change depending on the type of threat being considered in the scenario. For example, the ground station may be more resilient to physical adversities as compared to cyber-physical adversities.

4.2.3.2.2 Instigation

The second phase of the scenario concerns the initial actions carried out by both the threat actor and the defending ground station system in the lead up to an attack. For the cyber terrorist threat actor this includes activities to compromise the system and pre-position for the final Action on Objectives, including the Delivery, Exploitation, Installation, and Command & Control phases of the CKC, as presented in section 3.3.3.4. At the same time the defending ground station is in Anticipate mode and hence given the opportunity to React to identified malicious activity, such as delivery of malicious code or unexpected privileged activity, and

attempt to contain the threat before any adverse event inflicts impact to the system. These aspects of the CKC are somewhat easier to detect and identify as malicious compared to Reconnaissance activities.

Upon the successful Delivery of cyber weapons developed by the terrorist in the previous stage, the system is deemed compromised and the threat actor is well positioned to escalate their attack through the phases of the CKC. Delivery may involve a complex combination of different threat vectors and attacks and often leads to the installation of malicious code on the system. This allows several opportunities for the threat actor to be detected by the system and the React phase initiated as part of the resilience cycle.

As determined through the Delphi Study process, React refers to the system's ability to avoid, deter, or neutralise detected threats and respond to adverse events. For the ground station system, the following weaknesses in the React function of resilience were identified:

- No OT security
- Inherited ICT infrastructure and governance frameworks with little visibility or control
- No MFA in place.

Offsetting the above weaknesses, certain strengths were also identified for the defending ground station. Each identified strength can be said to limit the opportunities for the cyber threat actor to progress to more advanced stages of the CKC, and include:

- Human factors and safety engineering
- Strong identity and access management practices
- Dedicated cyber incident response
- Cryptography
- Intrusion prevention system for IT
- Anti-malware
- Physical security patrols.

Activities that are conducted as part of the Anticipate function are also required until the threat has successfully been detected and the system can enter the React phase of the resilience cycle. As such, some strengths and weaknesses may carry over from the Scoping stage to the Instigation stage. Accordingly, the following strengths and weaknesses in the ground station's

Anticipate function may be relevant to the successful deployment of React function activities in this case study scenario:

- Strengths
    - Verification and validation
    - Internal and external auditing
    - Intrusion detection system for IT
    - Secure code reviews
    - Data integrity checks.
- Weaknesses
    - Limited supply chain security
    - Inherited ICT infrastructure and governance frameworks with little visibility or control
    - No OT security
    - Some software and devices are COTS and have not been security reviewed
    - Limited cyber security monitoring
    - Limited social engineering awareness training.

From the cyber terrorist threat actor perspective, the Instigation phase is their chance to position themselves for the final cyber-physical attack. From the defending ground station's perspective, the Instigation (i.e., React) phase has only commenced once a threat is detected. The Instigation phase requires the threat actor to deliver malware and other weaponry to the target ground station. Such active techniques are more likely to be detected by the system, especially over an extended period of time. If the threat actor is perceptive, they may notice that they have been detected and quickly move to cause any impact possible to the system before being triaged and losing access.

With intrusion detection and prevention systems in place, as well as data integrity checks, routine auditing, anti-malware, and secure code reviews, it is likely that the ground station will detect threat actor escalation on IT infrastructure during the Instigation phase. The OT network is not secured, however access to the network is primarily through the secured IT network. This leaves two further avenues for the cyber terrorist to explore in their attempts to instigate an adverse event: a supply chain attack or access through an insecure remote access backdoor to OT devices. A supply chain attack may involve the threat actor compromising a supplier to

the ground station, such as a microcontroller manufacturer or a third-party software application provider and installing malicious code before it is installed on the target system. However, these attacks are sophisticated and require long periods of Scoping, and so are more commonly used by nation state threat actors rather than terrorists. Backdoor remote access is commonly configured on OT networks to allow for remote administration and maintenance, particularly on bespoke devices that are sourced through international supply chains. These connections are commonly the entry point for OT system compromise and can often be publicly searched through internet search engines such as Shodan. However, given the overall security posture of the ground station and the strong emphasis on identity and access management, it is likely that these maintenance ports are securely managed. Therefore, there is some possibility that the cyber terrorist threat actor would be able to achieve Command and Control on the ground station, however it is unlikely to be persistent. Persistence, however, is a more desirable objective for nation state actors who are likely to remain in the system for extended periods of time as an APT. In the case of the ground station, a cyber terrorist is likely to complete their Action on Objectives as soon as feasibly possible.

4.2.3.2.3 Adverse Event

In the third phase of the scenario, the cyber terrorist threat actor completes their action on objectives, causing a cyber-physical impact to the system and triggering the Survive and, later, Sustain response from the space system. It is at this stage that the space system's resilience mechanisms that aim to contain the threat and maintain operations in a degraded state are tested.

For the ground station to successfully defend against the cyber terrorist's Action on Objectives, it must be able to Survive (i.e., mitigate, absorb, or withstand the impacts of an adverse event) and Sustain operations (i.e., retain control and preserve core functions and services in a degraded state). In consideration of the analysis at Table 53, the following strengths and weaknesses were noted to be relevant to the Adverse Event stage of the case study scenario:

- Strengths
    - Disaster recovery and business continuity plans are in place
    - Physical hardening
    - High availability systems
    - Redundancy and backups in place for all systems
    - Reliability engineering.

- Weaknesses
    - Limited supply chain security
    - No OT security.

Although it was stated earlier that multiple attacks are common as part of a larger coordinated campaign, for the purposes of this case study only a single attack is considered. This simulates the system's Survive function without the added complexities of resilience cycles occurring simultaneously. An attack that aims to cause a cyber-physical impact to the launchpad would target the OT systems, for which there are no security controls in place to enhance its resiliency. This could mean that the cyber terrorist threat actor is able to achieve their objective of cyber-physical impact, as determined in Table 11.

Upon impact the ground station would seek to initiate Survive activities to mitigate, absorb, or withstand the consequences of the adverse event. Given that the core mission of the ground station is to communicate with space assets through the OT systems, a cyber-physical impact on the OT network could reduce the system's ability to deliver its core services. Without any security controls in place on the OT environment it is likely that any impacts would have enhanced effects and the recovery process may be longer and more complex. However, with high availability redundancies and backups for all systems, the ground station may be able to survive the attack. In order for the threat actor to be successful in degrading the services of the ground station, the attack must be comprehensive enough to target both the live systems and their backups and redundancies. This would require a sophisticated Scoping phase, particularly with respect to the Weaponisation aspects, and is unlikely to be related to a terrorist actor.

Having survived the initial impact, the ground station must now continue to deliver services in a degraded state by utilising activities under the Sustain function. As determined in the interview with the expert participant, the ground station has business continuity plans and disaster recovery processes in place that would be enacted upon impact. These plans and processes likely include a description of the actions to undertake post-incident in order to adhere to the strict high availability requirement. The key vulnerability in the Sustain function is the lack of supply chain security, which in the case of a cyber-physical impact may significantly delay the arrangement of any necessary replacement equipment after the incident; especially if the supply chain crosses national boundaries and also during times of war. This in

turn could interrupt the ground station's ability to continue to provide reliable services in a degraded state.

4.2.3.2.4 Remediation

The fourth and final phase of the scenario refers to the remaining resilience functions of Recover and Adapt. Activities related to these functions are initiated once the immediate impacts have been contained and the system is no longer under direct threat, such as after triage and post-incident reporting. Activities conducted in this phase include restoring the system back to its pre-event baseline and improving the resilience posture based on findings made during the adverse event. The threat actor is no longer considered at this stage in the scenario.

For the ground station, the following weaknesses in the Recover and Adapt functions of resilience were identified and are relevant to this scenario:

- Limited cyber risk management
- No OT security
- Immature cyber security culture
- Inherited ICT infrastructure and governance frameworks with little visibility or control
- Limited supply chain security.

By contrast, the following relevant strengths in the Recover and Adapt functions of resilience were identified for the ground station:

- Insurance
- Backups for all systems
- Strong data management practices
- Dedicated cyber security and governance roles
- Strong general security culture with a high availability mindset
- Strong policies in place.

In light of the above, the ground station system is likely to be able to be restored back to a previous state that was stored and documented prior to the adverse event. Depending on the level of insurance coverage, any economic impacts of the adverse event are also likely to be minimised. A good security culture will minimise social impacts to the Human Segment, in that there will be an increased emphasis on recovery rather than blame; even if the cyber

security aspects of the culture are still developing. Finally, as far as strengths are concerned, dedicated cyber security and governance roles accompanied by strong policies will allow for the ground station to Recover and Adapt using a structured and formally managed approach.

However, remediation efforts may be hampered by a lack of recovery processes on the OT network and limited risk management practices. Risk management allows for accurate communication and prioritisation of restoration and adaptation functions based on criticality. A lack of pre-existing processes and risk tolerance definition may hinder post-incident communication and slow the restoration process, thus extending the impact of the adverse event. Without OT recovery processes and procedures the full system restoration may also be slowed down with specific components or subsystems potentially deemed irrecoverable. This impact may also be exacerbated by the limited supply chain assurance. Finally, being connected to Government systems and networks, the response and recovery processes would likely be delayed by reporting and bureaucratic requirements due to the potential for cross-domain impacts to official data.

4.2.3.3 Space Vehicle and Payload

The space vehicle and payload, also referred to as the space asset, is perhaps the most recognisable space system. For the purposes of the case study, a generalised space asset was utilised with the cases for both individual payloads and constellations being considered in the resilience outcomes. The technologies that form the space asset in this case study include an IoT device, such as a Raspberry Pi, with an onboard processor that transmits and receives signals via the RF link to the ground station. Another example target on the space vehicle is the electricity system or spacecraft propulsion systems. These are cyber-physical systems that could be targeted by a cyber threat actor to cause a physical impact to the system and affect its availability. This section will simulate a cyber-physical attack against the space asset by a cyber terrorist actor, via a compromised ground station, with the goal to disable the asset.

Although no individual interview was conducted with an expert participant regarding the space vehicle and payload system, enough data was gathered through the other respective interviews in order to build a theoretical picture of the security and resilience status for the purposes of the case study. The data collected during these interviews, as captured in Table 49, was distilled into specific strengths and weaknesses in Table 54. This table provides a preliminary analysis of the space system's security and resilience posture. Without compensatory controls, specific

weaknesses may be exploited by the threat actor in pursuit of their objectives (see Table 11 for further detail on the cyber terrorist threat actor's defining features and objectives for the case study).

	Governance Segment	Human Segment	Ground Segment	Space Segment	C3 Segment (focused on space)
Non-Malicious	**Strengths** Adherence to strict legal and regulatory requirements. **Weaknesses** Business continuity and disaster recovery differs depending on the services delivered by the payload. Poor product assurance and limited V&V for many payloads. Space DevOps being developed.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.	**Strengths** A lot done well to protect against environmental adversities such as space debris and radiation. **Weaknesses** No specific weaknesses noted.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.
Cyber	**Strengths** No specific strengths noted. **Weaknesses** Little to no consideration of cyber security on the space vehicle post-launch.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.	**Strengths** No specific strengths noted. **Weaknesses** IoT devices often sent up as part of payload without secure practices. No anti-malware or IDS/IPS. Inherited vulnerabilities from COTS.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.
Electro-magnetic	**Strengths** Spectrum regulation and adherence to legal and regulatory requirements. **Weaknesses** Limited EW consideration in processes.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.	**Strengths** No specific strengths noted. **Weaknesses** Limited counter-EW technologies.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.

Kinetic	**Strengths** No specific strengths noted. **Weaknesses** No specific weaknesses noted.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.	**Strengths** No specific strengths noted. **Weaknesses** Some hardening of space hardware but nothing that could withstand a malicious kinetic attack.	**Strengths** Inherited from the ground station system security. **Weaknesses** Inherited from the ground station system security.

Table 54 – Space Vehicle and Payload Resilience Data

Resilience strengths that were identified through the interview process can be noted to assess aspects of the system that enhance its resilience to adversities. In reference to Table 54, the following high-level resilience strengths were identified in the interview data for the space vehicle and payload:

- General strengths in resilience:
    - Good protection against environmental adversities such as space debris and radiation.
- Strengths in resilience specific to cyber adversities:
    - No specific strengths noted.
- Strengths in resilience specific to electromagnetic adversities:
    - Spectrum regulation.
- Strengths in resilience specific to kinetic adversities:
    - Some physical hardening.

Resilience weaknesses that were identified through the interview process can be noted to assess aspects of the system that may be vulnerable to adversities. Vulnerabilities in resilience posture can be exploited by adversaries to cause greater, and perhaps irrecoverable, damage, such as the cyber-physical terrorist threat defined by the case study threat model. In reference to Table 54, the following weaknesses were identified in the resilience data for the space vehicle and payload:

- General weaknesses in resilience:

    - Business continuity and disaster recovery differs depending on the services delivered by the payload. For example, a satellite constellation may have a greater business continuity capability compared to a single CubeSat or rover.
    - Poor product assurance and limited V&V.
- Weaknesses in resilience specific to cyber adversities:
    - Little to no consideration of cyber security on the space vehicle post-launch
    - IoT devices without secure practices
    - No anti-malware
    - No onboard IDS or IPS
    - Inherited vulnerabilities from COTS.
- Weaknesses in resilience specific to electromagnetic adversities:
    - Inherited vulnerabilities from COTS
    - Limited counter-EW technologies.
- Weaknesses in resilience specific to kinetic adversities:
    - Some hardening of space hardware but nothing that could withstand a malicious kinetic attack.

The identified relevant strengths and weaknesses can be rearranged into the taxonomical pillars of space systems resilience, as determined in section 4.1.4.3. Rearranging the strengths and weaknesses in this manner provides a resilience lens on the security controls identified through use of the space systems security knowledge domain table. For the purposes of this case study exercise, only the strengths and weaknesses identified to be relevant to the cyber terrorist scenario are represented in Table 55 below.

Resilience Function	Strengths	Weaknesses
Anticipate – the system's ability to maintain situational awareness and proactively detect potential threats.	• Collision avoidance (COLA) systems in use.	• No security monitoring of payload or comms link.
React – the system's ability to avoid, deter, or neutralise detected threats and respond to adverse events.	• No specific strengths noted.	• IoT devices in payload without secure practices • Limited counter-EW technologies • No onboard IDS or IPS.

Survive – the system's ability to mitigate, absorb, or withstand the impacts of an adverse event.	• Some physical hardening • A constellation system may be able to absorb the impacts of individual space asset losses.	• Some hardening of space hardware but nothing that could withstand a malicious kinetic attack • No anti-malware.
Sustain – the system's ability to retain control and preserve core functions and services in a degraded state.	• No specific strengths noted.	• Poor product assurance testing • A system that relies on a single space asset to achieve the mission may not survive a cyber-physical impact.
Recover – the system's ability to respond, restore operations, and 'bounce back' from adverse events.	• No specific strengths noted.	• If the space asset is lost then a replacement system needs to be launched.
Adapt – the system's ability to evolve based on threat intelligence and lessons learned to better anticipate, react, survive, sustain and recover from future adverse events.	• No specific strengths noted.	• Space assets rarely allow for remote updates and software modifications to adapt to the changing threat environment.

Table 55 – Space Vehicle and Payload Resilience Strengths and Weaknesses

4.2.3.3.1 Scoping

The first phase of the case study threat scenario involves scoping activities conducted by both the cyber terrorist threat actor and the defending launchpad mission control system. In this phase the cyber terrorist actor conducts Reconnaissance and Weaponisation in line with the CKC model presented in section 3.3.3.4. At the same time, the space vehicle should carry out activities related to the Anticipate function of the resilience model.

As noted in Table 54, the Ground, Human, and C3 segments of the space system are inherited from the ground station. The most obvious way to attack the space vehicle is through the ground station communications channel. In order to do this the cyber terrorist threat actor must first compromise the ground station before they are able to gain access to the space vehicle and deliver a cyber-physical impact. The resilience strengths and weaknesses of the ground station, as well as a theoretical playthrough of the cyber terrorist threat scenario, are explored in the case study at section 4.2.3.2. A second method of compromising the space vehicle is through

the supply chain, where malicious software or hardware can be embedded in the payload prior to launch. This is an advanced attack that requires a great deal of forward planning and logistical power, and hence is more viable when modelling a nation state actor rather than a cyber terrorist actor. Therefore, for the purposes of this case study, only the first scenario will be considered using the available data and completed case study of the ground station system. The remainder of the space vehicle and payload case study assumes the successful compromise of the ground station.

Threat actor reconnaissance involves vulnerability scanning and social engineering techniques to identify weaknesses in the space vehicle that could be exploited in pursuit of the final objective to impact the control and/or services of the payload. During this period of time the cyber terrorist threat actor is collecting intelligence about their intended target and method of attack to achieve their overarching objectives, as determined in Table 11. As this occurs, the space vehicle should conduct resilience activities to Anticipate the cyber terrorist's scoping activities.

As determined through the Delphi Study process, Anticipate refers to the system's ability to maintain situational awareness and proactively detect potential threats. For the space vehicle and payload, one major weakness was identified in the Anticipate function of resilience; there is no security monitoring of the payload or communications link to the space vehicle. This allows for cyber threat actors with persistent access to the system to conduct Scoping activities without risk of detection. Another method to gain intelligence on the space vehicle is through social media monitoring and social engineering techniques to identify components and technologies that may offer leverage for the attack. Combined, these two methods allow the cyber terrorist threat actor to successfully complete the Weaponise objectives in the CKC.

4.2.3.3.2 Instigation

The second phase of the scenario concerns the initial actions carried out by both the threat actor and the space vehicle or payload in the lead up to an attack. For the cyber terrorist threat actor this includes activities to compromise the system and pre-position for the final Action on Objectives, including the Delivery, Exploitation, Installation, and Command & Control phases of the CKC, as presented in section 3.3.3.4. At the same time the defending space asset is in Anticipate mode and hence given the opportunity to React to identified malicious activity, such

as delivery of malicious code, and attempt to contain the threat before any adverse event inflicts damage to the system.

Upon the successful Delivery of cyber weapons developed by the terrorist in the previous stage, the space vehicle is deemed compromised and the threat actor is well positioned to escalate their attack through the phases of the CKC. As determined through the Delphi Study process, React refers to the system's ability to avoid, deter, or neutralise detected threats and respond to adverse events. For the space vehicle and payload, the following weaknesses in the React function of resilience were identified:

- IoT devices in payload without secure practices
- No onboard IDS or IPS.

The combined lack of intrusion detection with insecure IoT devices provide the threat actor with an undetectable and easily accessible escalation path. IoT devices offer various channels of connectivity and are commonly developed using COTS products such as the Raspberry Pi, which allow for ease of attack simulation prior to the Action on Objectives. In essence, once the threat actor gains access to the space vehicle and payload, there are few mechanisms in place to prevent further compromise and escalation on the platform.

4.2.3.3.3 Adverse Event

In the third phase of the scenario, the cyber terrorist threat actor completes their action on objectives, causing a cyber-physical impact to the system and triggering the Survive and, later, Sustain response from the space system. It is at this stage that the space system's resilience mechanisms that aim to contain the threat and maintain operations in a degraded state are tested.

For the space asset to successfully defend against the cyber terrorist's Action on Objectives, it must be able to Survive (i.e., mitigate, absorb, or withstand the impacts of an adverse event) and Sustain operations (i.e., retain control and preserve core functions and services in a degraded state). In consideration of the analysis at Table 53, the following strengths and weaknesses were noted to be relevant to the Adverse Event stage of the case study scenario:

- Strengths
    - Some physical hardening

    - A constellation system may be able to absorb the impacts of individual space asset losses.
- Weaknesses
    - No anti-malware
    - Poor product assurance testing
    - A system that relies on a single space asset to achieve the mission may not survive a cyber-physical impact.

Given the above strengths and weaknesses, it is likely that the cyber terrorist threat actor would be able to infect the space vehicle or payload with malware such as ransomware and the space asset would not be able to defend itself. Additionally, with a lack of product assurance testing the response of the system may be unknown, delivering unforeseeable flow-on effects and secondary impacts.

In this scenario, a single damaged asset that is part of a wider constellation may not impact the wider space system or the availability of its services. However, depending on how the attack is conducted, it may be plausible that multiple space assets are affected by the attack, which could cause flow-on impacts to the services. A cyber-physical impact on a single space asset, such as a rover or a scientific satellite used for data collection, could cause complete service failure, and deliver irrecoverable damage to the space asset.

4.2.3.3.4 Remediation

The fourth and final phase of the scenario refers to the remaining resilience phases of Recover and Adapt, which take place after the threat actor has completed their attack, any cascading impacts have been contained, and the system is no longer under direct threat. Activities conducted in the phase include restoring the system back to its pre-event baseline and improving the resilience posture based on findings made during the adverse event.

For most space vehicles that have sustained heavy cyber-physical damage, it will be necessary to physically replace the vehicle and payload in order to recover the services. Space assets rarely allow for remote updates and software modifications to adapt to the changing threat environment. The resilience of this aspect of the system would depend on the ability to relaunch a replacement at short notice. Supply chain considerations would be a fundamental component of this aspect of the resilience assessment. At this point it should also be noted that the space

vehicle inherits the security and resilience strengths and weaknesses of the launchpad and its mission control system, as detailed in the case study at section 4.2.3.1.

4.2.4 Case Study Outcomes

The case study analysis completed for the launchpad mission control, ground station, and space vehicle provided insights into the varying strengths and weaknesses in resilience to cyber-physical adversities for each respective space system. Based on the data collected through the interview process, high-level controls were identified using the space systems security domain developed in section 4.1.2. This data provided insight into threat-specific countermeasures that may enhance the resilience posture of the system in question. The case study tested the systems' resilience posture using a threat model of a cyber terrorist actor seeking to cause cyber-physical impact to the system. The resilience outcomes of each system are discussed in this section, with particular reference to the performance of the resilience assessment framework developed through the Delphi study.

Additionally, through analysis in the previous section, a number of findings were made that either raised the need for additional modifications to be made to the resilience assessment framework or were otherwise identified as important findings that deserve emphasis in this section. All findings and resulting outcomes of the case study, including from the interviews and the case study threat scenario analysis, are detailed in the section. Outcomes are grouped according to the space system against which the scenario was tested.

4.2.4.1 Launchpad Mission Control

The first case study scenario was conducted based on the interview data for a launchpad mission control system, for which the cyber-physical components include the communications equipment and space system launchpad. Hence, the cyber terrorist threat actor scenario involved the experimental simulation of a cyber-physical attack against these components. The scope of the study included the broader system outside of these components, including across the Governance, Human, Ground, and C3 segments of the system. The Space segment was out of scope to the scenario and was instead tested as a separate case study in section 4.2.3.3.

