SMARTSAT
COOPERATIVE RESEARCH CENTRE

TECHNICAL REPORT 07

Development of an Evil Digital Twin for LEO Small Satellite Constellations

Part One of Two

Technical Report No. 07

Development of an Evil Digital Twin for LEO Small Satellite Constellations

Part One of Two

June 2021

This report should be cited as:
SmartSat 2021, Development of an Evil Digital Twin for LEO Small Satellite Constellations, SmartSat Technical Report No. 07, SmartSat, Adelaide, Australia.

Disclaimer:
This publication is provided for the purpose of disseminating information relating to scientific and technical matters. Participating organisations of SmartSat do not accept liability for any loss and/or damage, including financial loss, resulting from the reliance upon any information, advice or recommendations contained in this publication. The contents of this publication should not necessarily be taken to represent the views of the participating organisations.

Acknowledgement:
SmartSat acknowledges the contribution made by Dr David Ormrod (Cygence) towards the writing and compilation of this technical report.

SMARTSAT
COOPERATIVE RESEARCH CENTRE

cygence

Executive Summary

‘…fortunately for us, your knowledge of us is deeply flawed. That’s the prime reason why you've been losing every other battle. It is not that you don't understand our decision-making processes… What you don’t begin to understand is how we see the world. To summarise your problem in a sentence: you don't give us credit for having what you have, which is vision’ (Kramer, 2007).

Space systems frequently employ the concept of a digital twin, to test engineering concepts in a simulated environment that replicates the functionality of the system in question.
Digital twins can have different fidelity levels and be designed for different purposes. This report introduces the concept of an ‘evil twin’ as a counterpart to the standard engineering perspective of a digital twin.

Anticipation of threats is critical to understanding the potential attacks delivered through cyber capabilities. Understanding reduces risk and increases the ability for engineers and operators to anticipate likely cyber-events. This, in turn, increases the cyber-resiliency and response capabilities of systems when under attack. Knowledge informs the development of effective countermeasures.

The ‘evil twin’ models and tests potential attacks by adversaries, to improve cyber-security outcomes. This approach builds upon the practice of threat modelling and red teaming, with the goal of enhancing the resilience of space systems and improving their survivability under cyber-attack. The evil twin is more than just a penetration test or a red-team exercise; it is intended to be a comprehensive methodology that matches the utility of a traditional digital twin in the reduction of risk to space missions.

This report is the first of two parts commissioned by SmartSat CRC through the University of South Australia, seeking to enhance the state of the art in cyber-security solutions for Low Earth Orbit (LEO) space systems. The aim of this two-part series is to establish a Cyber-Jeopardy and Response Concept (CY-JAR) for ongoing development and subsequent deployment into the space operational environment. The evil twin is a first step in developing an advanced CY-JAR capability.

This report discusses a variety of frameworks, models and approaches pertaining to cyber-security. Here, Part One provides an overview and analysis of the body of knowledge pertaining to concepts including mission assurance, resilience, risk and cyber-worthiness, as a means of enhancing the security posture of LEO systems. Principles and specific tools for the application of cyber-security to the LEO space system environment are considered with the intention of informing long-term sovereign Australian satellite cyber-security, digital twin modelling and simulation capability.

Part Two will build upon this report and provide a fully worked example of a cybersecurity solution, using a generic model of a LEO space system, as a precursor to the Cyber-Jeopardy and Response concept. Part Two will be published separately.

Table of Contents

Figures

Tables

Acronyms

Acronym	Meaning
AMICA	Analyzing Mission Impacts of Cyber Actions
ANAO	Australian National Audit Office
APTs	Advanced Persistent Threats
ASAT	Anti-Satellite Weapons
ASCCoE	Australian Space Cyber-security Centre of Excellence
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AWS	Amazon Web Services
BN	Bayesian Network
CAPEC	Common Attack Pattern Enumeration and Classification
CORIE	Cyber Operational Resilience Intelligence-led Exercises
COTS	Commercial-Off-The-Shelf
CRRA	Cyber Risk Remediation Analysis
CSCE	Cyber Security Centre of Excellence
CTI	Cyber Threat Intelligence
CTSA	Cyber Threat Susceptibility Analysis
CY-JAR	Cyber-Jeopardy and Response
DoD	Department of Defense (US)
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy
EDT	Evil Digital Twin
EU	European Union
FCC	Federal Communications Commission
FGPAs	Field Programmable Gate Arrays
FIC	Fundamental Inputs to Capability
GEO	Geostationary Orbit
HLA	High Level Architecture
IoT	Internet of Things
ISAC	Information Sharing and Analysis Center
ISO	International Standards Organisation
ISR	Intelligence, Surveillance and Reconnaissance
KM	Knowledge Management
LEO	Low Earth Orbit
MEO	Medium-Earth Orbit
MISP	Malware Information Sharing Platform and Threat Sharing
MoE	Measures of Effectiveness
MoP	Measures of Performance
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation

NIST	National Institute of Standards and Technology

NOAA	National Oceanic and Atmospheric Administration
openXSAM	OPEN format for eXchanging Security Analysis Models
OPSEC	Operations Security
OSINT	Open Source Intelligence
OT	Operational Technology
OWASP	Open Web Application Security Project
PASTA	Process for Attack Simulation and Threat Analysis
PNT	Position, Navigation and Timing
RAPAPORT	RAND Project Resilience Assessment Process and Portfolio Option Reporting Tool
RM	Risk Matrices
SDLC	Software Development LifeCycle
SOC	Security Operations Centre
SP	Special Publication
SpaceFOM	Space Reference Federation Object Model
STIX	Structured Threat Information Expression
SV	Space Vehicle
TARA	Threat Assessment and Remediation Analysis
TTPs	Tactics, Techniques and Procedures
UK	United Kingdom of Great Britain
UN	United Nations
US	United States of America
VV&A	Verification, Validation and Accreditation
WEF	World Economic Forum

Introduction – Why Cyber in Space?

On the success of SpaceX… 'it's going to encourage other countries and companies to raise their sights and say "we can do bigger and better", which is great" (Musk cited in Cheng & Harrington, 2017).

'Cyber security is one of the biggest unsolved challenges we have on Earth, and it's about to become a far larger challenge in space' (Abbany, 2018).

Space as a Contested Environment

Australia faces a contested global environment, featuring increasing geo-political competition across a rapidly evolving technological landscape, including new capabilities in cyber and space. The success of companies such as SpaceX has triggered increased awareness and interest in space-based capabilities by both industry and governments around the world.
sSpace provides options at a national and industrial level to solve technological and communication challenges and to achieve diplomatic, information, military, and economic objectives (US Department of Defense, 2020).

Freedom of action in space supports commercial, political and national security success. Space has been declared a warfighting domain by both US and Australian official sources (Defence Science and Technology Group, 2020; US Department of Defense, 2020). The opportunities derived from space innovation have resulted in rapid change and investment. The Australian space industry is expected to grow at an annualised 7.1% through to 2024 and create up to 20,000 jobs and $12 billion by 2030 as a market segment (Australian Space Agency, 2019). Industry has become increasingly capable of providing faster and cheaper systems, in support of both commercial and military objectives. There is a burning platform for research, investment and innovation to increase Australian space capabilities relative to international nation-state and non-state actors.

Low Earth Orbit (LEO) space systems, like most space systems, combine a range of end-to- end capabilities including ground control networks, Space Vehicles (SVs), and mission networks. Despite their similarities, LEO systems possess different attributes to other orbits, such as Medium-Earth Orbit (MEO) and Geostationary Orbit (GEO) missions. LEO SVs operate at a lower altitude, and a high speed, and can have tilted orbital planes, allowing for more satellite routes (European Space Agency, 2020b). Ground control networks and support systems for LEO are generally of a much smaller scale and lower cost than MEO or GEO missions. They offer good value for money and significant flexibility. The low altitude of LEOs reduce latency and offer quicker removal of SVs from orbit, reducing their lifespan and the potential for long-term orbital debris issues (Federal Communications Commission, 2021).

The US National Aeronautics and Space Administration (NASA) is one example of government agency and non-government organisation efforts to adopt small spacecraft as a means of balancing a broader space portfolio (NASA, 2019a). LEOs are seen by some military services as a means of increasing their communications and reconnaissance capabilities and resilience, using rapidly developed and deployed SVs. Proliferated LEO increases the number of SVs working together as a constellation. Proliferated LEO SVs are seen as less vulnerable, rapid to replace, capable of continual upgrades and contributing to a portfolio approach for space that is robust

and resilient to attack in a way that hasn't traditionally been the case (Sheftick, 2020).