Breaking the overall assessment down provides a stage-by-stage understanding of the launchpad mission control system's resilience to cyber-physical threats. During the Scoping stage of the scenario several weaknesses were identified, including a lack of security assurance

or monitoring and very limited security personnel. It was therefore concluded that Reconnaissance and Weaponisation activities conducted by the threat actor have the potential to go undetected or unactioned, meaning that the system was unlikely to enable the React function of the resilience cycle early in the threat actor's attack. Additionally, the OT systems are not being monitored or secured in any way, leaving the cyber-physical components of the system vulnerable to Scoping activities.

The Instigation stage determined that the launchpad mission control possesses several weaknesses to threat actor escalation, including insecure OT systems, supply chain weaknesses, a lack of encryption, and a lack of assurance activities, as well as no incident response plan or risk management activities. In combination, this resulted in the system being slow to detect or prevent threat actor escalation through the CKC, and slow to respond once detected. Additionally, it was found that these weaknesses could enhance the cyber-physical adversity due to the heightened potential for increased consequences and prolonged impact in the next stage.

In the Adverse Event stage it was determined that even if the threat is detected, it is likely that an impact will still occur to the system due to the limited response mechanisms in place. As such, the case study considered the following two scenarios:

1. The threat actor is successful in their Action on Objectives and the launchpad is rendered inoperable at the time of launch due to cyber attack, deeming the launch operation a failure.
2. The threat actor is detected before completing their Action on Objectives and the impact is delivered prior to the time of launch, allowing time for the launchpad to prove resilient and sustain operations in a degraded state.

In the first scenario, the system was shown to not be resilient to cyber-physical attacks because it failed to maintain control and deliver its core services. Due to the lack of incident response and security assurance processes, the impacts to the system were also both heightened in damage and lengthened in time. In the second scenario, the system was shown to have a level of resiliency due to the high redundancy of networks and devices. However, with no disaster recovery or incident response processes in place, and limited supply chain assurance or OT security, the system was found to be at risk of remaining unserviceable for extended periods of time. Therefore, the IT and communications aspects of the launchpad mission control system

were found to have moderate levels of resilience but the OT network, which was targeted by the threat actor, was demonstrated to have low levels of resilience to cyber-physical threat.

The final stage of the scenario involved Remediation, which tested the Recover and Adapt phases of the resilience cycle. Overall, it was found that the launchpad mission control system is likely to be able to be restored after an adverse event and some impacts may be minimised by insurance and a good security culture. This ensures that if the system were to survive the cyber-physical adversity, it would be able to "bounce back". However, it was also noted that remediation efforts may be hampered by the lack of recovery processes and risk management methodologies.

Taking into account the analysis in section 4.2.3.1 and the summary above, it can be said that the launchpad mission control system has a medium to high level of resilience in the IT network, but a low to medium level of resilience in the OT network. Given that the threat actor in the case study threat model was a cyber-physical terrorist, the OT network would be the primary target of the attack. Hence the launchpad mission control system can be said to have a low to medium overall level of resilience to cyber-physical adversities; particularly in a malicious context. The assessed level of resilience could be made more specific with lower-level data surrounding the security controls in place on the system, however this case study was purposely kept at a high-level to minimise any security concerns or the release of corporate information.

In addition to the above outcomes, additional findings were made regarding the resilience framework developed through the Delphi study process. All findings resulting in modifications to the framework are detailed in Table 56 below.

Ref	Modifications
C01	Add 'Insurance' to the Governance segment of the space systems security knowledge domain table.
C02	Add 'Public Relations' to the Governance segment of the space systems security knowledge domain table.

Table 56 - Case Study Outcomes for the Launchpad Mission Control

The modification documented at C01 of Table 56 above arises from the interview of the first case study participant, where it was identified that insurance was not previously raised by the Delphi study process; as recorded in the below snippet from the transcript:

> Expert Respondent: "The big one would be insurance."
>
> Interviewer: "Oh yeah, of course. Yeah. That's another one that wasn't captured by the Delphi process."
>
> Expert Respondent: "Yeah, the amount of insurance we're having to get, I don't know the specifics, but it's lots and it's, yeah, it lands on someone's house and kills someone…"

A second aspect that was identified to be missing from the framework was communications and public relations to minimise political, social, economic, or psychological impacts outside the system's boundary. A security-aware communications team was determined to be required post-incident to counter any negative perceptions among the public about the event and minimise any flow-on effects, particularly in relation to reputation management and maintaining a level of public and government trust. This finding resulted in a modification to the space systems security knowledge domain, as documented at C02 of Table 56 above.

The first iteration of the case study scenario also demonstrated that a threat-driven methodology can lead to the resilience phases being enacted non-homogenously. For example, React should only be triggered after a threat has been detected, however in this scenario both the React and Anticipate functions were analysed simultaneously in case the threat had not yet been detected. This is not the same for React and Survive because the adverse impact, being a cyber-physical one, should be detected almost immediately. However, it does mean that the way the system perceives the adverse event and stage of attack may not be directly correlated to the phase of the CKC as perceived by the threat actor. In this way, a system with weaknesses in the Anticipate function may not have the ability to React before the Survive function is initiated. This is a symptom of a system that lacks resilience.

A final note regarding the launchpad mission control case study can be made based on the following excerpt from the interview: "Pre-launch, everyone gets jittery. Post-launch, all of a sudden no one cares." This quote provides an time-based element to security and resilience, where the confidentiality of a space system may be required for short periods of time only.

4.2.4.2 Ground Station

The second case study scenario was conducted based on the interview data for a ground station system, for which the cyber-physical components primarily refer to the communications equipment. Hence, the cyber terrorist threat actor scenario focused on the experimental simulation of a cyber-physical attack against these components. However, the scope of the study also included the broader system, including the Governance, Human, Ground, and C3 segments. The Space segment was out of scope to the scenario and was instead tested as a separate case study in section 4.2.3.3.

Breaking the overall assessment down provides a stage-by-stage understanding of the ground station's resilience to cyber-physical threats. During the Scoping stage of the scenario it was determined that the ground station system is especially vulnerable to scoping activities conducted by the terrorist threat actor. This was identified to be due to limited cyber security monitoring and social engineering awareness training, as well as a lack of supply chain security combined with the use of COTS and inherited infrastructure. Additionally, the OT systems are not being monitored or secured in any way, leaving the cyber-physical components of the system especially vulnerable to Scoping activities conducted by the threat actor.

The Instigation stage of the scenario determined that it is likely that the ground station will detect threat actor escalation on IT infrastructure during the Instigation phase, however with no OT security in place the same is not true for the cyber-physical systems. Two avenues were identified outside the secured IT systems for the cyber terrorist to instigate an adverse event: a supply chain attack and a potential insecure remote access backdoor to OT devices. Supply chain attacks were determined to be more of a nation state tactic rather than a typical terrorist tactic, however backdoor remote access is commonly configured on OT networks and so was deemed to be more viable for the terrorist actor. However, given the overall security posture of the ground station and the strong emphasis on identity and access management, it was found that the cyber terrorist threat actor could achieve Command and Control on the ground station, albeit only for a limited period of time.

In the Adverse Event stage it was determined that a cyber-physical impact on the OT network could reduce the system's ability to deliver its core services. However, with high availability redundancies and backups for all systems, the ground station was found to be able to survive

the attack. It was also noted that without any security controls in place on the OT environment and poor supply chain security, cyber-physical impacts could have enhanced effects and a longer and more complex recovery process. Post-impact, the ground station was well positioned to operate at a reduced capacity, with business continuity plans and disaster recovery processes in place that would be enacted upon impact.

The final stage of the scenario involved Remediation, which tested the Recover and Adapt phases of the resilience cycle. Overall, it was found that the ground station is likely to be able to be restored after an adverse event with some impacts minimised by insurance, a good security culture, and dedicated security positions. This ensures that if the system were to survive the cyber-physical adversity, it would be able to "bounce back". However, it was also noted that remediation efforts may be hampered by the lack of OT recovery processes and risk management methodologies, as well as supply chain assurance concerns and any consequences of government network interconnectivity.

Taking into account the analysis in section 4.2.3.2 and the summary above, it can be said that the ground station system has a high level of resilience in the IT network and a medium level of resilience in the OT network. Given that the threat actor in the case study threat model was a cyber-physical terrorist, the OT network would be the primary target of the attack. Hence the launchpad mission control system can be said to have a medium overall level of resilience to cyber-physical adversities; particularly in a malicious context. The assessed level of resilience could be made more specific with lower-level data surrounding the security controls in place on the system, however this case study was purposely kept at a high-level to minimise any security concerns or the release of corporate information.

In addition to the above outcomes, additional findings were made regarding the resilience framework developed through the Delphi study process. All findings resulting in modifications to the framework are detailed in Table 56 below.

Ref	Modifications
C03	Add 'Organisational Culture' to the human segment of the space systems security knowledge domain table

Table 57 - Case Study Outcomes for the Ground Station

The modification documented at C03 of Table 57 above arises from the interview of the second case study participant, where it was identified that there are different aspects of the culture that should be acknowledged in the framework; as recorded in the below snippet from the transcript:

> Expert Respondent: "Yeah, cause the non-malicious, as you said, it's more of a safety culture. And you know, you're talking about non-malicious adversities. So, the things that you can't stop. You can pick on the fire and the flood and the other types of events, and they have a very strong culture to get the system back online. Whereas cyber is new. It really is quite new to them. But they're having to learn really fast."

This observation regarding security culture can be broadened to organisational culture, whereby the general culture surrounding the Human segment can have profound effects on the system's level of resilience. For example, a poor organisational culture may lead to blame shifting and limited accountability, which can conversely lead to insecure practices and 'evidence hiding' as well as disorganisation and lack of responsibility during an adverse event and remediation. On the other hand, a mission-oriented culture may operate a more resilient system where accountability is valued, and the core focus is service availability rather than office politics.

Another noteworthy finding, although not leading to any modifications, is that a system may be resilient to a majority of threats but vulnerable to a small number of attack vectors, such as supply chain and cyber-physical attacks. In the case of the ground station, the assessment may have demonstrated strong resiliency against most cyber attacks. However, the weak point in the expansive security controls related primarily to the cyber-physical systems, and so the ground station was assessed as significantly less resilient to a cyber-physical attack.

4.2.4.3 Space Vehicle and Payload

The final case study scenario was conducted based on aspects of the interview data for the other two systems that were found to be relevant to the space vehicle and payload. The scope of this case study was limited to the Space and C3 segments and was conducted as a cyber-physical terrorist threat scenario against a generic IoT-enabled space asset. This was necessitated due to the lack of specificity in the interviews regarding the type of space vehicle or payload. Interview excerpts that are relevant to this section are detailed in section 4.2.2.3 and provide the basis of the experimental analysis in section 4.2.3.3.

For the Scoping stage of the scenario, it was determined that a threat actor seeking to achieve Reconnaissance and Weaponisation objectives on the space vehicle and payload would likely be successful. The lack of onboard security monitoring or communications link monitoring or integrity checking allowed for the cyber threat actor to conduct Scoping activities without risk of detection by the Anticipate function.

The Instigation stage of the scenario determined that the combined lack of intrusion detection with insecure IoT devices provide the threat actor with an undetectable and easily accessible escalation path through the CKC. In essence, once the threat actor gains access to the space vehicle and payload, there are few React mechanisms in place to prevent further compromise and escalation on the platform.

In the Adverse Event stage it was determined that even if the threat was detected, the cyber terrorist threat actor would be able to infect the space vehicle or payload with malware and the space asset would not be able to defend itself. In this scenario, a space system comprising a single damaged asset that is part of a wider constellation may yet Survive and prove resilient, depending on the scale of the attack as well as the resilience architecture (i.e., D4P2 as per R053 in Table 19). However, a cyber-physical impact on a solitary space asset, such as a rover or a scientific satellite, could cause irrecoverable damage and may hence be deemed not resilient to cyber-physical adversities. The level of resilience in these situations should be linked back to the overall system objective that the space asset was contributing to, and whether or not it is still able to be achieved.

The final stage of the scenario involved Remediation, which tested the Recover and Adapt phases of the resilience cycle. The system's resilience after a successful cyber-physical attack against the space asset was found to depend, in addition to the D4P2 architectural considerations, primarily on its supply chain and ability to relaunch a replacement payload at short notice. It was also noted that the space vehicle inherits security and resilience strengths and weaknesses from the ground station and mission control system.

Taking into account the analysis in section 4.2.3.3 and the summary above, it can be said that the generic space asset has little to no inherent resilience to cyber-physical attacks, with all aspects of its resiliency relying on its ability to rapidly relaunch. However, the larger space system, including other space vehicles and terrestrial components, may gain overall resilience

through other measures, such as D4P2, which will enhance the system's ability to React, Survive, and Sustain.

No additional findings were made regarding the resilience framework that required modifications or additions to be made. However, it was demonstrated that the space systems resilience framework can be scaled to suit what is deemed in scope of the assessment. For example, the framework can be utilised to assess the resilience of a single space asset as well as taking the broader 'system of systems' approach to assess the overall resilience of the services.

4.3 Summary of Study Outcomes

The aim of the case study was to theoretically validate the research outcomes arising from the Delphi study by testing the resilience framework against real-world space systems. This was achieved by modelling the threat defined in section 3.3.3.3, using the CKC, against space systems whose security and resilience was determined through two separate interviews, as documented in section 4.2.2.

The Delphi study resulted in the following five primary outcomes, as summarised at Table 60 and visually represented in Figure 36 and Figure 37:

- PRO-2: A contemporary definition for 'Space Systems Security'.
- PRO-3: A comprehensive scope of the space security domain encompassing both functional and adversarial factors.
- PRO-4: A taxonomical catalogue of space systems resilience.
- PRO-5: A contemporary definition for 'Space Systems Resilience'.
- PRO-6: A functional model representing both phasal and temporal requirements to attain resiliency in a space system and taking into account both technical and non-technical aspects.

The approach to the case study scenario is detailed in Figure 32 and summarised below:

1. Scoping, including all scoping activities conducted by both the threat actor and the defending space system.
2. Instigation, which concerns the initial actions carried out by both the threat actor and the defending space system in the lead up to an attack.

3. Adverse Event, which simulates a cyber-physical impact to the system and triggers the Survive and Sustain response from the space system.
4. Remediation**,** including the remaining resilience phases of Recover and Adapt, which include restoring the system back to its pre-event baseline and improving the resilience posture based on findings made during the adverse event.

At each of the four stages outlined above, the threat actor's actions were theoretically simulated against each of the three space systems, as detailed by the case study expert participants, with potential outcomes being modelled based on gaps in resilience posture identified through the interviews.

The case study concluded that the launchpad mission control system had a low level and the ground station a low to medium level of resilience to cyber-physical attacks, both primarily due to a lack of OT security in place on the cyber-physical systems. The space asset itself was found to have little to no inherent resilience to a cyber-physical attack, but may prove resilient as part of a larger constellation. Additionally, modifications were made to the space systems knowledge domain table, which are summarised in Table 58 below.

Ref	Modifications
C01	Add 'Insurance' to the Governance segment of the space systems security knowledge domain table.
C02	Add 'Public Relations' to the Governance segment of the space systems security knowledge domain table.
C03	Add 'Organisational Culture' to the human segment of the space systems security knowledge domain table

Table 58 – Summary of Case Study Outcomes

Overall, and after the modifications noted above, it was determined that the space systems security knowledge domain is comprehensive, and the resilience framework is functional. The framework was able to be successfully applied to three different systems using a consistent threat model and a repeatable methodology regardless of size or complexity of the system. This outcome accomplishes the final primary objective, PRO-7, summarised at Table 60 and visually represented in Figure 36 and Figure 37. It should be noted that the framework was only tested against cyber-physical threats using high-level security control data.

5 Discussion

5.1 Chapter Introduction

In setting out to undertake the research described in this dissertation, three over-arching research goals were agreed on to help guide the study and its outcomes.

1. Research Goal 1: An experimental evaluation of the research related to space systems security to determine the scope of the domain and theories on the space-cyber threat environment.

2. Research Goal 2: An ontological discovery and taxonomical catalogue of space systems resilience for the purposes of resilience assessment by space systems security practitioners.

3. Research Goal 3: A space systems resilience framework, based on the outcomes of the ontological discovery exercise, for determining the high-level resilience status of a given space system to a malicious cyber-physical threat.

Having completed the study, these research goals can be re-framed into research outcomes. Each research outcome represents a unique contribution to academia and the space and security communities more broadly. The outcomes of the research described in this dissertation can be split into two general categories:

1. Primary research outcomes (PRO), and
2. Secondary research outcomes (SRO).

Primary research outcomes include those outcomes that are directly related to the research goals stipulated above. These are anticipated outcomes of the study and represent the key findings that would be expected when undertaking this body of work. All primary research outcomes have been verified through expert feedback via the Delphi Study and validated, where feasible, through the case study on real-world operational space systems. Primary research outcomes contribute new knowledge to the space security discipline and the space and security communities more broadly. The primary research outcomes arising from the research detailed in this dissertation are listed in Table 59 below.

Ref	Primary Research Outcomes
PRO-1	A comprehensive evaluation of existing and tangential research related to space systems security and resilience.
PRO-2	A contemporary definition for ‘Space Systems Security’.
PRO-3	A comprehensive scope of the space security domain encompassing both functional and adversarial factors.
PRO-4	A taxonomical catalogue of space systems resilience.
PRO-5	A contemporary definition for ‘Space Systems Resilience’.
PRO-6	A functional model representing both phasal and temporal requirements to attain resiliency in a space system and taking into account both technical and non-technical aspects.
PRO-7	A space system resilience assessment framework to assess the high-level resilience status to any given threat and aid in identifying high level security and resilience control gaps.

Table 59 - Primary Research Outcomes

Secondary research outcomes are indirectly related to the research goals stipulated above. These outcomes were not specifically identified at the onset of the study and were not initially expected as research findings when undertaking this body of work. Secondary research outcomes contribute new knowledge to the security community more broadly, namely in the disciplines of power systems resilience and cyber terrorism prevention and enforcement. The secondary research outcomes arising from the research described in this dissertation are detailed in Chapter 2 and summarised in Table 60 below.

Ref	Secondary Research Outcomes
SRO-1	A comprehensive evaluation of existing and tangential research related to power systems and critical infrastructure resilience.
SRO-2	A taxonomical catalogue of power systems resilience.
SRO-3	A homogenised definition for ‘Power Systems Resilience’.
SRO-4	A functional model representing both phasal and temporal requirements to attain resiliency in a power system and taking into account both technical and non-technical aspects.
SRO-5	A comprehensive evaluation of existing research related to cyber terrorism.
SRO-6	A taxonomical catalogue of the features inherent to cyber terrorism.
SRO-7	A homogenised definition for ‘Cyber Terrorism’.

Table 60 - Secondary Research Outcomes

The secondary research outcomes were necessarily produced in pursuit of the three specified research goals due to gaps in resilience and cyber-physical threat literature that underpin the

space systems security study. For example, due to the lack of existing literature on security resilience in the space systems domain, the study required that the resilience model of an alternate but comparable system be utilised as a starting point. Power systems resilience was identified as a viable candidate upon which to model space systems resilience, as detailed in Section 2.2. As such, it was first required to leverage existing power systems resilience literature to develop a comparable resilience model to that outlined in the research goals. Cyber terrorism, on the other hand, was investigated as part of activities required to develop the threat model for the case study. This was due to the reason that cyber terrorism represented the ideal threat case for testing the extremities of the resilience model to provide for more robust research outcomes, as discussed in Section 2.3.3.

The relationship between research outcomes, including both primary and secondary research outcomes, is illustrated in Figure 36. The figure demonstrates how secondary research outcomes shaped the results of the primary research outcomes, as well as highlighting the interrelationships between each individual outcome noted in Table 59 and Table 60.

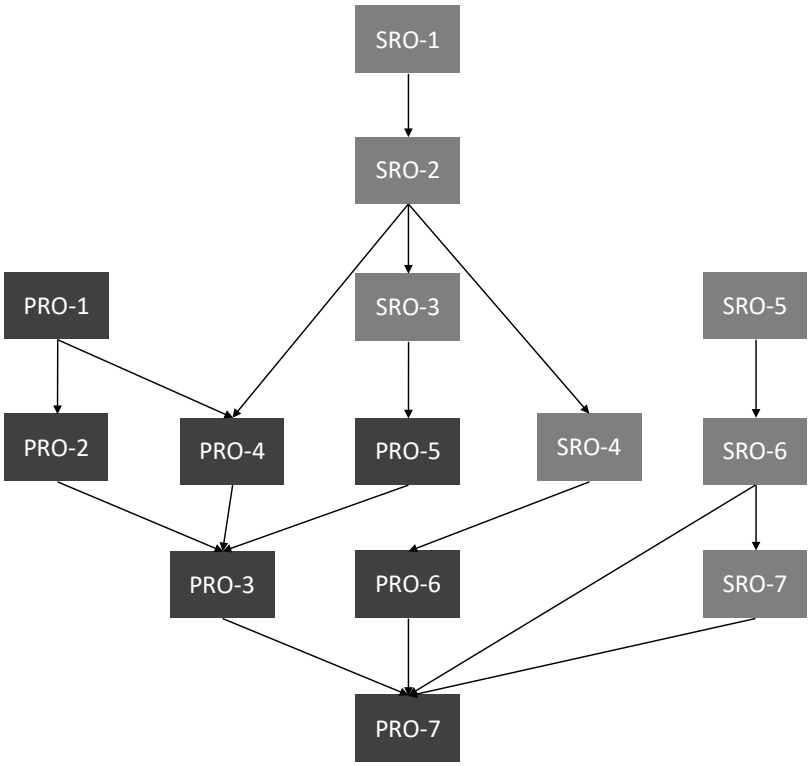

Figure 36 - Research outcomes and their interrelationships

This relationship can also be demonstrated in relation to each research goal, as depicted in Figure 37 below.

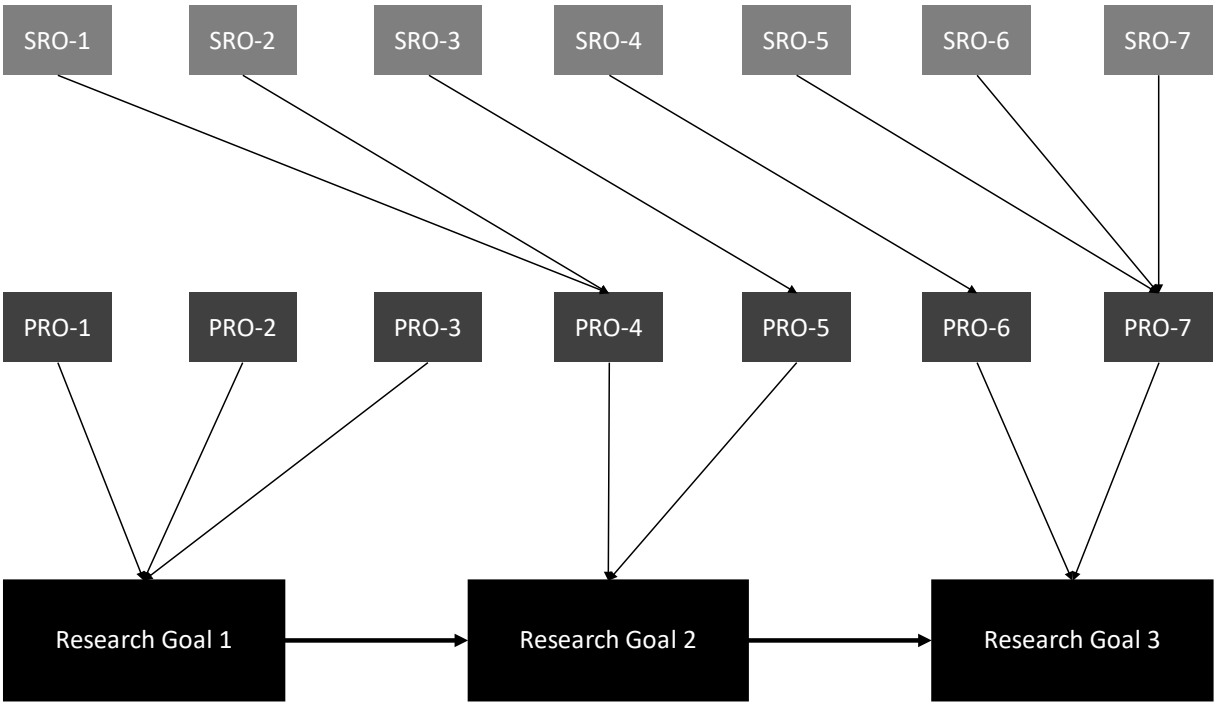

Figure 37 - Research Outcomes mapped to Research Goals

Figure 37 above provides a mapping between the research goals and the research outcomes. A discussion of how each research goal has been achieved by the research outcomes, as depicted in the figure, is provided in detail in the sections below.

5.2 Research Goal 1 – Space Systems Security Domain Mapping

At the commencement of the research project detailed in this dissertation, Research Goal 1 was defined as "an experimental evaluation of the research related to space systems security to determine the scope of the domain and theories on the space-cyber threat environment". As shown in Figure 37, Research Goal 1 feeds into Research Goal 2 and comprises of the following primary and secondary research outcomes (as detailed in Table 59 and Table 60):

- PRO-1: A comprehensive evaluation of existing and tangential research related to space systems security and resilience.
- PRO-2: A contemporary definition for 'Space Systems Security'.

- PRO-3: A comprehensive scope of the space security domain encompassing both functional and adversarial factors.

Research related to space systems security and the space-cyber threat environment was explored in Chapter 2. The initial scope of space systems security was determined through the three dimensions of space security proposed by Mayence (2010), as shown below:

1. security in space (i.e., protecting space systems);
2. space for security (i.e., military space operations); and
3. security from space (i.e., protecting Earth from space-based threats).

The first of the three dimensions above was identified as the differentiating factor of space systems security as compared to other domains of space security. This knowledge was then paired with Moltz's definition to develop a preliminary definition and domain scope for space systems security. Moltz defined space (systems) security as, "the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction" (Moltz 2011). This preliminary definition was then presented to two dozen space systems security experts around the world to obtain iterative feedback on improvements and modifications over three rounds through the Delphi methodology, as detailed in section 3.3.2. The expert feedback, including a final expert focus group to confirm the findings, was analysed in section 4.1 to identify iterative modifications and improvements until group consensus on a new definition was reached. The final definition for Space Systems Security (i.e., PRO-2) came to be: "the assurance of the services, control, and confidentiality of a space system throughout its lifecycle, including all ground, communications, and space components, as well as the people, data, processes, and supply chains that enable it."

As the definition evolved through each iteration of the Delphi study, a knowledge domain table was concurrently developed and presented to expert respondents. The initial space systems security knowledge domain table was constructed using outputs from PRO-1, including the space system segments initially identified through the literature review (detailed in Chapter 2) and the space threat assessment categories published by CSIS (Harrison et al. 2020; Harrison et al. 2022). Together this formed the preliminary scope of the space systems security domain, encompassing both functional and adversarial factors. Upon completing the Delphi study and expert focus group, the scope of the space systems security domain was found to encompass the protection of five segments (Governance, Human, Ground, Space, and C3) against four key

types of adversities (Non-Malicious, Cyber, Electromagnetic, and Kinetic. The segments can be graphically represented as per Figure 38 below.

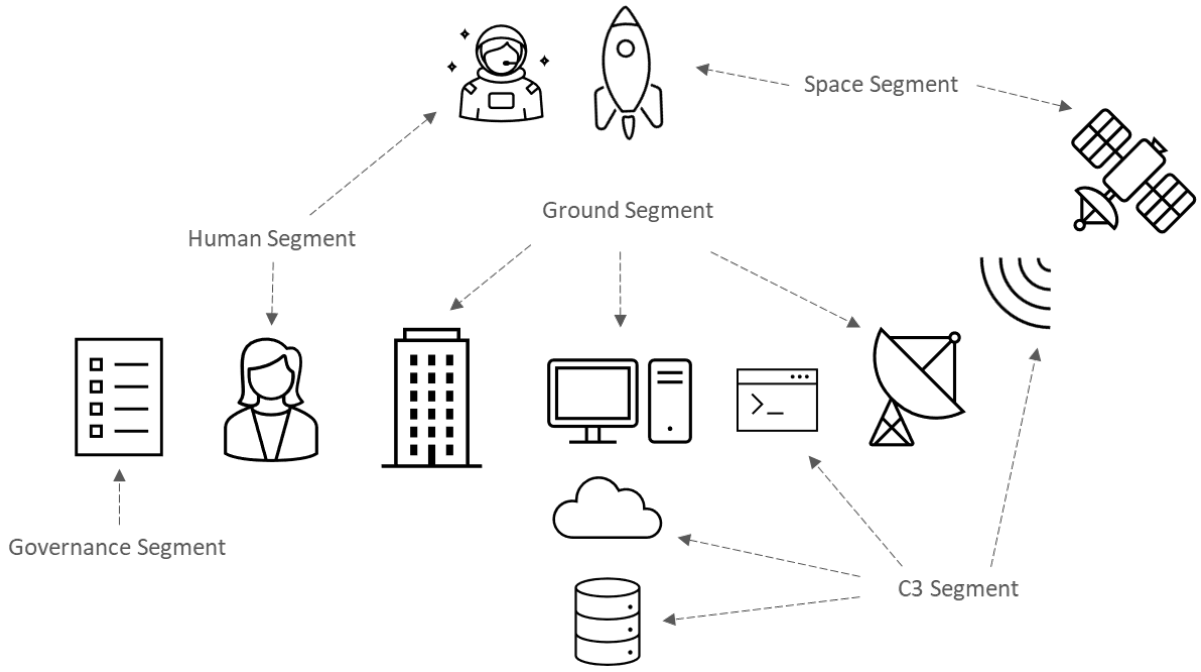

Figure 38 - Space System Segments and Example Components

Notably, based on the progressive research findings, the initial focus on the space-cyber threat environment was necessarily expanded to encompass all threat and adversity types. This was primarily due to the interconnected nature of security considerations and the complex threat environment surrounding space systems. Hence, it was determined that space systems security professionals require some knowledge across all key aspects of the domain to ensure a comprehensive approach to security and resilience. The experimental evaluation of the framework was conducted using a case study methodology, as detailed in section 3.3.2.6, and relied on the newly developed space systems security knowledge domain table to identify strengths and weaknesses in real-world space systems. Some findings were made during the case study interviews, as detailed in section 4.2.2, that necessitated minor additions to the domain table.

The final verified and validated scope of the space systems security domain is defined in the tables below:

	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.

Table 61 – PRO-3: Space Systems Security Knowledge Domain

Governance Segment	R&D, Procurement & Supply Chain, Legal, Ethical & Compliance, Insurance, Public Relations
Human Segment	Personnel, Users, Astronauts/Cosmonauts, Safety, Human Factors, Organisational Culture
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

Table 62 - PRO-3: Space systems segments

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

Table 63 - PRO-3: Space systems adversities

5.3 Research Goal 2 – Space Systems Resilience Ontology

At the commencement of the research project detailed in this dissertation, Research Goal 2 was defined as "an ontological discovery and taxonomical catalogue of space systems resilience for the purposes of resilience assessment by space systems security practitioners". As shown in Figure 37, Research Goal 2 comprises of the knowledge gained through Research Goal 1 plus the following primary and secondary research outcomes (as detailed in Table 59 and Table 60):

- SRO-1: A comprehensive evaluation of existing and tangential research related to power systems and critical infrastructure resilience.
- SRO-2: A taxonomical catalogue of power systems resilience.
- SRO-3: A homogenised definition for 'Power Systems Resilience'.
- PRO-4: A taxonomical catalogue of space systems resilience.
- PRO-5: A contemporary definition for 'Space Systems Resilience'.

The secondary research outcomes 1, 2 and 3 were required in order to complete the primary research outcomes 4 and 5 and are detailed in the Chapter 2 literature review. Due to extensive literature gaps in the space systems domain, power systems were selected as a compatible domain from which to draw foundational resilience concepts to establish a baseline understanding for space systems resilience.

Complex systems resilience is still a relatively young field and so a homogenised definition and taxonomy were developed based on existing power systems and critical infrastructure resilience literature. The new power systems resilience definition and taxonomy were adapted to a space systems context and presented to two dozen expert respondents for iterative feedback over three consecutive rounds of the Delphi study. Consensus was finally achieved and the research outcomes confirmed in the expert focus group, with the final space systems resilience taxonomy (PRO-4) and definition (PRO-5) presented in the remainder of this section. These findings feed into Research Goal 3, which describes the development of the space system resilience assessment framework for space systems security practitioners.

The space systems resilience taxonomy was expanded from the original power systems resilience taxonomy to include an additional sixth function, ‘React’. The ability to actively avoid, deter, or neutralise a detected threat is an aspect of resilience that was identified to be unique to space systems when compared to other critical infrastructures, such as the power grid. The final resilience taxonomy and corresponding functional definitions (PRO-4) is provided below:

- Anticipate, which refers to the system's ability to maintain situational awareness and proactively detect potential threats;
- React, which refers to the system’s ability to avoid, deter, or neutralise detected threats and respond to adverse events;
- Survive, which refers to the system’s ability to mitigate, absorb, or withstand the impacts of an adverse event;
- Sustain, which refers to the system’s ability to retain control and preserve core functions and services in a degraded state;
- Recover, which refers to the system’s ability to respond, restore operations, and 'bounce back' from adverse events; and

- Adapt, which refers to the system's ability to evolve based on threat intelligence and lessons learned to better anticipate, react, survive, sustain and recover from future adverse events.

As the taxonomy evolved through each iteration of the Delphi study, a space systems resilience definition was concurrently developed and presented to expert respondents. The final consensus on the definition for space systems resilience (PRO-5) was as per the below:
"Space systems resilience is the ability of a space system, including its services, sub-components, and supporting functions, to anticipate, react to, survive, recover from, and adapt to adverse events whilst maintaining control and sustaining core operations and services in a degraded state."

5.4 Research Goal 3 – Space System Resilience Assessment Framework

At the commencement of the research project detailed in this dissertation, Research Goal 3 was defined as "a space systems resilience framework, based on the outcomes of the ontological discovery exercise, for determining the high-level resilience status of a given space system to a malicious cyber-physical threat". As shown in Figure 37, Research Goal 3 comprises of the knowledge gained through Research Goal 2 plus the following primary and secondary research outcomes (as detailed in Table 59 and Table 60):

- SRO-4: A functional model representing both phasal and temporal requirements to attain resiliency in a power system and taking into account both technical and non-technical aspects.
- SRO-5: A comprehensive evaluation of existing research related to cyber terrorism.
- SRO-6: A taxonomical catalogue of the features inherent to cyber terrorism.
- SRO-7: A homogenised definition for 'Cyber Terrorism'.
- PRO-6: A functional model representing both phasal and temporal requirements to attain resiliency in a space system and taking into account both technical and non-technical aspects.
- PRO-7: A space system resilience assessment framework to assess the high-level resilience status to any given threat and aid in identifying high level security and resilience control gaps.

The secondary research outcomes 4, 5, 6, and 7 were required in order to complete the primary research outcomes 6 and 7 and are detailed in the Chapter 2 literature review. Due to extensive literature gaps in the space systems domain, power systems were selected as a compatible domain from which to establish a functional model representing both phasal and temporal space system resilience requirements. This was presented to expert respondents as part of the Delphi study, with iterative feedback being implemented across three rounds of surveys and finally verified in the expert focus group. The final space systems resilience model was then experimentally tested and evaluated through the case study methodology, as described in section 3.3.2.6 and further discussed in the remainder of this section. The final phasal and temporal space systems resilience models are presented in Figure 39 and Figure 40 below.

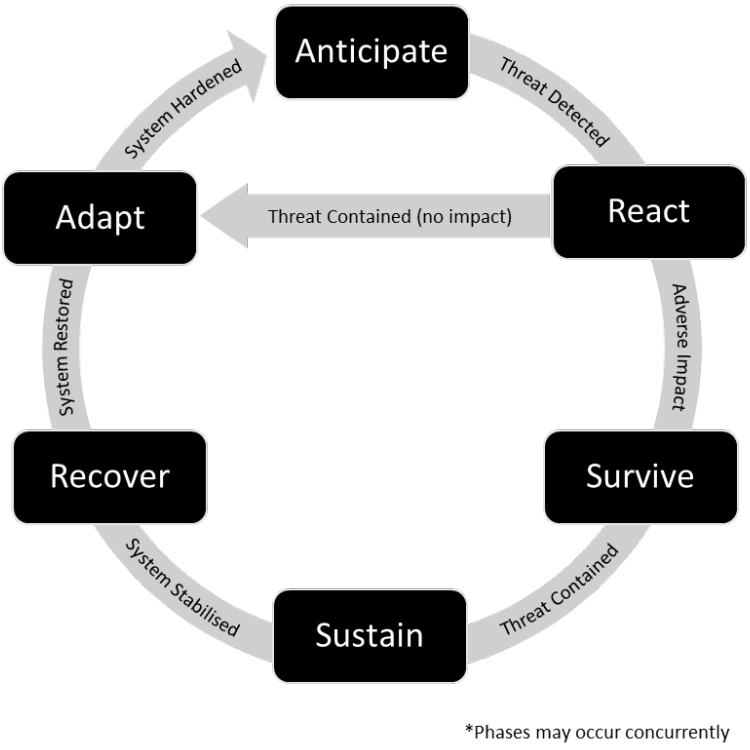

Figure 39 - PRO-6: Space Systems Resilience Phasal Model

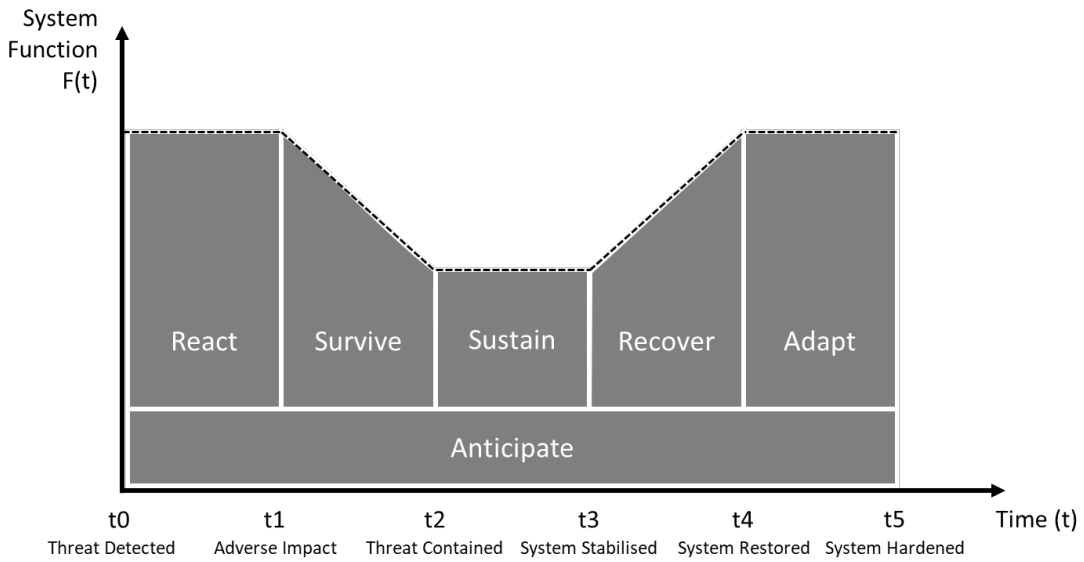

Figure 40 - SRO-6: Space Systems Resilience Temporal Model

Secondary research outcomes 5, 6, and 7 are related to the development of the threat model for the case study component of the research project. In line with Research Goal 3, the case study aimed to test the resilience of real-world space systems to cyber-physical threats. Cyber terrorism was selected as the threat actor for the case study threat model due to its preoccupation on unhindered disruptive and destructive techniques without the added complexities of advance persistence or state-based legal considerations. In the initial stages of research (SRO-5), it was discovered that cyber terrorism was not adequately defined in a way that it could underpin the case study, hence a cyber terrorism taxonomy and definition was constructed based on existing literature (SRO-6 and SRO-7).

Finally, a case study was conducted against three real-world space systems using security and resilience data obtained through expert interviews and documented in accordance with the knowledge domain table developed at PRO-3. The three space systems used to test the resilience assessment framework were: launchpad mission control, ground station, and the space vehicle and payload. Each of these systems' resilience strengths and weaknesses were experimentally tested against the cyber-physical terrorist threat using the Lockheed Martin Cyber Kill Chain (CKC) process and the resilience framework developed through the Delphi study methodology. In this way, the space systems security ontology and resilience framework were used to assess the high-level resilience of each system to cyber-physical adversities. The

framework proved to function agnostically to each space system, including an inherent ability to scale based on the scope of the system, and successfully identified critical flaws in resilience.

The final outcome was an experimentally evaluated space system resilience assessment framework for determining key space system security strengths and weaknesses to aid in assessing resilience to any given threat. However, it should be noted that adversities other than the malicious cyber-physical case study are yet to be tested to confirm universal applicability of the framework. Additionally, with further research the framework may be shown to have utility in other use-cases separate to the assessment methodology applied in the case study component of the research.

6 Conclusions

6.1 Summary

Space infrastructure provides vital services for many critical industries on Earth, including global communications and PNT, as well as non-satellite applications such as space exploration and human settlement. It is therefore essential that space technologies are built to be secure-by-design with inherent resilience to any given adversity. Adding to the complexities of resilient design, the space environment is becoming increasingly congested and contested with a burgeoning second space race that is seeing the rapid deployment of space systems containing a vast array of new technologies and, hence, vulnerabilities. The combined effect of an increasingly hostile threat environment with increasingly vulnerable space systems necessitates the development of a pragmatic, threat-oriented resilience assessment framework. The space systems resilience assessment framework, which was the final goal of this dissertation, was developed to aid space systems security practitioners in assessing the strengths and weaknesses of their system's resilience to any given threat.

In order to produce the threat-driven space system resilience assessment framework, a large body of preliminary research was required due to expansive gaps in the space systems security literature. Although well-articulated in political, legal, and international relations literature, the engineering, science, and technology aspects of space security were found to be under-studied and disjointed, leading to fragmented research and inconsistent terminology. The research project sought to develop a foundational space systems security ontology to guide future research and development, as well as a space system resilience assessment framework for determining the high-level resilience status of any given space system to any given adversity. Although the resilience assessment framework was designed to be threat-agnostic, a cyber-physical case study was utilised to experimentally evaluate the final framework against real-world space systems using data obtained through expert interviews.

In pursuit of this final outcome, the following research questions were posed at the onset of the research project:

1. Research Question 1: Is there research in the space security domain that includes cyber-physical threats to space systems as critical infrastructure?

2. Research Question 2: What is space systems resilience, and can a taxonomy for space systems resilience to cyber-physical threats be developed?
3. Research Question 3: Can a valid interdisciplinary (engineering, international security, and the social and computer sciences) framework be developed to establish space systems security as a professional domain?

The final findings related to Research Question 1 identified a literature gap across various areas related to space systems security and resilience, leading to the conclusion that there is inadequate existing space systems security and resilience literature to complete the final objective of a space systems resilience assessment framework. Research Question 2 was answered through the Delphi study process, with a final definition and taxonomy being developed and evaluated through the case study methodology. The final resilience definition and taxonomy was necessarily made broader than the original cyber-physical threat focus, however a cyber-physical case study threat model was developed to meet this initial inquiry. The final research question was answered through the development of the space systems security knowledge domain and associated ontology through the Delphi study process and validated through the case study.

In addition to the research questions above, complementary objectives were defined and used to guide the final outcomes of the research project:

1. Research Goal 1: An experimental evaluation of the research related to space systems security to determine the scope of the domain and theories on the space-cyber threat environment.
2. Research Goal 2: An ontological discovery and taxonomical catalogue of space systems resilience for the purposes of resilience assessment by space systems security practitioners.
3. Research Goal 3: A space systems resilience framework, based on the outcomes of the ontological discovery exercise, for determining the high-level resilience status of a given space system to a malicious cyber-physical threat.

In support of Research Goal 1, an experimental evaluation of the research related to space systems security was conducted to determine the scope of the domain and develop a cyber-physical threat model for the case study. Resulting from the literature review, a preliminary space systems security definition and knowledge domain was presented to two dozen space

systems security experts, with iterative feedback obtained over three rounds of the Delphi study. A final definition for space systems security was achieved, with a knowledge domain table being concurrently developed and presented to expert respondents based on their feedback. Together this forms the scope of the space systems security domain, encompassing both functional and adversarial factors, including the protection of five segments (Governance, Human, Ground, Space, and C3) against four key types of adversities (Non-Malicious, Cyber, Electromagnetic, and Kinetic). The experimental evaluation of the security ontology was conducted using a case study methodology to identify strengths and weaknesses in real-world space systems.