LEO SVs are increasingly intended to operate as part of a constellation, offsetting the limited capabilities of a single LEO SV with the benefit of mass and flexibility that large numbers of SVs can provide. The SpaceX Starlink constellation is an example of the evolving nature of LEO capabilities in a constellation framework. SpaceX announced its intent to launch the constellation of LEO SVs in 2015. By 2018, two SVs were launched (Mann, 2021). By mid-2021, six and a half years after they announced their intent, SpaceX had launched a cumulative total of 1737 SVs, with 1662 in orbit and 1047 operational (McDowell, 2021).

SpaceX has already been granted approval by the Federal Communications Commission (FCC) to operate 4408 SVs (Federal Communications Commission, 2021). This is likely to be just the beginning of an ever-increasing population of LEO SVs in orbit. Multiple nations and companies have announced LEO constellation projects, for a diverse array of missions.

Indeed, space systems such as LEO can provide capabilities for all sorts of different missions, such as communications, scientific, Intelligence, Surveillance and Reconnaissance (ISR) and Position, Navigation and Timing (PNT) services, to name just a few. However, SVs on their own do not provide a space capability. Satellites are just one critical part of an interconnected end-to-end service, from the ground station and its personnel through to various supporting services such as networking, cloud computing, radio, launch vehicles and launch sites. These assets collectively provide space capabilities and services.

Space services require space domain awareness, which is the ability to identify, characterise and understand the various factors that can impact space operations (Shaw, 2019). Space domain awareness in turn requires space control, which provides freedom of action and the ability to defend space systems from interference or attack (US DoD, 2020). Space control requires a range of options to defeat adversarial efforts to manipulate or deny space services. A function of space control is the provision of cyber-security services.

Cyberspace and Cyber-threats in Space

Cyberspace (not to be confused with the use of cyber capabilities in space) refers specifically to an environment within the information domain that supports computation and communication, enabled by digital systems. Cyberspace is an environment that utilises digital technology to enable computation, storage, and communication through software. Human users, physical systems and digital programs interact through network connections in cyberspace (Ormrod & Turnbull, 2016, pg 281).

The importance of software in the discussion of cyberspace is critical. *'*Software is eating the world*'* (Marc, 2011). Software-defined systems provide flexibility and agility to rapidly rearchitect and configure systems and networks. The value of this capability is significant for space missions, providing opportunities to affect change on systems after launch, or to modify mission control capabilities even after hardware has been installed. Digital systems feature increasingly powerful computer and software systems that have led to the convergence of space and cyber capabilities. However, this convergence and the flexible nature of software and network protocols presents a variety of continually evolving vulnerabilities and risk to SVs and their enabling systems.

Cyberspace is contested, in the same way that space has been declared a contested warfighting

domain. Increased competition has resulted in significant capability investment to create effects in and through cyberspace to defend and attack digital systems, by both nation-state and industry alike. Adversaries in cyberspace can generate a broad range of effects with reduced risk of attribution (R. Burch, 2013). An example of the increase in attention focused on cyberspace is evident in the United States (US) Department of Defense (DoD) development of a Cyber Mission Force, which commenced in 2012 and now consists of 133 teams organised to deliver offensive, defensive and operational missions around the world (Theohary, 2020). The US Intelligence Committee has declared that countries such as China, Russia, North Korea and Iran present significant threats through cyber-attacks and cyber-espionage to US allies such as Australia. This includes efforts by these nations to remain space competitors, 'developing, testing and fielding an array of non-destructive and destructive counterspace weapons – including jamming and cyberspace capabilities' (Office of the Director of National Intelligence, 2021).

The overall cyber-security capability evident across some of Australia's government entities lags the offensive capabilities demonstrated by advanced threat actors. An Australian National Audit Office (ANAO) audit of seven non-corporate Commonwealth entities revealed that none of these entities had fully implemented all the mandatory Top Four mitigation strategies (Australian National Audit Office, 2021). The Top Four mitigation strategies represent a minimal baseline level of cyber-security compliance. This is exacerbated by a recent South Australian government report regarding 292 public-facing environments, which found that 79% of total environments had not been penetration tested and 40% had not been vulnerability scanned in the last three years. Of those that had performed vulnerability scanning, 50% of entities did not track remediation of issues (South Australian Auditor-Generals Department, 2021).