The findings made in pursuit of Research Goal 1 were used as an input into the Delphi study methodology, which served to validate the outcomes of the novel space systems resilience taxonomy developed for Research Goal 2. A significant literature gap was found to exist in the field of space systems resilience and so an initial taxonomy was derived from adjacent power systems resilience literature. The preliminary model was iteratively modified based on expert feedback through the Delphi study process. The final space systems resilience taxonomy was found to consist of 6 functions; Anticipate, React, Survive, Sustain, Recover, and Adapt. Each function of the resilience taxonomy may also serve as phases in the resilience cycle, with each phase describing a resilient space system's capabilities to withstand an adverse event over each stage of the incident. The taxonomy and resilience cycle model were tested against the cyber kill chain (CKC) framework through the case study methodology. These findings were then fed into Research Goal 3, which served to develop the space system resilience assessment framework.

In line with the final Research Goal 3, the case study aimed to test the resilience of real-world space systems to cyber-physical threats. This was achieved through the case study methodology, where cyber terrorism was selected as the threat actor due to its preoccupation on unhindered disruptive and destructive techniques without the added complexities of advance persistence or state-based legal considerations. In the initial stages of research, it was discovered that cyber terrorism was not adequately defined in a way that it could underpin the case study, hence a cyber terrorism taxonomy and definition was constructed based on existing literature. The findings from the cyber terrorism research were used to build a detailed threat model against the CKC, against which the real-world space systems would be theoretically tested. The case study test involved gaining high-level security and resilience data on three

real-world space systems using data obtained through expert interviews. The three space systems used to test the resilience assessment framework were: launchpad mission control, ground station, and the space vehicle and payload. Each of these systems' resilience strengths and weaknesses were experimentally tested against the cyber-physical terrorist threat model and the resilience framework developed through the Delphi study methodology. In this way, the space systems security ontology and resilience framework were used to assess the high-level resilience of each system to cyber-physical adversities. The framework proved to function agnostically to each space system, including an inherent ability to scale based on the scope of the system, and successfully identified critical flaws in resilience.

The final outcome of this body of research is an experimentally evaluated space system resilience assessment framework for determining key space system security strengths and weaknesses. The framework is designed to aid in assessing the high-level resilience status of any given space system to any given threat. With further research it is expected that this novel space systems resilience framework may have utility in other use-cases separate to the assessment methodology applied in the case study component of the research. Additionally, the framework could be elaborated on for specific space systems or adversities, such as a cybersecurity resilience assessment framework for LEO satellites.

6.2 Limitations

Although the research detailed in this dissertation aimed to be comprehensive, there were limitations to the study due to time, resources, and available literature that should be acknowledged.

Firstly, the types of space systems considered in the space threat review of Section 2.3.1 was limited to available open-source research published in the English language. This limitation may skew results largely towards Western Anglo-centric threats and past events. Another result of this limitation is the limited available literature to guide the study and its outcomes, potentially leaving gaps or oversights in the final resilience assessment framework. For example, most cited space systems literature related to Earth-orbiting satellite systems, primarily in LEO, resulting in the resilience assessment framework being largely satellite-centric. Efforts were made to enable the space systems security and resilience findings to apply to any given space system, however future research on non-satellite space systems may serve to enhance the framework and ontology to be truly agnostic.

Another limitation to the research comes from the limited scope of the study. Although the resilience assessment framework is intended to be applicable to all malicious and non-malicious threats, not all threats to space systems were identified or modelled. Due to timing and resource constraints, the scope of the testing was limited to cyber-physical threats. This was then only tested using an extreme example model of cyber-physical terrorism, which is expected to differ to other types of cyber-physical threats such as cyber warfare or non-targeted malware.

It should also be noted that the framework was only tested against high-level security controls due to the security constraints of publishing real-world space system data. This may limit the perceived utility of the framework, where further vulnerability determination and lower-level resilience analysis may be possible. The high-level data limitations may also limit the assessed robustness of the framework, where further improvements may be identified once in use in industry.

This highlights a final limitation to the study, which is the theoretical evaluation of the framework. Although the framework was tested using real-world data, it has not yet been formally implemented in an operational system and evaluated over a period of time or in response to a real adverse event. This limitation may necessitate future and continued improvements to the resilience assessment framework as the field of space systems and their security advances.

Finally, the case study component of the research only tested the progression of a single adverse event through the resilience cycle. Even though it is stated that the resilience cycle may be initiated several times by different concurrent attacks, this aspect of the framework has not been examined in depth. A resilience assessment can take place without this aspect of the framework being verified in depth; however adverse event concurrency may be desirable for future studies that wish to explore the resilience cycle of a space system.

6.3 Recommendations

The body of research detailed in this thesis provides a foundational ontology, domain scoping, and framework for assessing resilience. These outcomes can be expanded on in a number of

ways that would add value to the field of space systems security and resilience. This section outlines some high-level recommendations for future research and expansion on this work.

Future work could entail incorporating existing space systems engineering language and ontology into this assessment framework so that the developers and operators of space systems can effectively use it in their operational environment. Tangential spacecraft engineering concepts could also be analysed, with future research identifying parallels between reliability and resilience engineering as well as incorporating threats and incidents identified through relevant fault management literature. As space systems continue to evolve the knowledge domain constructed at Table 61 should be expanded on to include any extra scope of knowledge that would be required to effectively cover the space systems security domain. For example, a security risk taxonomy for commercial space missions (Falco and Boschetti 2021) was recently published and could be used to investigate a risk-based approach to the resilience framework. These improvements can then be periodically applied to the resilience assessment framework and tested to ensure ongoing agnosticism to space systems and any relevant adversities.

The resilience assessment framework should also be tested against other case studies, threat types, and for different sized systems. For example, the framework's viability to assess resilience against electromagnetic, physical, and non-malicious threats could be evaluated in addition to other cyber threat scenarios that are not necessarily cyber-physical in nature. More extensive case studies can also be conducted using other methodologies for attack analysis, such as attack trees as demonstrated against CubeSats in Falco et al. 2021 conference paper (Falco et al. 2021). Further research could be conducted on applying literature for satellite security to non-orbital systems such as rovers and life-supporting space vehicles. This could include an expansion on the types of space systems considered in the space threat review conducted in Section 2.3.1.

Secondary or indirect threats could also be evaluated in relation to the framework, for example how it relates to the Kessler effect and other related risks such as a decommissioned satellite being maliciously propelled back out of the junk belt orbit. The framework could also be evaluated for use on non-orbital systems such as rovers or outer space probes and lunar habitats. The resilience assessment framework should be examined in relation to other complementary frameworks such as D4P2, NIST, MITRE ATT&CK, and others to build a more

comprehensive resilience framework that encompasses both resilience assessment and resilient design considerations.

On space technologies, Georgescu et al. (2019a) established space systems as critical infrastructure that can be divided into five key categories: Remote Sensing, Communications, Meteorological, GNSS, and Administrative and Legislative Frameworks. This CSI taxonomy should be verified by future referential research and perhaps expanded to identify and include non-critical space systems. Expanding on Harrison et al. (2020) we can class malicious (i.e., non-environmental) space threats under four categories: kinetic physical, non-kinetic physical, electronic, and cyber. These four categories are more descriptive for general security use compared to the three law-driven categories (kinetic, virtual, and hybrid) proposed by Housen-Couriel in their earlier paper (Housen-Couriel 2016), however more research may be required to determine a universally robust space threat taxonomy. In that same paper, Housen-Couriel (2016) identifies five stages of satellite operations: pre-launch; at launch; telemetry, tracking, and command (TT&C); transmissions; and end-of-life. This satellite lifecycle should be validated by the aerospace community and analysed from a mission security perspective – perhaps using the four satellite cybersecurity sub-domains identified by Pavur and Martinovic (2020): satellite radio-link security, space hardware security, ground station security, and operational/mission security.

Finally, in relation to the secondary research outcomes, future research could seek to develop a power system resilience assessment framework to assess the high-level resilience status of an electric grid to any given threat. This could be based on the work already completed to develop a similar resilience framework for space systems, as detailed in this dissertation.

References

Adler, M., Ziglio, E., 1996. Gazing Into the Oracle: The Delphi Method and Its Application to Social Policy and Public Health, Social Science. Jessica Kingsley Publishers.

Akhgar, B., Staniforth, A., Bosco, F. (Eds.), 2014. Cyber Crime and Cyber Terrorism Invesitgators Handbook. Elsevier Syngress.

Al Majali, A., 2014. A Function-Based Methodology for Evaluating Resilience in Smart Grids (Doctor of Philosophy). University of Southern California, California.

Al Mazari, A., Anjariny, A.H., Habib, S.A., Nyakwende, E., 2018. Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies, in: Cyber Security and Threats Concepts Methodologies Tools and Applications. pp. 608–621.

Albasrawi, M.N., Jarus, N., Joshi, K.A., Sarvestani, S.S., 2014. Analysis of Reliability and Resilience for Smart Grids, in: 2014 IEEE 38th Annual Computer Software and Applications Conference. IEEE, Vasteras, Sweden, pp. 529–534.

Amin, M.G., Closas, P., Broumandan, A., Volakis, J.L., 2016. Vulnerabilities, threats, and authentication in satellite-based navigation systems. Proceedings of the IEEE, Scanning the Issue 104, 1169–1173. https://doi.org/10.1109/JPROC.2016.2550638

Arghandeh, R., von Meier, A., Mehrmanesh, L., Mili, L., 2016. On the Definition of Cyber-Physical Resilience in Power Systems. Renewable and Sustainable Energy Reviews 58, 1060–1069. https://doi.org/10.1016/j.rser.2015.12.193

Australian Government, 2018. Security of Critical Infrastructure (SOCI) Act, No. 29, Compilation No. 4, Section 8D.

Australian Government, 2017. Foreign Policy White Paper. Australian Government.

Bardin, J., 2013. Satellite Cyber Attack Search and Destroy, in: Computer and Information Security Handbook. Elsevier Science & Technology, pp. 1093–1102.

Baros, S., Shiltz, D., Jaipuria, P., Hussain, A., Annaswamy, A.M., 2017. Towards Resilient Cyber-Physical Energy Systems 10.

Bie, Z., Lin, Y., Li, G., Li, F., 2017. Battling the Extreme: A Study on the Power System Resilience. Proceedings of the IEEE 105, 1253–1266.

Blinken, A., 2022. Attribution of Russia's Malicious Cyber Activity Against Ukraine. URL https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/ (accessed 01.03.23).

Bosch, O., 2012. Critical Information Infrastructure and Cyber-Terrorism, in: Law, Policy, and Technology - Cyberterrorism, Information Warfare, and Internet Immobilization. Information Science Reference, Hersey, PA, pp. 31–40.

Boschetti, N., Gordon, N., Falco, G., 2022. Space Cybersecurity Lessons Learned from the ViaSat Cyberattack, in: 2022 AIAA Ascend Conference. Aerospace Research Central, Las Vegas, USA.

Bradbury, M., Maple, C., Hu, Y., Ugur, I.A., Cannizzaro, S., 2020. Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures, in: 2020 IEEE Aerospace Conference. Presented at the 2020 IEEE Aerospace Conference, IEEE, USA, pp. 1–20. https://doi.org/10.1109/AERO47225.2020.9172785

Bugos, S., 2021. Russian ASAT Test Creates Massive Debris. Arms Control Association. URL https://www.armscontrol.org/act/2021-12/news/russian-asat-test-creates-massive-debris (accessed 01.03.23).

Bryman, A., 2003. Triangulation. Encyclopedia of Social Science Research Methods.

Chanda, S., Srivastava, A.K., 2015. Quantifying Resiliency of Smart Power Distribution Systems with Distributed Energy Resources, in: 2015 IEEE 24th International Symposium on Industrial Electronics (ISIE). IEEE, Rio de Janeiro, Brazil, pp. 766–771.

Chiaradonna, S., Giandomenico, F.D., Murru, N., 2014. On a Modeling Approach to Analyze Resilience of a Smart Grid Infrastructure, in: 10th European Dependable Computing Conference. IEEE, Newcastle, United Kingdom, pp. 166–177.

Clark, A., Zonouz, S., 2019. Cyber-Physical Resilience: Definition and Assessment Metric. IEEE Transactions on Smart Grid 10, 1671–1684.

Clarke, V., Braun, V., 2013. Successful Qualitative Research: A Practical Guide for Beginners, First. ed. Sage Publications.

Creswell, J.W., 2009. Research design: Qualitative, quantitative, and mixed methods approaches, 3rd ed. Sage Publications.

Critical Five, 2014. Forging a Common Understanding for Critical Infrastructure. Critical Five, New Zealand.

CSRIC, 2015. Cybersecurity Risk Management and Best Practices Working Group 4: Final Report (Working Group No. 4). The Communications Security, Reliability and Interoperability Council, USA.

Cyber Peace Institute, 2022. Viasat Case Study [WWW Document]. Cyber Peace Institute. URL https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat#footnote-3 (accessed 01.03.23).

Czerpak, P., 2005. The European Dimension of the Fight against Cyber-Terrorism - A Theoretical Approach, in: Europe and Complex Security Issues. pp. 309–318.

Dalkey, 1967. An experimental study of group opinion: The Delphi method. Elsevier Futures 1, 408–426. https://doi.org/10.1016/S0016-3287(69)80025-X

Day, J., Bobeva, M., 2005. A Generic Toolkit for the Successful Management of Delphi. The electronic journal of business research methodology 3, 103–116.

de Abreu Faria, L., de Melo Silvestre, C.A., Correia, M.A.F., 2016. GPS-Dependent Systems: Vulnerabilities to Electromagnetic Attacks. Journal of Aerospace Technology and Management 8, 423–430. https://doi.org/10.5028/jatm.v8i4.632

Defense Intelligence Agency, 2022. Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion. Defense Intelligence Agency, USA.

del Monte, L., 2013. Towards a cybersecurity policy for a sustainable, secure and safe space environment, in: Proceedings of the 64th International Astronautical Congress (IAC).

Denning, D., 2007. A View of Cyberterrorism Five Years Later, in: Internet Security: Hacking, Counterhacking, and Society. Jones and Bartlett, London, pp. 123–140.

Denning, D., 2000. Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism. The Terrorism Research Center, U.S. House of Representatives.

Denzin, N.K., Lincoln, Y.S., 1994. Handbook of qualitative research. Sage Publications, California, USA.

Dessavre, D.G., Ramirez-Marquez, J.E., Barker, K., 2015. Multidimensional Approach to Complex System Resilience Analysis. Reliability Engineering & System Safety 149, 34–43.

Donnelly, D., 2021. War fears as China vows punishment on Australia for Taiwan support - Long-range strikes. Express.

Eisenberg, D.A., Park, J., Kim, D., 2014. Resilience Analysis of Critical Infrastructure Systems Requires Integration of Multiple Analytical Techniques. Urban Sustainability and Resilience 15.

Eshghi, K., Johnson, B.K., Rieger, C.G., 2015. Power System Protection and Resilient Metrics, in: 2015 Resilience Week (RWS). IEEE, pp. 1–8. https://doi.org/10.1109/RWEEK.2015.7287448

Falco, G., Boschetti, N., 2021. A Security Risk Taxonomy for Commercial Space Missions, in: Proceedings of the AIAA Ascend Conference.

Falco, G., Viswanathan, A., Santangelo, A., 2021. CubeSat Security Attack Tree Analysis, in: Proceedings of the IEEE 8th International Conference on Space Mission Challenges for Information Technology.

Falco, G., 2018. Cybersecurity Principles for Space Systems. Aerospace Research Central 16(2). https://doi.org/10.2514/1.I010693

Farley, R., 2020. Space Force: Ahead of Its Time, or Dreadfully Premature? CATO Institute Policy Analysis 904.

Foltz, C.B., 2004. Cyberterrorism, Computer Crime, and Reality. Information Management & Computer Security 12, 154–166.

Fraccascia, L., Giannoccaro, I., Albino, V., 2018. Resilience of Complex Systems: State of the Art and Directions for Future Research. Wiley Hindawi 2018, 1–44.

Friedberg, I., McLaughlin, K., Smith, P., 2016. A Cyber-Physical Resilience Metric for Smart Grids, in: 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, Washington, DC, USA, pp. 1–5.

Friedberg, I., McLaughlin, K., Smith, P., 2015. Towards a Cyber-Physical Resilience Framework for Smart Grids, in: Latré, S., Charalambides, M., François, J., Schmitt, C., Stiller, B. (Eds.), Intelligent Mechanisms for Network Configuration and Security. Springer, Cham, pp. 140–144.

Friedberg, I., McLaughlin, K., Smith, P., Wurzenberger, M., 2017. Towards a Resilience Metric Framework for Cyber-Physical Systems, in: 4th International Symposium for ICS & SCADA Cyber Security Research 2016.

Genge, B., Kiss, I., Haller, P., 2015. A System Dynamics Approach for Assessing the Impact of Cyber Attacks on Critical Infrastructures. Elsevier International Journal of Critical Infrastructure Protection 10, 3–17.

Georgescu, Alexandru, Gheorghe, A.V., Piso, M., Katina, P.F., 2019a. Critical Space Infrastructures, in: Critical Space Infrastructures: Risk, Resilience and Complexity, Topics in Safety, Risk, Reliability and Quality. Springer, Switzerland, pp. 21–36.

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

Gholami, A., Shekari, T., Amirioun, M.H., Aminifar, F., Amini, M.H., Sargolzaei, A., 2018. Toward a Consensus on the Definition and Taxonomy of Power System Resilience. IEEE Access 6, 32035–32053. https://doi.org/10.1109/ACCESS.2018.2845378

Glenn, C., Sterbentz, D., Wright, A., 2016. Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector (No. INL/EXT-16-40692, 1337873), Mission Support Center Analysis Report. Idaho National Laboratory, USA.

Hannan, N., 2018. An Assessment of Supply-Chain Cyber Resilience for the International Space Station. The RUSI Journal 163, 28–32. https://doi.org/10.1080/03071847.2018.1469249

Hardy, K., Williams, G., 2014. What Is Cyberterrorism? Computer and Internet Technology in Legal Definitions of Terrorism, in: Cyberterrorism Understanding Assessment and Response. Springer Science+Business Media, New York, pp. 1–24.

Harrison, T., Johnson, K., Makena, Y., 2021. Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons, CSIS Reports. Center for Strategic and International Studies.

Harrison, T., Johnson, K., Roberts, T.G., Young, M., 2020. Space Threat Assessment 2020. Center for Strategic & International Studies, Washington, United States.

Harrison, T., Johnson, K., Young, M., Wood, N., Goessler, A., 2022. Space Threat Assessment 2022 (A Report of the CSIS Aerospace Security Project). Center for Strategic and International Studies (CSIS), USA.

Haseman, B., 2006. A manifesto for performative research.

Henry, D., Ramirez-Marquez, J.E., 2012. Generic Metrics and Quantitative Approaches for System Resilience as a Function of Time. Reliability Engineering & System Safety 99, 114–122.

Hickford, A.J., Blainey, S.P., Ortega Hortelano, A., Pant, R., 2018. Resilience Engineering: Theory and Practice in Interdependent Infrastructure Systems. Springer Environment Systems and Decisions 38, 278–291. https://doi.org/10.1007/s10669-018-9707-4

Housen-Couriel, D., 2016. Cybersecurity threats to satellite communications: Towards a typology of state actor responses. Acta Astronautica 128, 409–415. https://doi.org/10.1016/j.actaastro.2016.07.041

Hua, J., Bapna, S., 2012. How Can We Deter Cyberterrorism? Information Security Journal: A Global Perspective 21, 102–114. https://doi.org/10.1080/19393555.2011.647250

Ikitemur, G., Karabacak, B., Igonor, A., 2020. A Mixed Public-Private Partnership Approach for Cyber Resilience of Space Technologies, in: Space Infrastructures: From Risk to Resilience Governance, NATO Science for Peace and Security Series - D: Information and Communication Security. IOS Press, pp. 120–130.

Ioannides, R.T., Pany, T., Gibbons, G., 2016. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. Proceedings of the IEEE 104, 1174–1194. https://doi.org/10.1109/JPROC.2016.2535898

Jackson, M., Fitzgerald, J.S., 2016. Resilience Profiling in the Model-Based Design of Cyber-Physical Systems. 14th Overture Workshop.

Jarvis, L., Macdonald, S., 2014. What Is Cyberterrorism? Findings From a Survey of Researchers. Terrorism and Political Violence 27, 657–678. https://doi.org/10.1080/09546553.2013.847827

Jarvis, L., Macdonald, S., Whiting, A., 2016. Unpacking Cyberterrorism Discourse: Specificity, Status, and Scale in News Media Constructions of Threat. European Journal of International Security 2, 64–87. https://doi.org/10.1017/eis.2016.14

Kallberg, J., 2012. Designer Satellite Collisions from Covert Cyber War. Strategic Studies Quarterly, Spring 6, 124–136.

Kang, M., Hopkinson, K., Betances, A., Reith, M., 2018. Mitigation of Cyber Warfare in Space Through Reed Solomon Codes. Presented at the 13th International Conference on Cyber Warfare and Security, ACPI, Washington DC, USA.

Kaplan, B., Duchon, D., 1988. Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. MIS Quarterly, Management Information Systems Research Center, University of Minnesota 12. https://doi.org/10.2307/249133

Kaspersky Lab, 2019. Threat Landscape for Industrial Automation Systems. Kaspersky Lab ICS CERT, Moscow, Russia.

Kellner, D., 2015. Media Spectacle and the Crisis of Democracy: Terrorism, War, and Election Battles. Routledge.

Kenney, M., 2015. Cyber-Terrorism in a Post-Stuxnet World. Orbis 59, 111–128. https://doi.org/10.1016/j.orbis.2014.11.009

Knittel, C., 2013. The Mystery of the Creepiest Television Hack. VICE.

Kshetri, N., Voas, J., 2017. Hacking Power Grids: A Current Problem. Computer 50, 91–95. https://doi.org/10.1109/MC.2017.4451203

Kwasinski, A., 2016. Quantitative Model and Metrics of Electrical Grids' Resilience Evaluated at a Power Distribution Level. Energies 9, 93. https://doi.org/10.3390/en9020093

Lee, R.M., Asssante, M.J., Conway, T., 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid.

Lewis, J.A., 2002. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies.

Linstone, H.A., Turoff, M., 2002. The Delphi Method: Techniques and Applications.

Liu, C.-C., McArthur, S., Lee, S.-J. (Eds.), 2016. Smart Grid Handbook. John Wiley & Sons, Chichester, UK.

Livingstone, D., Lewis, P., 2016. Space, the Final Frontier for Cybersecurity? Chatham House.

Macdonald, S., Jarvis, L., Chen, T., 2013. Cyberterrorism Project Research Report, in: A Multidisciplinary Conference on Cyberterrorism. Swansea University, UK.

Mantel, B., 2009. Terrorism and the Internet: Should Web Sites That Promote Terrorism Be Shut Down? CQ Global Researcher 3.

Manulis, M., Bridges, C.P., Harrison, R., Sekar, V., Davis, A., 2020. Cyber security in New Space. International Journal of Information Security 20, pp. 287–311. https://doi.org/10.1007/s10207-020-00503-w

Mayence, J.-F., 2010. Space security: transatlantic approach to space governance, in: Robinson, J., Schaefer, M., Schrogl, K.-U., von der Dunk, F. (Eds.), Prospects for Transparency and Confidence-Building Measures in Space. ESPI, Vienna, Austria, p. 35.

Maynard, T., Beecroft, N., 2015. Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid, Emerging Risk Report, Innovation Series. Centre for Risk Studies, University of Cambridge.

McAfee, 2005. McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet. McAfee.

McLeod, G., Nacouzi, G., Dreyer, P., Eisman, M., Hura, M., Langeland, K.S., Manheim, D., Torrington, G., 2016. Enhancing Space Resilience Through Non-Materiel Means (Technical Report No. AD1085075). RAND Project Air Force Santa Monica, Santa Monica, United States of America.

MITRE, 2022. ICS Matrix [WWW Document]. MITRE. URL https://attack.mitre.org/matrices/ics/ (accessed 05.03.23).

Moltz, J.C., 2011. The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests, Second. ed. Stanford University Press, California, USA.

Moore, J.E., 2008. The Economic Costs and Consequences of Terrorism. Edward Elgar Publishing.

Mshvidobadze, K., 2011. State-Sponsored Cyber Terrorism: Georgia's Experience. Tbilisi, Georgia.

Nacos, B., 2016. Mass-Mediated Terrorism: Mainstream and Digital Media in Terrorism and Counterterrorism. Rowman & Littlefield.

Nagpal, R., 2002. Cyber Terrorism in the Context of Globalization, in: Second World Congress on Informatics and Law. Madrid, Spain, pp. 1–23.

Naser, M.Z., Chehab, A.I., 2018. Materials and design concepts for space-resilient structures. Progress in Aerospace Sciences 98, 74–90. https://doi.org/10.1016/j.paerosci.2018.03.004

Nidecki, T.A., n.d. What Is Persistent XSS. The Acunetix Blog. URL https://www.acunetix.com/blog/articles/persistent-xss/ (accessed 11.27.22).

NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, USA.

Okoli, C., Pawlowski, S.D., 2004. The Delphi method as a research tool: an example, design considerations and applications. Information & Management 42, 15–29.

O'Neill, I.J., Handal, J., 2021. https://www.jpl.nasa.gov/news/nasa-analysis-earth-is-safe-from-asteroid-apophis-for-100-plus-years. NASA Jet Propulsion Laboratory.

Ormrod, D., Slay, J., Ormrod, A., 2021. Cyber-Worthiness and Cyber-Resilience to Secure Low Earth Orbit Satellites. Presented at the 16th International Conference on Cyber Warfare and Security, Academic Conferences Limited, p. 257.

Osman, K.O., Osman, W.R.S., Al-Khasawneh, Y., Duhaim, S., 2014. Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Science and Mobile Computing 3, 1082–1090.

Panteli, M., Mancarella, P., Trakas, D.N., Kyriakides, E., Hatziargyriou, N.D., 2017. Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems. IEEE Transactions on Power Systems 32, 4732–4742. https://doi.org/10.1109/TPWRS.2017.2664141

Pavur, J., Martinovic, I., 2020. SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research. arXiv preprint arXiv:2010.10872. https://doi.org/10.48550/arXiv.2010.10872

Pearson, J., 2022. Russia downed satellite internet in Ukraine.

Phillips, D.M., Mazzuchi, T.A., Sarkani, S., 2018. An architecture, system engineering, and acquisition approach for space system software resiliency. Information and Software Technology 94, 150–164. https://doi.org/10.1016/j.infsof.2017.10.006

Planck, M., 2009. Air and Space Law, in: Max Planck Institute for Comparative Public Law and International Law, World Court Digest (Formerly Fontes Iuris Gentium). Springer, Berlin, Germany.

Plotnek, J.J., 2022a. Enhancing Cyber Resilience in Smart Grids. Australian Institute of Energy, Energy News 40, 7–10.

Plotnek, J.J., 2022b. Space-Cyber trends and opportunities in Australia. Australia in Space Magazine 18–21.

Plotnek, J.J., Slay, J., 2022a. Space Systems Security: A Definition and Knowledge Domain for the Contemporary Context. Journal of Information Warfare 21, 103–119.

Plotnek, J.J., Slay, J., 2022b. A New Dawn for Space Security, in: Proceedings of the 17th International Conference on Cyber Warfare and Security 2022. Presented at the 17th International Conference on Cyber Warfare and Security, State University of New York, Albany, USA, pp. 253–261. https://doi.org/10.34190/iccws.17.1.17

Plotnek, J.J., Slay, J., 2021a. Power systems resilience: Definition and taxonomy with a view towards metrics. International Journal of Critical Infrastructure Protection 33. https://doi.org/10.1016/j.ijcip.2021.100411

Plotnek, J.J., Slay, J., 2021b. Cyber terrorism: A homogenized taxonomy and definition. Computers & Security 102, 102–145. https://doi.org/10.1016/j.cose.2020.102145

Plotnek, Jordan J., Slay, J., 2021. Satellite Cyber Resilience Whitepaper. SmartSat CRC, Adelaide, Australia.

Plotnek, J.J., Slay, J., 2019. What is Cyber Terrorism: Discussion of Definition and Taxonomy, in: 18th Australian Cyber Warfare Conference 2019. Presented at the Australian Cyber Warfare Conference, Deakin University, Melbourne, Australia, pp. 1–4.

Pollitt, M.M., 1998. Cyberterrorism - Fact or Fancy? Elsevier Computer Fraud & Security 8–10.

Popik, T.S., 2017. Testimony of the Foundation for Resilient Societies, in: Reliability Technical Conference. Federal Energy Regulatory Commission.

Rahiminejad, A., Plotnek, J.J., Atallah, R., Dubois, M.-A., Malatrait, D., Ghafouri, M., Mohammadi, A., Debbabi, M., 2023. A Resilience-Based Recovery Scheme for Smart Grid Restoration following Cyberattacks to Substations. International Journal of Electrical Power and Energy Systems 145. https://doi.org/10.1016/j.ijepes.2022.108610

Roege, P.E., Collier, Z.A., Mancillas, J., McDonagh, J.A., Linkov, I., 2014. Metrics for Energy Resilience. Energy Policy 72, 249–256. https://doi.org/10.1016/j.enpol.2014.04.012

Rose, G.J., Henry, W., Hodson, D., Falco, G., 2022. Building A Moat: Fortifying Satellite Software from Vulnerabilities. Presented at the AIAA Ascend Conference, Las Vegas, United States of America.

Santamarta, R., 2014. SATCOM Terminals: Hacking by Air, Sea, and Land. IOActive, USA.

Scholz, R.W., Tietje, O., 2002. Embedded Case Study Methods: Integrating Quantitative and Qualitative Knowledge. Sage Publications.

Shandiz, S.C., Foliente, G., Rismanchi, B., Wachtel, A., Jeffers, R.F., 2020. Resilience framework and metrics for energy master planning of communities. Energy 2013. https://doi.org/10.1016/j.energy.2020.117856

Sheehan, M., 2020. Defining Space Security, in: Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., Giannopapa, C. (Eds.), Handbook of Space Security. Springer, New York, USA, pp. 7–21.

Skinner, R., Nelson, R.R., Chin, W.W., Land, L., 2015. The Delphi Method Research Strategy in Studies of Information Systems. Association for Information Systems 37, 31–63.

Skulmoski, G., Hartman, F., Krahn, J., 2007. The Delphi method for graduate research. Journal of Information Technology Education: Research 6, 1–21.

Sobczak, B., 2019. Cyber Event Disrupted U.S. Grid Networks - DOE.

Stambaugh, H., Beaupre, D.S., Icove, D.J., Baker, R., Cassaday, W., Williams, W.P., 2001. Electronic Crime Needs Assessment for State and Local Law Enforcement. National Institute of Justice, Washington DC, USA.

Steinberger, J.A., 2008. A Survey of Satellite Communications System Vulnerabilities. Joint Electronic Warfare Center, United States.

Stephens, D., 2021. The Woomera Manual [WWW Document]. URL https://law.adelaide.edu.au/woomera/ (accessed 3.29.21).

Straub, J., 2014. Building space operations resiliency with a multi-tier mission architecture. Sensors and Systems for Space Applications VII 9085. https://doi.org/10.1117/12.2050175

Thangavel, K., Plotnek, J.J., Sabatini, R., 2022. Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity. Presented at the 41st AIAA/IEEE Digital Avionics Systems Conference (DASC), USA.

The White House, 2013a. Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The White House, USA.

The White House, 2013b. Presidential Policy Directive - Critical Infrastructure Security and Resilience. USA.

Thompson, M.A., Ryan, M.J., Slay, J., McLucas, A.C., 2016a. A New Resilience Taxonomy, in: 26th Annual International INCOSE Symposium. Edinburgh, UK.

Thompson, M.A., Ryan, M.J., Slay, J., McLucas, A.C., 2016b. Harmonized Taxonomies for Security and Resilience. Information Security Journal: A Global Perspective 25, 54–67. https://doi.org/10.1080/19393555.2016.1145772

Tsamis, N., Bailey, B., Falco, G., 2021. Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles, in: AIAA Ascend Conference 2021.

Unal, B., 2019. Cybersecurity of NATO's Space-based Strategic Assets. International Security Department, The Royal Institute of International Affairs, Chatham House.

Union of Concerned Scientists, 2022. Union of Concerned Scientists Satellite Database [WWW Document]. Union of Concerned Scientists. URL https://ucsusa.org/resources/satellite-database (accessed 01.03.23).

United States Department of Defense, 2015. Space Domain Mission Assurance: A Resilience Taxonomy. Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, USA.

United States Government, 2006. Critical Infrastructure Threats and Terrorism: Handbook. Deputy Chief of Staff for Intelligence, Kansas, USA.

Van der Watt, R., Slay, J., 2021. Modification of the Lockheed Martin Cyber Kill Chain (LMCKC) for cyber security breaches concerning Low Earth Orbit (LEO) Satellites. Presented at the 16th International Conference on Cyber Warfare and Security.

Wang, P., 2019. Death by Hacking: The Emerging Threat of Kinetic Cyber, in: Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications. Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore, p. 17.

Wang, S., Payman, D., Mohannad, A., Mostafa, N., 2019. Advanced control solutions for enhanced resilience of modern power-electronic-interfaced distribution systems. Journal of Modern Power Systems and Clean Energy 7, 716–730. https://doi.org/10.1007/s40565-019-0559-9

Watson, J.-P., Guttromson, R., Silva-Monroy, C., Jeffers, R., Jones, K., Ellison, J., Rath, C., Gearhart, J., Jones, D., Corbet, T., Hanley, C., Walker, L.T., 2014. Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States (No. SAND2014-18019, 1177743).

Weimann, G., 2004. Cyberterrorism: The Sum of All Fears? Studies in Conflict & Terrorism 28, 130. https://doi.org/10.1080/10576100590905110

Wheeler, W.A., Cohen, N., Betser, J., Ewart, R.M., 2018. Cyber Resilient Flight Software for Spacecraft, in: AIAA SPACE and Astronautics Forum and Exposition. American Institute of Aeronautics.

World Economic Forum, Marsh & McLennan Companies, Zurich Insurance Group, 2019. The Global Risks Report 2019, 14th ed. World Economic Forum, Geneva, Switzerland.

Wright, D., Laura, G., Lisbeth, G., 2005. The Physics of Space Security: A Reference Manual. American Academy of Arts and Sciences, Cambridge, USA.

Yadav, T., Mallari, R.A., 2016. Technical Aspects of Cyber Kill Chain, in: Abawajy, J., Mukherjea, S., Thampi, S., Ruiz-Martínez, A. (Eds.), Security in Computing and Communications, Communications in Computer and Information Science. Springer, Cham.

Yin, R.K., 2014. Case Study Research Design and Methods, 5th ed. Sage Publications, California, USA.

Yin, R.K., 2009. Case study research: Design and methods, 4th ed. Sage Publications, California, USA.

Yunos, Z., Ahmad, R., Mohd Sabri, N.A., 2015. A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia. Information Security Journal: A Global Perspective 24. https://doi.org/10.1080/19393555.2014.998844

Zelkowitz, M.V., Wallace, D.R., 1998. Experimental models for validating technology. IEEE Computer 31, 23–31. https://doi.org/10.1109/2.675630

Zhang, H., Yuan, H., Li, G., Lin, Y., 2018. Quantitative Resilience Assessment under a Tri-Stage Framework for Power Systems. MDPI Energies 11, 1427. https://doi.org/10.3390/en11061427

Zissis, C., 2010. China’s Anti-Satellite Test. Council on Foreign Relations.

Appendix A

Table 64 – Examples of Cyber Terrorism Definitional Propositions Over Time.

Ref	Year	Cyber Terrorism Definition
Akhgar et al. (2014)	1980s	"the convergence of cybernetics and terrorism"
Pollitt (1998)	1998	"the premeditated, politically motivated attack against information, computer systems, and data which result in violence against non-combatant targets by subnational groups"
Denning (2000)	2000	"Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear."
Stambaugh et al. (2001)	2001	"The premeditated, politically motivated attack against information systems, computer programs, and data to deny service or acquire information with the intent to disrupt the political, social, or physical infrastructure of a target resulting in violence against non-combatants. The attacks are perpetrated by subnational groups or clandestine agents who use information warfare tactics to achieve the traditional terrorist goals and objectives of engendering public fear and disorientation through disruption of services and random or massive destruction of life or property"
Lewis (2002)	2002	"the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population"
Nagpal (2002)	2002	"the premeditated use of disruptive activities or the threat thereof in cyber space with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives"
Foltz (2004)	2004	"an attack or threat of an attack, politically motivated, intended to: interfere with the political, social, or economic functioning of a group, organization or country"
Weimann (2004)	2004	"the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)"
Czerpak (2005)	2005	"politically-driven attacks perpetrated by the use of computers and telecommunication capabilities, which lead to death, bodily injury, explosions and severe economic loss"

United States Government (2006)	2006	“a criminal act perpetrated by the use of computer systems and telecommunication networks causing violence, destruction and/or disruption of services to create fear due to confusion and uncertainty within a given group or population, with the goal of motivating a government or population to conform to a particular political, social, or ideological agenda”
Denning (2007)	2007	“highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction and disruption against digital property.”
Mantel (2009)	2009	“highly damaging computer attacks by private individuals, designed to generate terror and fear to achieve political or social goals”
Mshvidobadze (2011)	2011	“cyber acts designed to foment terror or demoralization among a target population for some purpose of the perpetrator”
Hua and Bapna (2012)	2012	“an activity implemented by computer, network, Internet, and IT intended to interfere with the political, social, or economic functioning of a group, organization, or country; or to induce physical violence or fear; motivated by traditional terrorism ideologies”
Bosch (2012)	2012	“the use of cyber tools to interfere with or destroy critical information infrastructure to cause casualties or destruction so as to affect change in government policies”
Osman et al. (2014)	2014	“almost any politically or socially motivated use of information technology by terrorists to perform attacks against computers, networks and information systems resulting in violence against noncombatant targets, and causing injuries, bloodshed, or serious damage or fear”
Akhgar et al. (2014)	2014	“The use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation amongst (part of) the general public, or to influence political decision-making by the government or an international governmental organisation; made for the purposes of advancing a political, religious, racial or ideological cause; by affecting the integrity, confidentiality, and/or availability of information, information systems and networks, or by unauthorized actions affecting information and communication technology based control of real-world physical processes; and it involves or causes: - violence to, suffering of, serious injuries to, or the death of (a) persons(s) - serious damage to a property - a serious risk to the health and safety of

		the public - a serious economic loss - a serious breach of ecological safety - a serious breach of the social and political stability and cohesion of a nation."
Kenney (2015)	2015	"These four elements—computer generation, political motivation, physical violence, and psychological coercion—are the essential attributes of cyber terrorism. To qualify as cyber terrorism, an act must contain all four properties, the combination of which distinguishes it from its broader genus and other cyber-attack species, such as hacktivism and cyber-warfare."
Yunos et al. (2015)	2015	Motivation: political, ideological, social, economic Target: Critical National Information Infrastructure computer systems, Critical Infrastructure, civilian population Impact: mass disruption or seriously interfere critical services operation, cause fear / death or bodily injury, severe economic loss Method of Action: unlawful means, illegal acts Domain: cyberspace, borderless Tools of attack: network warfare, psychological operation

Appendix B

Table 65 – Examples of power system definitional convergence since 2016

Ref	Year	Resilience Definition	System Features	Threat Event Features
Jackson and Fitzgerald (2016)	2016	"the ability of a system to degrade gracefully under extreme perturbations, and recover quickly after the events have ceased"	degrade gracefully, recover	extreme perturbations
Arghandeh et al. (2016)	2016	"the resilience of a system presented with an unexpected set of disturbances is the system's ability to reduce the magnitude and duration of the disruption. A resilient system downgrades its functionality and alters its structure in an agile way."	reduce magnitude and duration of disruption	unexpected disturbances
Friedberg (2016)	2016	"resilience in a system is rooted in two potentials. The absorbing potential is the degree in which challenges can be handled without performance degradation. The recovery potential describes a system's ability to restore normal operation in the face of challenges."	absorption, recovery	any challenge
Thompson et al. (2016a)	2016	"the maintenance of the nominated state of security"	security maintenance	-
Thompson et al. (2016b)	2016	"resilience is maintained if and only if a security breach is detected, contained and resolved"	detection, containment, resolution	security breach
Liu (2016)	2016	"resilience focuses on low-probability, high-consequence events"..."extending the focus beyond preparedness,	preparedness, mitigation, response, recovery,	low-probability high-consequence events

		mitigation, response, and recovery, the measure of a resilient system should assess whether social well-being has indeed been preserved after a critical event."	preservation of social well-being	
Baros et al. (2017)	2017	"the ability of a CPS to sustain and recover from extreme and severe disturbances that can drive the system to its physical operational limits"	sustainment, recovery	extreme and severe distrubances
Bie et al. (2017)	2017	"the ability of an entity to anticipate, resist, absorb, respond to, adapt to and recover from a disturbance"	anticipate, resist, absorb, respond, adapt, and recover	any disturbance
Friedberg et al. (2017)	2017	"resilience of a system depends on three potentials. The absorbing potential (the ability to withstand negative effects), the recovery potential (the ability to recover nominal performance during or after a challenge) and survivability (the ability to prevent system collapse)."	absorption, recovery, survivability	negative effects, challenges
Panteli et al. (2017)	2017	"the ability of a system to anticipate and withstand external shocks, bounce back to its pre-shock state as quickly as possible and adapt to be better prepared to future catastrophic events"..."operational resilience, as its name suggests, refers to the characteristics that would secure operational strength for a power system, e.g., the ability to ensure the uninterrupted supply to customers or generation	withstand, bounce back, adapt	high impact low probability catastrophic events

		capacity availability in the face of a disaster. The infrastructure resilience refers to the physical strength of a power system for mitigating the portion of the system that is damaged, collapsed or in general becomes nonfunctional."		
Gholami et al. (2018)	2018	No succinct definition is provided, but the following statement is made which summarises the paper's perspective on resilience: "assess the resilience by evaluating the system performance in each sequential phase of the system temporal behavior (i.e., avoidance, survival, and recovery) following the given HR [High-impact Rare] event."	avoidance, survival, recovery	high-impact rare events
Zhang et al. (2018)	2018	"anticipate possible disasters, adopt effective measures to decrease system components and load losses before and during disasters, and restore power supply quickly. Additionally, valuable experience and lessons can be absorbed from disasters suffered, to prevent or mitigate the impact of similar events in future."	anticipate, adopt measures to decrease losses, restore, learn from experience	disasters
Hickford et al. (2018)	2018	"resilient infrastructure systems should be able to anticipate and absorb any disruptions, then adapt and recover quickly"	anticipate, absorb, adapt, recover	any disruptions

Clark and Zonouz (2019)	2019	"cyber-physical intrusion resilience aims at i) full correctness maintenance of the core (possibly empty) set of crucial sub-functionalities despite ongoing adversarial misbehaviors. Put in other words, it is acceptable for non-crucial sub-functionalities to be affected (partially degraded or complete failure) temporarily; and ii) guaranteed recovery of the normal operation of the affected sub-functionalities within a predefined cost limit, so-called resilience threshold."	maintenance of core crucial functions, recovery	adversarial misbehaviors

Appendix C

The full transcript of the case study interview regarding the launchpad mission control system (MCS) security and resilience is provided in this Appendix. Minor redactions have been made to remove any identifiable information regarding the expert respondent and their organisation for the purposes of privacy, security, and intellectual property. Some general modifications were also made to improve clarity, for example removing filler words such as ‘um’, ‘uh’, and ‘you know’, as well as any double-up words that can be common in verbal speech but reduce clarity in written text. No information of importance to the study has been modified in any way that may impact the integrity of the data.

Interviewer: So, this is one of the final findings out of the Delphi study. And the idea is that it's supposed to represent an end-to-end knowledge domain for security. And that's beyond cyber security. The original intention was just for cyber, but as we started to build it out, we realised everything's a bit too interlinked for that.

Expert Respondent: I would agree with that statement. Yeah, I'm finding exactly the same.

Interviewer: Yeah, so anyway, I'll give you a quick overview and then I'll run you through what we're gonna do. But, just before I get to the overview for your own context, essentially what I've got here is just a blank version of this knowledge domain table, and the goal is that we'll put in a couple of words in each one for some high level security controls that you're aware of being in place for the space system you are responsible for. So, System 1 in this case will be, well, how about I ask you that question. What kind of system have you got exposure to?

Expert Respondent: I'm cheating by looking at your slides and it looks like you want me to give you three systems?

Interviewer: These ones are pre-prepared for other respondents, so that's fine.

Expert Respondent: Oh, okay. Right.

Interviewer: So, for you, I believe it's a launchpad, but I'll let you say that. And then we've got this one, which is going to be a satellite constellation. And honestly, I don't think we're gonna manage to get a third respondent. But that's okay.

Expert Respondent: Oh, I might be able to help you with that. Well, yeah, you never know. Maybe I'll just give you a ten second spiel. So, I'm looking generally after the mission control systems for {redacted}, which is more the ground based segment around the range you know, the air situational awareness, maritime situational awareness. You know, turning on water systems, controlling drones and media and cameras and communications. Right? Now, that includes ground stations, so receiving telemetry. Ground segment is probably the bit I'm best at, or I know the best. For the up-and-coming launch in a couple of weeks I've also been working with some people on payloads. So, we're putting up three payloads from three different customers. One being ours and looking at how to make sure that the local bus talks to each other. Making sure frequency management, that's been a huge thing. Frequency security. And then the other pieces around it, like the people and the physical, blah, blah, blah. So, to just go back to your original question, yeah, I'm calling it mission control or ground segment.

Interviewer: Yep. No, that's fantastic. Thanks for that overview. Yeah, that's perfect. And you know, if we get onto payload stuff, then that's cool too.

Expert Respondent: For sure.

Interviewer: But that's some really good background, so, I'll give you an overview. I understand that there are gonna be a number of boxes that either you won't have visibility on or it won't be relevant to the system. And that is, that's totally fine. So because this is supposed to be an agnostic framework it is quite comprehensive. The way that this table is structured is we've got our different segments here. It originally started with just the ground and space segment, and then after three iterations, turns out that we've had a bit more granularity here around governance, human and C3, which in this case is communications, control and computing.

Expert Respondent: Okay. Cause I was gonna ask you, what are your three Cs? Cause usually it's either two Cs or four Cs or five Cs. What's the going with the three Cs?

Interviewer: That's right, yep. These days I see C5ISR, and you know, the acronyms just keep getting more complex. So, the reason why we've only gone for the C3 is that the other two Cs are kind of scattered across, the cyber being one which is covered here {in the knowledge domain table}. And then the ISR component I see is more of a function of the system rather than a segment of the system, which also goes across all of them. Yeah, so those are the segments. And, and that's essentially the, I don't wanna use the word taxonomy, but I'm going to, cuz nothing else is coming to my mind. So, it's the basic taxonomy that we've used for a space system. And then along the sides here, the way that we've tried to build out the knowledge domain is taking I suppose a threat-based approach. So, looking at what kind, if we're talking about security, what are we trying to secure against? And in broad strokes, that is non-malicious, which is generally more InfoSec or just general engineering. But it's there for completeness. Cyber, I think everyone's quite familiar with that one. Electromagnetic security, formally electronic warfare. I understand it expanded, which is a good thing, especially for space systems because of you know, LPI/LPD kind of waveforms and stuff. And then finally, kinetic, which is your, from the ground segment perspective, your physical security. But you can also include things like preventative measures that you may build into the space system if we're talking about military systems. And, you know, for very advanced systems, I know there's some discussion around being able to manoeuvre, the International Space Station is a good example. So, they're manoeuvring around space debris that the Russians created in their recent ASAT test.

Expert Respondent: So, yeah, and there's definitely literature that I'm seeing in my role around some of that stuff.

Interviewer: Yeah, so that's the thousand-foot view. And at the cell level I've just put words in here with some examples. But each one effectively is just a correlation. So, we're looking at, in this cell, for example, governance measures that protect against non-malicious. We're using the word adversities, very academic term, but it was originally threats and a few people had issue with that because it's not quite all encompassing.

Expert Respondent: I use the word, and again certainly not telling you what to do, I use the word actors.

Interviewer: Yeah, definitely. I think at the end of the day, in this context at least, we can think of them synonymously.

Expert Respondent: Cool.

Interviewer: So, let's step through. The outcomes of this will form the case study to essentially prove that we've tested it and there's data that we can get out and make use of the framework. So, we'll see what comes out of it. But the goal is that I'll run it through a theoretical cyber physical case study. Cyber physical meaning I'm essentially taking the most extreme threat that I could think of, which was a cyber terrorist, a cyber terrorist actor with the capability to conduct a cyber physical attack.

Expert Respondent: So, yeah, let's say like nation state or, I can't remember what the tier is, like tier four, I think it is off the top of my head.

Interviewer: Yeah, exactly. Like a high tier actor with capability and intent to cause maximum damage. In reality we know that that's not exactly the case because a lot of the actors that we see are state-based and there are implications both politically and for your own space systems if you cause debris and other things like that.

Expert Respondent: The example I'd use is Taiwan trying to put up a rocket in Australia. China might not like that too much, right?

Interviewer: Exactly. Yeah, that's a perfect example. And because it is such an international sphere as you know, it is very political. That is one of the reasons why we steered away from the cyber warfare part. I think it's an extremely interesting and an extremely relevant example, but it's almost too relevant in that it would make the case study unruly.

Expert Respondent: Agree. There's so many factors. So, yeah, touching on the classification issue too, right?

Interviewer: Oh, exactly. And I've tried very hard to keep away from that because I don't want any of this knowledge to be, you know, scooped away into some little hole that only a few

people see. Because I think, at the end of the day, it's in everyone's interest for our space systems to be secure. So, this needs to be public information, in my opinion.

Expert Respondent: Great.

Interviewer: So, without further ado, let's step through. Let's start with the governance segment. I think because that's kind of overarching and it may set the scene and then we'll come down and dig down into the ground parts. And if you've got awareness over the human parts for example, any security training and things like that, we'll get to that too. But yeah, if that works for you, we can go cell by cell.

Expert Respondent: Yep.

Interviewer: Cool. So, the first one we're looking at is governance to assure against non-malicious adversities. So, things like business continuity plans, DRP, there will always be legal regulatory stuff.

Expert Respondent: So, we've got literally two guys and that's all they do.

Interviewer: Yeah, so I might as well just drop that straight in.

Expert Respondent: So, I would say 10% of the {redacted} workforce is literally focused on regulatory compliance.

Interviewer: Are you aware of any SOCI movements? Cause I know SOCI's come out and added Space Tech to the list.

Expert Respondent: Actually. Okay, so {redacted} is, I don't really know his full background, he sort of touches on that. He spent some time over in Canberra working with some of the folk. He's been talking to me and some others around trying to create one of those for the Australian space.

Interviewer: Oh, that's cool. There you go.

Expert Respondent: Yeah. {Redacted} wanna try and drive and lead that, because obviously they see the cash in that.

Interviewer: It is an interesting one because it's very high level and there's not much to it at the moment. So, it would be good to have some lower-level guidance, but hopefully this work can help with some of that as well eventually.

Expert Respondent: So, in this space we are doing things like, and I gotta be honest some of this stuff is pretty loose, like, disaster recovery plans, backup plans, quick recovery plans such as imaging all of our equipment. If something falls over, we can rapidly redeploy. Those kinds of, not clustering and not, you know, high end enterprise equipment… It's like, you got one NUC, but the whole, you know, there's 10, eight of them are being used and then two are hot spares. So, you lose a piece of kit, you image that onto another one, and you're up, sort of. It's a poor man's version.

Interviewer: I'll call it redundancy for this one. Cause yeah, you're right, High Availability tends to insinuate cloud and stuff like that as well.

Expert Respondent: We'll get there. What else do you have in there? V&V. So, V&V we do some of that and I do that in the context of, I have an IRAP assessment done on my systems. Only because I know the guy and I trained him, so he does it for cheap. And we have third party do reviews of one of my big pieces of work, the tech security plans, which is a requirement for the ASA licensing. So that probably falls under that governance piece as well. I think it's Section 50 of the Space Act or something, off the top of my head. Governance. Yeah. V&V, compliance, legal, disaster recovery. Assurance, probably not so much, we should, but we don't.

Interviewer: Mm-hmm.

Expert Respondent: So cyber, from a governance point of view. Yeah, we do IRAP. What else do we do there? You know, we're running things like Splunk and Zeek and those things to give us some sort of monitoring, logging, auditing.

Interviewer: This may be a little bit low level, but out of curiosity, is it centralised?

Expert Respondent: Yes. Well, as best it can be. Yeah. As best it can be. Have I got every single node? No.

Interviewer: It's difficult, especially when you're dealing with OT stuff.

Expert Respondent: Exactly, yeah. Yeah, that's why I said not every node. I had some people come through and do a tour of it and one young engineer goes, oh, I thought you'd be on Linux for everything. And I was like, well, yeah, in theory, but yeah, everybody wants to see a Windows.

Interviewer: No, that's right. And especially if you're getting IRAP, it's a hundred percent Windows focused. And so when you're trying to do IRAP on any Linux stuff, it just doesn't make sense. It's really, it's like fitting a square peg into a round hole.

Expert Respondent: Yeah. That's right.

Interviewer: So yeah, I mean, I think that's pretty good for this section. How about supply chain?

Expert Respondent: Supply chain, yeah, best intent. But yeah, not so much. Like, I get it. But yeah, trying to have a small business understand that is really hard. Well, understand it and do anything about it is also hard, right? We've been using a lot of raspberry pies and you know, all of those kinds of bits and pieces, so, you know, you got no idea.

Interviewer: Yeah. Do you do any secure code review?

Expert Respondent: {shakes head} Should we? Yeah, we tried…when did we actually try to do that? We got another mate of mine, {redacted}, who used to do a lot of coding with me. He started to do some reviews and then we just couldn't afford it to be perfectly honest.

Interviewer: No, that's fair enough. It’s, yeah, especially in small companies, like, this stuff you can spend more than you will ever make on it.

Expert Respondent: Yeah. We just couldn't do it. And a lot of it now is because {redacted} has got an affinity with Matlab, so a lot of the stuff we're doing is in Matlab. So, you can still do code reviews, right, but a lot of us just pull boxes together.

Interviewer: Yeah, makes sense. Any threat intel?

Expert Respondent: Not through {the company}. Obviously, I get a bit through my {redacted} work. Like, I get emails. A million a day. Do I read 'em? No. I get the ASD security reporting as a small business sign up. So, we get some come through. But no dedicated function. Best intents.

Interviewer: Reasonable for a small company.

Expert Respondent: Yeah, I'm basically one guy and I've got a tech that's like a turn the screws kind of guy working for me.

Interviewer: Ah, yeah. Cool. I think that's probably a good level for the governance. Yeah. Do you know anything about the, any like, EM testing, or…

Expert Respondent: Yeah. So, this has been a huge problem for me. So, me and one of our, one of our young lawyers in the regulatory team, well, one of the two. We've been trying to work through the ACMA licensing. So maybe not so much electromagnetic threat, but electromagnetic governance is certainly a huge problem for us.

Interviewer: Yeah. Do you have TEMPEST testing?

Expert Respondent: Oh, TEMPEST testing. Yeah. So, {redacted} did our building and all of that kind of stuff. So, this is the tricky bit. I know lots and lots of stuff about that. What is {the company} doing? As a small company? Yeah, nothing.

Interviewer: Yeah, okay.

Expert Respondent: I can say, and this is not around the electromagnetic pieces, it's actually around ASA requirements, the ASA regulator comes out and checks the launch vehicle to make

sure it doesn't have any nuclear payloads. With a Geiger counter. So that's a fascinating little tidbit.

Interviewer: Yeah, that is one that actually is a very interesting thing for you to bring up because that didn't come up at all in the Delphi study. I guess I'll say nuclear inspection.

Expert Respondent: Yeah, it's pretty funny, he comes and holds the Geiger counter up and goes, not sure if he knows how it works, but, you know, he ticks the box. So, that's interesting. And on the electromagnetic one, yeah, no. So, we run a spectrum analyser on-site as part of our countdown our integrated countdown. We do a spectrum, I don't wanna say management, cause it's not that, what would you call it? A spectrum analysis check, you know, to make sure there's no weird signals.

Interviewer: Okay. So basically is that for availability requirements?

Expert Respondent: Yeah, so to make sure that nothing is popping up in the bands that we're about to try and use for our ground station and for our telemetry, you know, to make sure that those slots are clear. The other element, and again, I'm not the explosives expert, is to ensure that all the RF around the launch vehicle is okay that there's not a spike of some sort.

Interviewer: Yeah, that's, that's actually really good, honestly.

Expert Respondent: It often comes down to the experience of the people.

Interviewer: Yeah, I guess it does. Now, you said you were having some spectrum regulation or spectrum management concerns?

Expert Respondent: Oh, challenges is one word. So, what we're finding is the ACMA, there's so many spectrums that are blocked out. And there's reams of doco on this. The licensing of spectrum trying to find a free slot that's allocated for space use, something that doesn't clash with existing bands has been a huge challenge.

Interviewer: Yeah, that's actually something, in one part of my research at least, that came up as one of the issues for space moving forward. Because spectrum is directly equivalent to what services you can provide, how much money you can make, for example.

Expert Respondent: Okay. So, to get our radars accredited, all of that, I've actually got a meeting in about 15 minutes to talk to our radar people about some of their technical specs. Because of frequency issues. So huge problem.

Interviewer: Right. Well, let's definitely note that on the slide. Let's go to the kinetic side. This is very generic. Stuff like, basically, how the site is managed. There's building sort of inspections and stuff like that.

Expert Respondent: I would probably go, I know you've got it in the space segment there, but I would probably say kinetic governance. The big one would be insurance.

Interviewer: Oh yeah, of course. Yeah. That's another one that wasn't captured by the Delphi process.

Expert Respondent: Yeah, the amount of insurance we're having to get, I don't know the specifics, but it's lots and it's, yeah, it lands on someone's house and kills someone…

Interviewer: I can only imagine. And, not to mention, you know, most launches don't go so well.

Expert Respondent: That is my experience so far.

Interviewer: Yeah, alright. We can leave that one a little bit light on. I don't know how hugely it will play in the case study anyway. Let's go to the ground segment. And then we can go back to the human segment afterwards. I think, and, well also, I think a lot of what we're saying, even though we're going cell by cell, I'm also getting information that can help populate some of the other cells. There's a bit lot of correlation between then segments, which is why I was hesitant to call it a taxonomy. They're not necessarily distinct from each other, it's more just a framework.

Expert Respondent: I'd agree with that. I reckon that's a fair statement.

Interviewer: Alright, so assurance of ground components. So, things like debris, celestial monitoring and reliability engineering just in general.

Expert Respondent: We do the celestial piece there, we have COLA which is our collision, and what's the o stands for, collision and avoidance, essentially, of existing space-based assets. So, we have a system, well, it's really an internet stream, don't make it sound more complicated than it is, that basically tells us where everything already is and lines up which windows when we can actually launch. Okay? So, we have that system, we call it COLA, c-o-l-a. I think that's a wider used term. So maybe just Google that. Yeah, that's a good one.

Interviewer: Right. I'll do some Googling on that. I'll highlight that.

Expert Respondent: We've got a guy that could talk about that all day long.

Interviewer: That's good. Maybe I'll have to have a call with him at some point.

Expert Respondent: Yeah, I'm happy to do that.

Interviewer: So I think that one's a light one, unless you have anything else to add?

Expert Respondent: Yeah, the software reliability is definitely problematic. I've got a real bugbear about that at the moment. The ICT and telecoms, that's on me. And we've got multi-level of redundancy for those systems.

Interviewer: For the telecom systems, you said?

Expert Respondent: Yeah.

Interviewer: So, telecom system reliability is robust.

Expert Respondent: Yeah, very, very much so. So we've got UHF, we've got SATCOM phones, we've got VoIP systems, we've got mobile phones, we've got, what else we got? Yeah,

it's about, it's about three or four layers of redundancy in that plan. That's probably something that I've actually had got a run of.

Interviewer: That's fantastic. Especially once something's up, that's the only way to deal with it. And it's also, as you know, the vector for cyber attacks. Okay, any sort of SOC or equivalent? But yeah, it's quite a big function, so I don't expect to see that very often.

Expert Respondent: No, we've had third parties offer to do that for us, and then try and indicate that, “oh yeah, we'll do it on the cheap” and then send us six figures, you know, sums of money, you know what I mean?

Interviewer: Yeah, invoices.

Expert Respondent: Yeah, and you go, they're only really available to large organizations, I feel.

Interviewer: Have you got cyber incident response?

Expert Respondent: Yeah, that would be me So, not a serious one, no.

Interviewer: I'll say small CIRT.

Expert Respondent: Yeah. Small in-house CIRT. On-site. So, if something did go wrong everyone's gonna look to me. I'm gonna try and resolve it. If I can't, we'll hold the count down. Give me more time. And then, you know, everything's logged, audited. We try and identify the problem. If we can eliminate it, we will. And then decide whether we crack on. And then obviously we'd feed that into the ACSC or do whatever reporting we need to do. Yeah, for DISP compliance reporting.

Interviewer: That's cool. Do you have any security engineers, or someone involved in… So what I'm looking for here is secure by design practices, really, from a cyber security perspective.

Expert Respondent: So, I'd say we are doing that because I'm trying to, as best I can put in you know, ISM controls. Not to the level that you'd for highly classified Defence stuff, but sort of to try and give it some protection.

Interviewer: No, that's good.

Expert Respondent: So, sort of aiming maybe at like maybe that Protected type level.

Interviewer: Yep, I'm unfortunately far too familiar with the ISM.

Expert Respondent: Yeah, I went to explain it to you, and I went, no, no. He knows.

Interviewer: The only reason why I'm not an IRAP is because I've been fighting tooth and nail to not be.

Expert Respondent: Yeah, I've been thinking about it, but, not my thing. So yeah, I've been through those spreadsheets for red networks. So, I'm trying to sort of limit it to some of the Protected level type stuff. Because, oh, where would you put this, a perfect example. We've got two factor authentication. Beautiful. We get out to the range, no one's got any phone signal. So yeah, it is practice.

Interviewer: I've had my own challenges with MFA lately. I think with the latest hacks, everyone's sort of really looking into them and it's very rarely rolled out well to begin with. And secondly, there's so many problems. Like, half the time it gets sent to your mobile, which, one is a little bit less secure, and two, even if it doesn't get sent to your mobile phone, you still usually need a mobile device to be able to access it as your second factor. And so with remote operations, which is pretty much all critical infrastructure, you have troubles with this. Some people use those old tokens.

Expert Respondent: Oh, the RSA ones. I love the fact that they're usually made {offshore} too.

Interviewer: Yeah, lowest cost dealer. That's often the rule. How about OT security?

Expert Respondent: Again, not really. We should, but we just don't. That's a challenging one. But yeah, it is probably very critical.

Interviewer: Alright, let's go to electromagnetic for the ground. I think we sort of covered this before, but yeah, we kind of did cover this. How about surveillance? So, on-site is there security? Do you have swipe access? Security cameras?

Expert Respondent: We do actually have swipe access. Given everything we do is transportable. We're about to deploy the range. I'm deploying swipe systems at the front gate and to come down to the path. So, we've actually got multiple swipe systems within the range.

Interviewer: That's awesome. I'll note defence in depth for physical boundary security.

Expert Respondent: And we've probably got about 20 security cameras across the range. Is that enough? No, but it's a pretty good start for a small company.

Interviewer: Yeah, that's, I mean, every single thing you add you have to monitor and manage.

Expert Respondent: Yeah, exactly. And then the funny story on that is we got accused then of trying to spy on the topless women on the beach, and I don't think my security cameras are that good.

Interviewer: "You're giving us a lot of credit there". That's funny.

Expert Respondent: So, yeah. We got key locks, but they're not, they're house locks. They're not, you know, SCEC-endorsed or anything.

Interviewer: Okay. Locks, but not SCEC. So, actually on the electromagnetic part for the ground segment, because one of the problems, well, some past incidents, at least at airports that we've seen, have been either incidental or purposeful, what's it called?

Expert Respondent: Jamming?

Interviewer: Jamming. That's the one, yeah. Very obvious word...

Expert Respondent: So, in my tech security plan I've actually got a section. It needs a lot of work, but there's a section in there about jamming mitigations, and one of the mitigations is that the location of the range is remote. And there's a lot of terrain barriers, that's not the word. What the word I'm looking for? Basically, it's a s**tload of scrub. So, if you can get from our control, you know, access to the launchpad, or get close enough, we got probably three or four kilometres of scrub. So, we're saying we got that physical or environmental barrier, whatever word you want to use there, you know, security through distance.

Interviewer: Through inaccessibility.

Expert Respondent: Yeah, inaccessibility, yes. There you go.

Interviewer: I'm just gonna say remote range. I don't think we even need to get to that level, honestly. So, but yeah, that's cool. All right. Human segment. Let's look at that. This one was actually interesting because we've pulled human out as its own segment, which was raised throughout the Delphi study. Essentially the way that we find security vulnerabilities these days is through people, so, I was happy to see this development. Let's get into it a little. I guess the main thing that I'm probably gonna be interested in here, for the case study… Workplace safety and stuff, you know, that's all important, but it's probably not gonna come out in this study. But security culture I'm very interested in. Maybe I'm putting you on the spot here, but how would you describe your security culture?

Expert Respondent: Quite high because I hammer it into people. I've got them a little bit, I don't wanna say bluffed, but fooled. Then they're all like, oh, {redacted name}, can I do this?

Interviewer: Nice.

Expert Respondent: So we've basically got quite a good culture. They good with reporting. I've got them all cleared now to NV1. You know, we've got our DISP compliance. I give them a security brief as per the DISP, but I also will give them one when we get out on range, which will be a physical one and a cyber security one. And then I actually also bring in a third party, which is my IRAP. He'll probably do it remote this time. So that then they can hear it from

someone else as well. So it's not just {redacted name} talking s**t, it actually comes from that third party as well.

Interviewer: People always respect a third party for some reason.

Expert Respondent: Yeah, I know, right? Yeah, no, it's weird. So, he gives them a couple of examples out of the SANS courses and goes, oh look, you can do this. And everyone goes, oh. So, we do, we do all that.

Interviewer: That's actually really good.

Expert Respondent: Yeah, I'd like to think I'm the guy in the background doing a lot of that, so, there you go.

Interviewer: So, you said you did some briefings and stuff. Do you have routine cyber training and awareness?

Expert Respondent: Yes, we do. I've got a yearly refresher slide deck which is like a DISP one that I put a bit of flavour in, and then a new starter one. And then I do one which will only be a verbal at the start of the campaign.

Interviewer: Nice. So, campaign specific. That's really good. How about identity and access management? I know that that covers a huge amount, but for the mission control system at least.

Expert Respondent: So, given the containers are small and everyone's known, you sort of have a little bit of that eyes on approach, you know, obviously someone who's not meant to be there… We're gonna know that obviously is not scalable, but for what we're doing that works. We've got security cameras in those containers. We've got, you know, password protections, two factor authentication on some of the systems, which {redacted} mentioned is a bit of a risk. And we have, ID passes with varying levels of security. So, staff, client, contractor, and whether they can go down to the pad or not. So, we've got that actually pretty well, pretty solid.

Interviewer: That's really good. And the, oh no, it doesn't matter. I keep going into lower levels in my mind just because I'm used to going through a security audit, but that's not what I'm doing here, so I don't need to know if it's a group password or not.

Expert Respondent: That's fine. No, it's all individual pass. Some systems have a single password that multiple people know. Multiple people being two. So, that is a security measure as far as I understand.

Interviewer: Exactly. You said you had personnel vetting, NV1?

Expert Respondent: Yeah, for all staff. So, NV1 minimum. Obviously, some of us have got more. But for {redacted company name}, NV1.

Interviewer: Alright, so I think we've covered a lot of this stuff. Bug sweeping. How about that?

Expert Respondent: I don't have capability to do that. We have enough trouble getting the fucking flies out of there let alone anything else.

Interviewer: No, that's really fine. I don't think it will come out in the case study because that's more of a cyber warfare tactic rather than cyber terrorist tactic.

Expert Respondent: But, yeah, I've got 'em all well trained with, you know, USBs and all of those things. We've got dedicated USBs for various transfer functions and no one holds a USB other than me. And they're, you know, I'll say they're signed out, but all of that kind of stuff.

Interviewer: Actually, that's a good point. We didn't capture any registers in the governance section. So, I can probably say for cyber governance we've got a media register?

Expert Respondent: So, in theory I have all of that. I've just gotta write it yet, before we get on-site.

Interviewer: That's alright. And the other thing, which is a huge thing that we didn't even talk about yet, what kind of risk management practices are there? Is there a cyber risk management plan or anything like that?

Expert Respondent: {shakes head} I have a risk matrix and identified risks with mitigations in my tech security plan. But it's definitely not a standalone plan and it's not something I'd be proud of to, you know, throw on the table in front of you and go, “there you go, job done”.

Interviewer: Fair enough.

Expert Respondent: It's a couple of pages maybe of spreadsheet. It's pretty loose.

Interviewer: Is there any, and I guess this sort of ties into the supply chain security as well, is there any board level representation? Like, is there a CISO that sits on the board?

Expert Respondent: Oh, that's a hot button. There should be. So, I am that person and I am the chief security officer. Do I sit on the board or present to the board? No. I should, but I don't.

Interviewer: They've got you as the one stop security shop.

Expert Respondent: Yeah.

Interviewer: Alright, well we'll move somewhere else. So, kinetic for the human segment. Social engineering awareness and stuff like that. Have we got anything?

Expert Respondent: Fascinating. So, that's a problem. I've actually had that come up. Are we trying to put in mitigations? Yes. Are we training our staff around this? Yes. Have we had an incident? Absolutely.

Interviewer: Yeah, no, that's totally fine for this level. Okay, so I think we've got, you know, obviously it's pretty high level, but that's all we're going for. I think the lower level stuff should come out in future research when we have a bit more, you know, this research is obviously suggestive. At some point it could be a standard, but we're not going to that level just yet. So,

C3 segment, let's step through that. And then if you've got anything on the space segment for mission control, but I'm not sure how much there might be.

Expert Respondent: Yeah, it depends whether you're looking at that as sort of the ground station link, or whether you're talking about that as just the payload, or you're talking about that as satellite-to-satellite comms. What do you got?

Interviewer: So, essentially it's the payload. And then C3 we split out because there was a lot of discussion like before. Like I said, we started with just ground and space segment and everyone's like, what about the comms stuff. And then we ended up separating it out because the links are basically their own component in a lot of ways. But there's a lot of crossover. I do have a diagram showing how all of these relate to each other. But essentially, the governance segment is the overarching box or bubble. And then inside that you've got the human segment, governance basically controls your humans. So, the government segments defines your scope and puts administrative controls, et cetera. The humans do the stuff, as we know and lament in security. And then underneath that you've got your C3 segment, which essentially connects these two together and allows for human input. So that's the way we've looked at it.

Expert Respondent: Yeah, that makes sense.

Interviewer: So, I'm sure we've captured a lot of the C3 segment already. I think elements of this I'll have to re-jiggle, but what we're looking at is your data management. We've talked about redundancy, reliability, engineering, but do we have any data management. Usually when we're talking about critical infrastructure, it's primarily availability oriented, but in the space domain there is often a lot of sensitivities around aspects. So probably it's an especially challenging space because you need to look at confidentiality often equally to your availability, which is tough.

Expert Respondent: Yeah. So, what I've been finding from my experiences is the data management is very timely. Like, the data is sensitive, but it's only sensitive for a short period of time. All of a sudden the data is not that important. It's sort of what I'm getting from the client space every time I go, “okay, so now we've got your telemetry and we'll need to secure it, and how are we gonna transport it back to your home country? Because we don't wanna do it on the internet. Do we wanna do like some sort of secure USB?” and they're like, “We don't

give a fuck". And I'm like, "oh…oh, ok". That's interesting, isn't it? Every time so far for I'll say four, five clients. And, same answer every time.

Interviewer: Would you say it's specific to pre-launch?

Expert Respondent: Pre-launch, everyone gets jittery. Post-launch, all of a sudden no one cares. Yeah.

Interviewer: Wow. That, that is very interesting.

Expert Respondent: Yeah, that's what I've found.

Interviewer: Well, I've taken note. I'm not sure how that will come out, but that is an interesting point to note because I feel like we haven't elaborated on that in the discussion so far.

Expert Respondent: Yeah, you're probably getting there now.

Interviewer: Yeah, pretty close. Okay, so Cyber C3 we're looking at cryptography, which is less interesting given what you just stated. We talked about secure coding briefly. I'm interested, on any of the payloads that you deal with, do you come across IoT at all?

Expert Respondent: What I'm finding is a lot of the payloads are thrown together IoT devices, yeah. They're not built from the ground up at all. I'm not seeing payloads that are something that you'd put in geostationary that are a serious piece of kit. It's lots of people smashing together raspberry pies, other stuff.

Interviewer: So probably not so much security on there. I never expected anything more, in the space race environment especially.

Expert Respondent: Yep. That's a big problem. It's all about who gets up there first and how you can monetise it, not secure it.

Interviewer: I think that that's an interesting vector. Speaking of which, is there anti-malware on the ground segment?

Expert Respondent: On my stuff, yes. On payloads, I definitely haven't seen anything like that.

Interviewer: I don't think it exists. We talked about security monitoring, how about on the comms link?

Expert Respondent: {shakes head}

Interviewer: Okay, is there encryption on the comms link?

Expert Respondent: On the comms link? Not on ours. On some of the others, I wouldn't know, but every time I've raised that with a client their answer has been no.

Interviewer: Yeah, they're very fearful of the power that it takes. And the extra bandwidth of the very limited…

Expert Respondent: Yep, yep, and the extra coding and the, you know. People don't seem to wanna do it. Nah, it's a big gap.

Interviewer: It's a massive gap.

Expert Respondent: Yeah, I talk about that a lot. We've been contemplating, and we literally can't afford it, to only use our drones for a single mission. Replace them because of that whole challenge that we probably both know a lot about.

Interviewer: Yeah, that's right.

Expert Respondent: Size, weight, and power.

Interviewer: Yeah, exactly. Okay, how about, if we're not doing encryption stuff, are we doing any integrity checks for data received back or anything like that?

Expert Respondent: No, no CRC type stuff. Nothing like that.

Interviewer: Well, this is good for me, for my case study.

Expert Respondent: It gives you some gaps to talk about.

Interviewer: Exactly. Yeah, good in the theoretical context.

Expert Respondent: I'm trying to fill all the holes so you've got nothing to talk about, but I just haven't got there yet.

Interviewer: I mean, I don't think you will, unfortunately for everyone.

Expert Respondent: Nah.

Interviewer: Yeah… How about electromagnetic monitoring and integrity checking? I mean, I'm guessing not the integrity checking, it's even more advanced.

Expert Respondent: Yeah, no, no, and no.

Interviewer: You've got signature management?

Expert Respondent: You could maybe say that. Well, we've got frequency management. We know what frequencies we're supposed to be getting and we're making an attempt. I wouldn't say signature as in we know what's coming in on whatever the frequency is, say, {redacted} megahertz. We should be seeing a packet that looks, you know, like this proper EW signature. We're definitely not doing that.

Interviewer: Okay.

Expert Respondent: That'd be way…

Interviewer: Yeah, that's very advanced. As soon as we get into the electromagnetic stuff, it gets very expensive and lots of equipment.

Expert Respondent: Oh yeah. Wow, equipment and experienced personnel that are very expensive as well.

Interviewer: Yeah, and only a handful of them around Australia. Now, I'm just trying to think electromagnetic pulse and stuff. Is there any control on the comms link?

Expert Respondent: Yeah. If someone works out what our payload's gonna transmit through some means, whether they dig out our licensing permits for particular frequencies or they get access to our technical specs and then they try and jam it by something simple like overpower. What are we gonna do about that?

Interviewer: Yeah, actually that is interesting. I'm sure you're following it, but SpaceX, they were getting jammed like crazy over in Ukraine and they were able to defend themselves pretty well, which was very impressive.

Expert Respondent: I'd like to know what they did.

Interviewer: They must have just had advanced military technology being pumped into them from the US as like a secret thing down the side, because, I don't know.

Expert Respondent: So much going on.

Interviewer: Yeah, absolutely. Good for people like us.

Expert Respondent: Oh yeah, it keeps us tight.

Interviewer: Yeah. And actually, that's a realisation that came out even, especially, for the kinetic and the space segment. I feel like this is exceptionally difficult to achieve.

Expert Respondent: Yeah, I'd agree with that.

Interviewer: Yeah. And I doubt you guys are doing any kinetic defence against your C3 segment? I think that's more of a military capability.

Expert Respondent: We've talked about TACLANEs and things like that for when we go remote mission control, but it's, except for the limited technologies, it's really just cost. We can do simple stuff, but nothing, yeah.

Interviewer: And the space segment for mission control, you are the expert on this one, but I think it is mostly N/A? Is this most of it?

Expert Respondent: Yeah, I think so. Let's just double check. Material reliability, no, nothing there I'd say. Assurance of components? No. We're not there yet. We're not putting up big stuff yet.

Interviewer: I think, at least for {redacted company name}, I feel it's probably down to your clients to do a lot of the protection of the space segment.

Expert Respondent: Yeah.

Interviewer: Alright.

Expert Respondent: I think we got there.

Interviewer: Yep, I think we've got some pretty good stuff there. I can probably stop the recording.

Appendix D

The full transcript of the case study interview regarding the ground station security and resilience is provided in this Appendix. Minor redactions have been made to remove any identifiable information regarding the expert respondent and their organisation for the purposes of privacy, security, and intellectual property. Some general modifications were also made to improve clarity, for example removing filler words such as ‘um’, ‘uh’, and ‘you know’, as well as any double-up words that can be common in verbal speech but reduce clarity in written text. No information of importance to the study has been modified in any way that may impact the integrity of the data.

Interviewer: So, before we get into it there will be a little bit of a process. You know academia, we've gotta do things in a certain way.

Expert Respondent: Yep.

Interviewer: So, here is the table that I sent to you and that you've been involved in throughout Delphi study process.

Expert Respondent: Mm-hmm.

Interviewer: I've got a blank version of it, and the goal is that we'll put in some high-level controls that you're aware of in your system. And then after this, I'll take this information and I'll run it through a case study, which I've pre-prepared a cyber physical terrorist threat scenario, which is, you know, the extreme end of the stick. And we'll run it through the cyber kill chain process and basically test current state versus an ideal resilient state. So, that's the process. How about we start with, maybe you could give me a little overview of the kind of system you work with. So, for example, some of the other ones we've done include a mission control system for a launchpad and some payload stuff. But whatever you work with, that's good.

Expert Respondent: So, ground segments, that’s a definite. And I'm assuming the C3 is the, not just the RF, it's the links between sites?

Interviewer: That’s correct, yeah.

Expert Respondent: Yeah, that's what I assumed. So, I can cover C3, ground, and potentially part of governance and human, in the relation to those segments. Human segment, but not for space. So I don't have much to do with anything in orbit.

Interviewer: Yeah, I’ve found that actually throughout Australia, I mean, we’re a bit nascent.

Expert Respondent: Yeah, well until JP9102 actually happens, I don't think we're gonna have many people in the country who really know it well.

Interviewer: Yeah, absolutely. So, what do you refer to the system as? Is it mission control or just ground station?

Expert Respondent: I'd just call it ground stations, or something like that. Or ground segments, or whatever you want.

Interviewer: Yeah, we'll go with that. Ground station. Alright, so space segment's probably gonna be N/A, which is fine. We've had that for all the other stuff as well so far.

Expert Respondent: Mm. Well, it's probably something useful to document, right? That we just don't.

Interviewer: Oh, yeah. And honestly, I've done a little bit of the payloads, like, we've got some data on the payload, but even then this table ends up usually pretty empty.

Expert Respondent: Yeah, there's not much we can talk about, so, no.

Interviewer: Yeah. No one has onboard detection software or even encryption is difficult with the power that of cube stats and stuff that we tend to deal with.

Expert Respondent: Yeah, I just got back from the US and we did visit a whole bunch of companies that are part of us. And they are doing it. I just can't really talk about it. They barely

showed me. They are doing stuff, so they'll use a DevOps process to secure code, they've done some quite smart stuff with the software. So, it's good from a cyber point of view and there is a lot of work going on on the electromagnetic side.

Interviewer: Oh, yeah.

Expert Respondent: Kinetic, no idea. That's kind of the cool stuff you watch on Space Force, but not seeing much on that. And then the non-malicious, not really seeing much, but they've been doing a lot of work in the non-malicious side for a long time. Cause they don't wanna send up a payload and it gets interrupted or corrupted or damaged from a non-malicious environment. So, they do have very stringent environmental controls in place. So, I'd say that is actually done well. There is a lot done well when it comes to payloads on that area. And cyber's, I just can’t give you too much information on it.

Interviewer: Yeah.

Expert Respondent: So, you can just put in there, environmental controls are in place. Quite strict.

Interviewer: We're using the word adversities, by the way. It's a bit of an academic term, but you know, that's what's come out of the Delphi study. It's a bit more encompassing. In this context we can use it interchangeably with threats or threat events.

Expert Respondent: Yeah. No, that's cool.

Interviewer: Alright, so in the interest of time, how about we get started?

Expert Respondent: Yep.

Interviewer: So, we'll take a cell-by-cell approach, if that works for you.

Expert Respondent: Yeah.

Interviewer: And I'll keep referencing back to this little segment {signalling to the space systems security knowledge domain on the shared screen}. Basically, it gives us some ideas of things that we can talk about. And then, anything else that you may think is relevant we'll note down.

Expert Respondent: {nods in agreement}

Interviewer: So to begin with, as we just said, non-malicious, it's important, but it's there more for completeness because it's more of traditional InfoSec, I suppose, and just general engineering. But, yeah, let's just put some things in there.

Expert Respondent: It is important because it's that notion of disaster recovery brings that up. Because, before cyber was a problem, they should have already had things in place for disaster recovery. So, flooding, absolutely. Fire, or whatever it is, whatever adversity is there.

Interviewer: Yeah. {nods in agreement}

Expert Respondent: So, the good news is that there are good controls for this in my experience.

Interviewer: Okay, cool.

Expert Respondent: And, only speaking for these ground segments, they do have good controls and disaster recovery plans in place.

Interviewer: Business continuity as well, I guess?

Expert Respondent: Between different installations?

Interviewer: For example, the disaster recovery plan may focus on getting the system back online or dealing with emergencies. Whereas, the business continuity plan will focus more on services being delivered.

Expert Respondent: Oh yeah, sorry. Yes, they have good things for both.

Interviewer: Awesome. And in legal and regulatory compliance? I mean, that has to be kind of up to spec, but…

Expert Respondent: Yeah. Cause we're talking sort of military installations, so they're very thorough in this area.

Interviewer: Oh yeah. No one wants to be dragged into the courtroom.

Expert Respondent: No. And, well, it's high availability systems, so they can't allow them to go down. So probably worth mentioning. It's the same for just about any ground-based establishment. You talk about JORN or anything, right? They're all gonna be similar.

Interviewer: Yeah, actually on that note, I know we're in governance segment right now, but on the same trail for the ground segment and high availability, is there redundancy backups, supply chain control, stuff like that?

Expert Respondent: Redundancy, backup, yes. But supply chain is probably not amazing

Interviewer: Yep.

Expert Respondent: As we've seen. First with COVID and then potential threats from where things are made. I think military's no better than any civil system, where we've got similar supply chains, we use a lot of COTS.

Interviewer: Yeah, which is completely standard as you said.

Expert Respondent: Yeah. So they're not special in that problem.

Interviewer: Yeah. Are you aware of any verification, validation, and quality or product assurance kinda stuff?

Expert Respondent: Yep. Very much so.

Interviewer: Cool. To a MIL-SPEC?

Expert Respondent: Yes. Or Australian standards, depending on which part you're talking about. Because not everything gets MIL spec'd.

Interviewer: That's fair. Well, I think we've got that box well covered.

Expert Respondent: Mm-hmm.

Interviewer: So, governance from a cyber perspective. Is there a cyber security strategy for the ground segment?

Expert Respondent: I think it's evolving. So, there is, but you can tell it's, I'd say it's embryonic. Like, it's there, it just needs work.

Interviewer: Yeah.

Expert Respondent: I think everyone's coming to grips with how to do the governance.

Interviewer: Yeah, it's a big piece. Like, cyber risk management?

Expert Respondent: Yep, so there are cyber requirements, now, which is good.

Interviewer: Based on ISM? Or otherwise?

Expert Respondent: Normally ISM. DSPF, sort of, yeah.

Interviewer: Which at the ground segment makes sense. Do you have any OT stuff? Any operational technology?

Expert Respondent: A lot, yeah. That stuff tends to be not as good. That's my job. So, my job is to harden that side. That's not governed by or connected to a classified system. But there's a lot of work going on now, which is good. But that's why I say embryonic. I think that's the embryonic bit, I think.

Interviewer: Oh, okay.

Expert Respondent: When you say cyber strategy for a whole system, I think we've done a lot to look at, you know, that ISM approach. But then when you start looking at the OT, you know, PLCs and cameras and building management, and all those sorts of things that happen, that's an area that kind of just got missed. So that's what we are doing now. So, we are doing it, but I'd say it's embryonic, right? It's still early days.

Interviewer: Yeah, no, that makes sense. It's always the challenging part and it's the same across all critical infrastructure.

Expert Respondent: I think it is, yeah. And once again, I don't think we're any different.

Interviewer: Yeah. No, I don't think so. Certainly not from my experience.

Expert Respondent: Yeah.

Interviewer: Threat intelligence?

Expert Respondent: Yep, certainly feeding that in.

Interviewer: Is it a dedicated function? Or are you sourcing it from ACSC or something like that?

Expert Respondent: It's dedicated.

Interviewer: Cool. That's actually some really good data because it's quite different to the other case study I've done.

Expert Respondent: It is, yeah. And I guess the difference is that we'll have a program office, or whatever would manage a system, and then they would have dedicated IT security managers and offices embedded in that organisation. And that's their job. So, they're meant to take threat

intelligence and make sure that all this governance is happening. So there are dedicated functions and positions and roles, if you like, in the organisation.

Interviewer: Cool, that's fantastic. Electromagnetic governance.

Expert Respondent: Mm-hmm.

Interviewer: So, electronic assurance testing, spectrum management, et cetera?

Expert Respondent: Yeah. Very similar to your non-malicious answer. So, they've got a long history of doing what we'd say was E cubed (E3) or electromagnetic protection and TEMPEST. So E3 and TEMPEST is pretty much core business.

Interviewer: Awesome. Threat intelligence I've got there {under electromagnetic-governance}, but we've kind of covered that. It's often grouped under cyber threat.

Expert Respondent: Yeah, it is a bit weird, and we do it too. We're actually under the same heading, but you look at it and go, well, it's a very different discipline.

Interviewer: Yeah, that's right.

Expert Respondent: Yeah. Guy who does that, he sits outside my office actually. He's a wizard in that area, but we are very different people. We look at different things.

Interviewer: Oh, absolutely. Yeah, they're very different. But both kind of complementary.

Expert Respondent: But hey, you're still looking at vulnerabilities in a system at the highest level.

Interviewer: Yeah. I think at the business level, they look at it and they're like, well, it's an intangible threat. So, you guys are the same. Stick together.

Expert Respondent: Yeah.

Interviewer: Alright, and kinetic governance?

Expert Respondent: Yes, based on that, but really huge for the ground segment, right? So, physical security, the codes, the requirements. Very strong controls. So, things like, layers of security, fencing, and then access, and then access to systems. So they have that whole onion defence model and they have really good governance and policy around that. And auditing as well. So, its probably worth mentioning, it's audited as well.

Interviewer: Yeah, that's good. Is it external and internal auditing? Maybe a bit low level for this…

Expert Respondent: Let me think. Yeah, it would be. Yes. Yeah, it would be.

Interviewer: So, auditing. I think there's something else you mentioned that I might have missed here. Oh, policies. Yeah.

Expert Respondent: Yeah, strong policy.

Interviewer: Dedicated functions, we spoke about before. Same as above.

Expert Respondent: Correct, yeah.

Interviewer: I've just put some of those more tangible controls over on the ground segment side.

Expert Respondent: Sure. Yep.

Interviewer: And while we're on the same topic and I'm looking at kinetic ground. Fencing, restricted access to systems, swipe cards?

Expert Respondent: Yep, definitely. Yep.

Interviewer: Access badges which sort of show your identity, correct?

Expert Respondent: Yeah. And password protections.

Interviewer: Okay. I know multifactor is difficult sometimes with remote operations but is that in place? MFA?

Expert Respondent: No. {shakes head}

Interviewer: Yeah.

Expert Respondent: Well, it might be in places, but generally, no. But it's something that's part of that embryonic.

Interviewer: Yeah. Honestly, it's very challenging anyway.

Expert Respondent: Yeah, like, how to make that efficient and work, yeah.

Interviewer: Yeah. Especially if you don't have phone reception, then what. A lot of these places are remote.

Expert Respondent: Yeah. We're more worried about someone breaking in.

Interviewer: No, that's fair. I guess I can add another control here, remote site.

Expert Respondent: It is a little bit of a layer of defence.

Interviewer: Yeah, perhaps not so intentional, but it kinda works.

Expert Respondent: It does, it does. It stops a lot of people going. “I'm not gonna drive that far”. I'll try and do remote. Or if you do, you're gonna get noticed.

Interviewer: Oh, cause you said cameras as well.

Expert Respondent: CCTV, yeah. Doesn't prevent, but at least observe.

Interviewer: Do you know if it happens to have an alerting feature?

Expert Respondent: Some would, yeah. Yeah, definitely. And they're monitored, so yeah.

Interviewer: Oh, site monitoring.

Expert Respondent: And quite often physical patrols.

Interviewer: I mean, that's kind of ideal for this case study. I wonder how it's gonna play out once I run it through the threat scenario because so far it's looking pretty robust.

Expert Respondent: Just do a supply chain.

Interviewer: Supply chain?

Expert Respondent: Yeah, just a supply chain attack. You just forget all the physical controls and just get straight in.

Interviewer: Oh, supply chain attack. Yeah, pretty much. Speaking of which, on the ground segment, is there any secure code review or anything like that?

Expert Respondent: Yes and no. So once again, I think there'd be examples of it. It depends on the classification of the system.

Interviewer: Okay, cool. Let's go to the human segment just because it's very closely related to the governance. So, non-malicious human segment. We're looking at things like, and honestly the non-malicious human segment is probably less security relevant, but you've got WHS and stuff like that.

Expert Respondent: Which that's all relevant. Everything you've got there is relevant. Yeah, you get the right person out and… All of that stuff is definitely relevant.

Interviewer: So, we've got security training and awareness, legal and regulatory compliance. So this is like your working permit permits and insurance, work safety…

Expert Respondent: Yep. Definitely. Safety, human factors, safety engineering. Yep.

Interviewer: And how would you describe the security culture at a high level?

Expert Respondent: I'd say it's there. It's there for the non-malicious, right? The culture for that is very strong. But when you go into the cyber culture, that's embryonic.

Interviewer: You could probably say it's growing?

Expert Respondent: Yeah, that's probably a better answer because it is growing quite strong and quite fast, so.

Interviewer: I might use the word, developing cyber strategy. So growing cybersecurity culture, strong non-malicious security culture.

Expert Respondent: Yeah, cause the non-malicious, as you said, it's more of a safety culture. And you know, you're talking about non-malicious adversities. So, the things that you can't stop. You can pick on the fire and the flood and the other types of events, and they have a very strong culture to get the system back online. Whereas cyber is new. It really is quite new to them. But they're having to learn really fast.

Interviewer: As everyone is right now, I think.

Expert Respondent: But we do the training and awareness, definitely. I have a training and awareness program. All of those are applicable.

Interviewer: How would you say your identity and access management control is?

Expert Respondent: Pretty good, yeah. I would say it was bad five, ten years ago. Yeah, it's definitely quite good now.

Interviewer: That's fantastic. It's a difficult thing to bring up to spec.

Expert Respondent: There's a lot of work put in that area.

Interviewer: Oh, I bet. Cybersecurity monitoring?

Expert Respondent: There is. But I'd say maybe it's developing because it's there, but it's a long way to go and I think it's not exactly where it needs to be. Well, you could say the monitoring is, a person goes “that's not right”, but we're trying to get a bit smarter about that.

Interviewer: Yeah, some of these copy across, I'm just copying some over {referring to on-screen data entry}. So, data classification?

Expert Respondent: Yeah. Very strong, very strict.

Interviewer: That also applies to the C3 segment?

Expert Respondent: Yeah, it does.

Interviewer: Which we'll get to.

Expert Respondent: Mm-hmm.

Interviewer: Alright, electromagnetic for the human segment. Things like, bug sweeping, cell phone lockers…?

Expert Respondent: They do that. Yep, all of this.

Interviewer: Fantastic. It's gonna be a tough nut to crack.

Expert Respondent: Well, you'd hope so. That it would be a little bit tough.

Interviewer: Yeah. No, I would hope so. It's true. I'm just used to having a few more blanks.

Expert Respondent: Yeah, a lot of our civil stuff is a bit different. They've never felt threatened before.

Interviewer: Yeah. Until now, with what's happening in Ukraine and SpaceX. Very much applies to the civilian space. They see all space as now part of the military domain I think.

Expert Respondent: Yeah. Didn't a train just get hacked in Denmark?

Interviewer: Yeah, it did. Critical infrastructure's always a hot target.

Expert Respondent: It's an easy target.

Interviewer: Oh, absolutely. Between the OT and the usually traditional kind of mindsets that that exist in some of these areas, yeah, it's quite an open door in general. And I think that's a big challenge that we're finding with space. Because it inherits a lot of critical infrastructure problems.

Expert Respondent: It does.

Interviewer: But then you've also got a start-up mentality, especially in the commercial sector. Like, with the space race stuff just gets up put there.

Expert Respondent: Yeah, it’s just like, “just get it out there”. But they didn’t think of security.

Interviewer: They didn’t even think about it, yeah. The faster it's out there, the faster they’re making money.

Expert Respondent: A really hard balance in our area is to, cause we've bought some very smart start-up companies in the US, and trying to temper it a bit so that they know, “yeah, we still want you to be innovative. We still like those features, but we have to add the security”. And that obviously slows them down or they're not wrapped about it. But I think that now they see it. But I think in the early days, they would've been very frustrated.

Interviewer: Yeah, I definitely see that attitude in industry. I mean, it is frustrating at the end of the day having to deal with this stuff. Cause the only reason why you have to do it is because people are assholes out there hacking you, trying to break it. And I think in the space industry a lot of people are a bit more idealistic about some of these things.

Expert Respondent: Yeah.

Interviewer: Okay, so, 'kinetic-human'.

Expert Respondent: All of that. Now, the only thing that probably isn't in there is the social engineering awareness. It's more, security awareness.

Interviewer: I'll say no social engineering awareness training.

Expert Respondent: No. So, we've got safes, locks, building security, we've already covered that, but no social engineering awareness training. Well, they have it built, so you'll have security training and there are elements of it if you like, but it's not a strong part. It's part of an overarching security awareness training. But you and I, we probably know where to go and listen to, you know, the dark net diaries and you realise that that's a great avenue to get in. And it's not that hard if you know what you're doing.

Interviewer: Definitely. So, it's not dedicated, right?

Expert Respondent: It's not a dedicated thing.

Interviewer: I'll say not dedicated; I think that's a good word. I think the social engineering mixed with the supply chain can be an interesting factor.

Expert Respondent: Yeah, it definitely, yeah.

Interviewer: Alright, let's look. Ground segment, non-malicious. So, we're just a ground station, which means we're probably not interested in debris and celestial monitoring, is that correct?

Expert Respondent: No. Yeah, correct. But we do reliability engineering and reliability engineering.

Interviewer: Yep. I'll get rid of the aerospace engineering part there. So, mainly things like your comms and your radar and your computing stuff as well.

Expert Respondent: That they'll have for the non-malicious swim lane that we're in. That, they have good things in place to try and keep the system up and running or prevent those things affecting it. And they've had a strong culture of that.

Interviewer: High availability, yes?

Expert Respondent: Yes, it's that.

Interviewer: Out of curiosity, is any cloud infrastructure used as part of high availability?

Expert Respondent: No.

Interviewer: Okay, cool.

Expert Respondent: Not yet, but it's been talked about. But, no.

Interviewer: Hmm, that's interesting. There's a lot of different critical infrastructures putting stuff in the cloud. I've even seen control systems in the cloud.

Expert Respondent: {client name} are a bit nervous, but they're definitely looking because it does bring benefits. I think it's more the security of the cloud and how do you secure your data and how do you make sure you get it to where you need it to and when you need it. But it's definitely happening. I don't think we can avoid it. Not for what I work on.

Interviewer: Okay, cool.

Expert Respondent: We're very air gaped in that sense. We use government infrastructure for ICT, so we'll get to that in the C3 bit.

Interviewer: Yeah, we will. So, there is a bit of crossover here, which is somewhat intentional. I've got a diagram that I'll pull up just to show you how everything sits. You may have seen this.

Expert Respondent: Yeah. Yeah, it's good.

Interviewer: So, the idea is the governance segment sets the scope and controls the humans. The humans basically control the system, or the technical components of the system. And then you've got your C3 segment, which is your computing and communications, which link your ground and the space segment.

Expert Respondent: Mm-hmm.

Interviewer: And obviously we're just talking about this ground segment here.

Expert Respondent: Yeah. Think of a building housing it. You know, a mission system.

Interviewer: Yeah. So, there'll naturally be some crossover, which is expected. Okay, let's look at cyber security for the ground segment in a non-governance way. So, things like actual technical controls in place.

Expert Respondent: What you've got is true. So, it's that developing cybersecurity monitoring. All of that's developing. So, it's there, but it's growing, monitoring. But cyber instant response is pretty solid.

Interviewer: Perfect.

Expert Respondent: And that's due to those roles that we talked about earlier. That's part of the dedicated function.

Interviewer: I'll say dedicated function or dedicated roles.

Expert Respondent: Yeah. They're dedicated roles for all of the above.

Interviewer: Awesome. This is looking pretty good. Okay, we spoke about all of that {gesturing on the screen}.

Expert Respondent: Yeah.

Interviewer: So, in electromagnetic governance, I'll just say TEMPEST management, or even I'll just say EM Management probably.

Expert Respondent: Yeah, keep it broad.

Interviewer: And then the actual tempest testing over on this side. Are there any electronic counter measures on the ground segment? So, things like monitoring for jamming? Potentially even prevent it?

Expert Respondent: No, it's more about the link segments for that.

Interviewer: Yeah, that's for the C3 I guess. So, just no jamming or no ECM for buildings.

Expert Respondent: Yeah. Infrastructure.

Interviewer: And we've got physical security. Well, it's a little bit different for electromagnetic. I think the remote operations helps a little bit here too.

Expert Respondent: Yep.

Interviewer: Because you do need some level of proximity to conduct these attacks.

Expert Respondent: Yes, that's right.

Interviewer: Cool. We've pre-filled a lot of the kinetic ground segment, but let's just double check.

Expert Respondent: Yeah. I think we've got that.

Interviewer: Yep. Sweet. Space segments not relevant.

Expert Respondent: No, I don't have a lot to do with that.

Interviewer: Yeah, that's cool. C3 segments, so this is the links themselves now.

Expert Respondent: I don't have a lot to do with the RF to the space segment.

Interviewer: Okay.

Expert Respondent: It's probably worth noting that I'm really more about the ICT infrastructure between ground segments and how data's transferred around terrestrially. I'm not really looking at the RF part. And then that means it's governed by government ICT infrastructure.

Interviewer: Okay.

Expert Respondent: I don't even get a choice of that being solid. It's there, so I can just inherit it from government ICT.

Interviewer: I'll say inherited from government ICT infrastructure.

Expert Respondent: It's everything. It's their policy all the way down to the physical, what exists. There's a framework, maybe it's an infrastructure and framework or something like that.

Interviewer: Makes sense. So, C3 segment includes the actual links themselves, space and stuff we don't need to think about right now.

Expert Respondent: Yeah.

Interviewer: But it also does include any computing for communications. And software as well.

Expert Respondent: Mm-hmm.

Interviewer: So, where the ground segment is more of the infrastructure, C3 segment's all the soft stuff I guess. So, yeah, we've got data classification noted there but there's also a lot of other things here that we can talk about. So, there's all of the crypto, et cetera.

Expert Respondent: I'm not responsible for the monitoring, but I know it's there. All of that is definitely there. There's a lot of redundancy going on in engineering. Lots of integrity checks and classification. So that's all true.

Interviewer: Sweet. And how about code review for the communications component?

Expert Respondent: Yep. It's particularly dependent on the classification of the data.

Interviewer: We're not really looking at the RF part, so I might get rid of the OT security there.

Expert Respondent: Yeah.

Interviewer: Cool, so electromagnetic may be not so relevant here either?

Expert Respondent: Yeah, and I wouldn't know. Well, if it's a comms system…let's forget it. The ICT infrastructure, if it's communications, say we've got set phones between sites and things like that.

Interviewer: Oh yeah.

Expert Respondent: But I'm not familiar with any of that happening. It's a lot of COTS or government provided, so do you assume they've done all of that? But I don't see it.

Interviewer: Okay. And finally, kinetic for the C3 is notoriously difficult, but…

Expert Respondent: There's definitely those aspects of resilience, redundancy, engineering, physical hardening, definitely. So, you don't need counter-space, but there is monitoring and there is resilience, redundancy, physical hardening. Definitely.

Interviewer: Alright. There we go. Just double checking the little things down here. Just to make sure we've covered every aspect. Data management, how's your data management?

Expert Respondent: It's very strong.

Interviewer: Okay.

Expert Respondent: And that applies to all of them. So, there'll be a lot of redundancy in data management. There's a lot in the way it's managed to stop it getting accessed or compromised.

Interviewer: I'll put it over in the government segment.

Expert Respondent: Mm-hmm.

Interviewer: Fantastic. So, we powered through that. Is there anything else that you think is missing or should be sort of noted or added?

Expert Respondent: No, I think you've covered it pretty well with the way you've framed the table. It sort of captures just about everything. I think especially at this level, it's fine. Yeah, I think you've covered it. I'm really interested to see the difference between the different applications. I only ever really work in this area, so we've only just started talking to people like CSIRO and others, which is a bit of an eyeopener. Very different, but they've got a different purpose, so.

Interviewer: Yeah. No, that's fair. They've definitely got a different purpose. I may just stop recording.

Expert Respondent: Yeah, sure.

Appendix E

Although no individual interview was conducted with an expert participant regarding the space vehicle and payload system, enough data was gathered through the other respective interviews in order to build a theoretical picture of the security and resilience status for the purposes of the case study. Excerpts from the other interviews that shed light on the security status of the space vehicle are provided as samples in this Appendix.

Minor redactions have been made to remove any identifiable information regarding the expert respondent and their organisation for the purposes of privacy, security, and intellectual property. Some general modifications were also made to improve clarity, for example removing filler words such as ‘um’, ‘uh’, and ‘you know’, as well as any double-up words that can be common in verbal speech but reduce clarity in written text. No information of importance to the study has been modified in any way that may impact the integrity of the data.

Launchpad Mission Control Expert Respondent: For the up-and-coming launch in a couple of weeks I've also been working with some people on payloads. So, we're putting up three payloads from three different customers. One being ours and looking at how to make sure that the local bus talks to each other. Making sure frequency management, that's been a huge thing. Frequency security. And then the other pieces around it, like the people and the physical, blah, blah, blah.

…

Launchpad Mission Control Expert Respondent: Supply chain, yeah, best intent. But yeah, not so much. Like, I get it. But yeah, trying to have a small business understand that is really hard. Well, understand it and do anything about it is also hard, right? We've been using a lot of raspberry pies and you know, all of those kinds of bits and pieces, so, you know, you got no idea.

Interviewer: Yeah. Do you do any secure code review?

Launchpad Mission Control Expert Respondent: {shakes head} Should we? Yeah, we tried…when did we actually try to do that? We got another mate of mine, {redacted}, who used to do a lot of coding with me. He started to do some reviews and then we just couldn't afford it to be perfectly honest.

Interviewer: No, that's fair enough. It's, yeah, especially in small companies, like, this stuff you can spend more than you will ever make on it.

Launchpad Mission Control Expert Respondent: Yeah. We just couldn't do it. And a lot of it now is because {redacted} has got an affinity with Matlab, so a lot of the stuff we're doing is in Matlab. So, you can still do code reviews, right, but a lot of us just pull boxes together.

…

Launchpad Mission Control Expert Respondent: I can say, and this is not around the electromagnetic pieces, it's actually around ASA requirements, the ASA regulator comes out and checks the launch vehicle to make sure it doesn't have any nuclear payloads. With a Geiger counter. So that's a fascinating little tidbit.

Interviewer: Yeah, that is one that actually is a very interesting thing for you to bring up because that didn't come up at all in the Delphi study. I guess I'll say nuclear inspection.

Launchpad Mission Control Expert Respondent: Yeah, it's pretty funny, he comes and holds the Geiger counter up and goes, not sure if he knows how it works, but, you know, he ticks the box. So, that's interesting.

…

Launchpad Mission Control Expert Respondent: I would probably go, I know you've got it in the space segment there, but I would probably say kinetic governance. The big one would be insurance.

Interviewer: Oh yeah, of course. Yeah. That's another one that wasn't captured by the Delphi process.

Launchpad Mission Control Expert Respondent: Yeah, the amount of insurance we're having to get, I don't know the specifics, but it's lots and it's, yeah, it lands on someone's house and kills someone…

Interviewer: I can only imagine. And, not to mention, you know, most launches don't go so well.

Launchpad Mission Control Expert Respondent: That is my experience so far.

…

Launchpad Mission Control Expert Respondent: We do the celestial piece there, we have COLA which is our collision, and what's the o stands for, collision and avoidance, essentially, of existing space-based assets. So, we have a system, well, it's really an internet stream, don't make it sound more complicated than it is, that basically tells us where everything already is and lines up which windows when we can actually launch. Okay? So, we have that system, we call it COLA, c-o-l-a. I think that's a wider used term. So maybe just Google that. Yeah, that's a good one.

…

Interviewer: Yeah, pretty close. Okay, so Cyber C3 we're looking at cryptography, which is less interesting given what you just stated. We talked about secure coding briefly. I'm interested, on any of the payloads that you deal with, do you come across IoT at all?

Launchpad Mission Control Expert Respondent: What I'm finding is a lot of the payloads are thrown together IoT devices, yeah. They're not built from the ground up at all. I'm not seeing payloads that are something that you'd put in geostationary that are a serious piece of kit. It's lots of people smashing together raspberry pies, other stuff.

Interviewer: So probably not so much security on there. I never expected anything more, in the space race environment especially.

Launchpad Mission Control Expert Respondent: Yep. That's a big problem. It's all about who gets up there first and how you can monetise it, not secure it.

Interviewer: I think that that's an interesting vector. Speaking of which, is there anti-malware on the ground segment?

Launchpad Mission Control Expert Respondent: On my stuff, yes. On payloads, I definitely haven't seen anything like that.

…

Interviewer: I don't think it exists. We talked about security monitoring, how about on the comms link?

Launchpad Mission Control Expert Respondent: {shakes head}

Interviewer: Okay, is there encryption on the comms link?

Launchpad Mission Control Expert Respondent: On the comms link? Not on ours. On some of the others, I wouldn't know, but every time I've raised that with a client their answer has been no.

Interviewer: Yeah, they're very fearful of the power that it takes. And the extra bandwidth of the very limited…

Launchpad Mission Control Expert Respondent: Yep, yep, and the extra coding and the, you know. People don't seem to wanna do it. Nah, it's a big gap.

Interviewer: It's a massive gap.

Launchpad Mission Control Expert Respondent: Yeah, I talk about that a lot. We've been contemplating, and we literally can't afford it, to only use our drones for a single mission. Replace them because of that whole challenge that we probably both know a lot about.

Interviewer: Yeah, that's right.

Launchpad Mission Control Expert Respondent: Size, weight, and power.

Interviewer: Yeah, exactly. Okay, how about, if we're not doing encryption stuff, are we doing any integrity checks for data received back or anything like that?

Launchpad Mission Control Expert Respondent: No, no CRC type stuff. Nothing like that.

Interviewer: Well, this is good for me, for my case study.

Launchpad Mission Control Expert Respondent: It gives you some gaps to talk about.

Interviewer: Exactly. Yeah, good in the theoretical context.

Launchpad Mission Control Expert Respondent: I'm trying to fill all the holes so you've got nothing to talk about, but I just haven't got there yet.

Interviewer: I mean, I don't think you will, unfortunately for everyone.

Launchpad Mission Control Expert Respondent: Nah.

Interviewer: Yeah… How about electromagnetic monitoring and integrity checking? I mean, I'm guessing not the integrity checking, it's even more advanced.

Launchpad Mission Control Expert Respondent: Yeah, no, no, and no.

Interviewer: You've got signature management?

Launchpad Mission Control Expert Respondent: You could maybe say that. Well, we've got frequency management. We know what frequencies we're supposed to be getting and we're making an attempt. I wouldn't say signature as in we know what's coming in on whatever the frequency is, say, {redacted} megahertz. We should be seeing a packet that looks, you know, like this proper EW signature. We're definitely not doing that.

…

Interviewer: Yeah, and only a handful of them around Australia. Now, I'm just trying to think electromagnetic pulse and stuff. Is there any control on the comms link?

Launchpad Mission Control Expert Respondent: Yeah. If someone works out what our payload's gonna transmit through some means, whether they dig out our licensing permits for particular frequencies or they get access to our technical specs and then they try and jam it by something simple like overpower. What are we gonna do about that?

…

Interviewer: And the space segment for mission control, you are the expert on this one, but I think it is mostly N/A? Is this most of it?

Launchpad Mission Control Expert Respondent: Yeah, I think so. Let's just double check. Material reliability, no, nothing there I'd say. Assurance of components? No. We're not there yet. We're not putting up big stuff yet.

Interviewer: I think, at least for {redacted company name}, I feel it's probably down to your clients to do a lot of the protection of the space segment.

Launchpad Mission Control Expert Respondent: Yeah.

…

Interviewer: Oh, yeah. And honestly, I've done a little bit of the payloads, like, we've got some data on the payload, but even then this table ends up usually pretty empty.

Ground Station Expert Respondent: Yeah, there's not much we can talk about, so, no.

Interviewer: Yeah. No one has onboard detection software or even encryption is difficult with the power that of cube stats and stuff that we tend to deal with.

Ground Station Expert Respondent: Yeah, I just got back from the US and we did visit a whole bunch of companies that are part of us. And they are doing it. I just can't really talk about it. They barely showed me. They are doing stuff, so they'll use a DevOps process to secure code, they've done some quite smart stuff with the software. So, it's good from a cyber point of view and there is a lot of work going on on the electromagnetic side.

Interviewer: Oh, yeah.

Ground Station Expert Respondent: Kinetic, no idea. That's kind of the cool stuff you watch on Space Force, but not seeing much on that. And then the non-malicious, not really seeing much, but they've been doing a lot of work in the non-malicious side for a long time. Cause they don't wanna send up a payload and it gets interrupted or corrupted or damaged from a non-malicious environment. So, they do have very stringent environmental controls in place. So, I'd say that is actually done well. There is a lot done well when it comes to payloads on that area. And cyber's, I just can’t give you too much information on it.

Interviewer: Yeah.

Ground Station Expert Respondent: So, you can just put in there, environmental controls are in place. Quite strict.