Australia's space industry must aim for a much higher level of cyber-security than these statistics demonstrate, if it is to be successful in providing a defendable, well-governed and responsive capability to a contested and competitive cyber environment in space. The potential for resourced and capable actors to target space assets increases the risk significantly. Cyber-security is explicitly named as a government concern in the development of Australia's space industry, and requiring a corresponding 'world-class regulatory system that enables entrepreneurship while ensuring national safety and security' (Australian Space Agency, 2019). This type of target sits neatly within the sights of many threat actors.

Anti-Satellite Weapons (ASAT) provide attackers with an evolving variety of options to deny, disrupt, disable, destroy or deceive SVs and their supporting infrastructure. The attack surface for the space sector is broad; encompassing a large ecosystem across industry and government institutions, as well as the various engineering and support systems that enable the sector. As an example, attacks can target individual users to establish a beachhead and gain initial access to systems. Other approaches can include scanning systems and protocols for vulnerabilities to support penetration onto networks. 'Cyber-threats pose a significant and complex challenge due to the absence of a warning and speed of an attack, the difficulty of attribution, and the complexities associated with carrying out a proportionate response' (Unal, 2019). Space systems and the services they deliver have already been subjected to cyber-attack by Advanced Persistent Threats (APTs) such as the Turla group, who have targeted Middle Eastern and African systems (Drozhzhin, 2020). Open-source reporting on nation-state capabilities provided by the Centre for Strategic and International Studies suggests a growing industry and capability to target space systems, including multiple cyber-attacks in 2007, 2008 and 2014 that disrupted NASA and National Oceanic and Atmospheric Administration (NOAA) systems and, in some cases, achieved unauthorised command of SVs (Harrison, Johnson, Roberts, Way & Young,

2020). The advantage of counter-space cyber-attack capabilities is the potential to contest and degrade adversary space capabilities while reducing the risk of both attribution (through anonymity and deniability) and avoiding Kessler syndrome, where cascading debris collisions can be counter-productive to an attacker.

Falco (2018) discusses the dire state of space cyber-security in his analysis, blaming a unique confluence of challenges due to the critical nature of space technologies, lack of standards, complex supply chain, dependence on Commercial Off-The-Shelf (COTS) software, highly specialised workforce, and various resource constraints.

*'*Despite their importance, space systems are riddled with cybersecurity issues – both cubesats and sophisticated systems alike. There is little support infrastructure for improving space asset security such as space-specific standards or space system information sharing organisations, which exacerbates the problem. While space assets suffer similar cybersecurity issues to other industries, they are faced with a unique confluence of challenges making their cybersecurity risk mitigation considerably more complex*'* (Falco, 2018).

Cyber-attacks can target the entire space-system solution, including terrestrial and networked systems integrated with the solution. Offensive cyber-payloads provide a potentially scalable, pre-emptive and reversible option to the attacker. Cyber-attacks against space systems include spoofing and corruption, compromising systems, conducting denial- of-service attacks and injecting malicious code (US Whitehouse, 2020). Pavur and Martinovic (2020) provided a comprehensive review of satellite hacking incidents over a 60-year period, categorising four sub-domains:

1. Satellite radio-link security,
2. Space hardware security,
3. Ground station security, and
4. Operational/mission security.

Attacks commonly involve radio interference rather than specifically being software-driven cyber-attacks (Bardin, 2013). However, the nature of cyber-security for space systems and vehicles is changing. Increasing use of cloud solutions for ground station service provision, such as Microsoft Azure Orbital (Microsoft, 2020) and Amazon Web Services (AWS) Ground Station (AWS, 2020), will change the risk profile for operators. In addition, the use of open and low-cost hardware on LEO satellites, and the increasing proliferation of services, creates an attack surface consisting of both operational and information technology. Emerging space threats for soft kill cyber-attack are much more aligned to the types of Tactics, Techniques and Procedures (TTPs) seen across much of the critical infrastructure and industrial control system terrestrial attack surface, which is a perfect hunting ground for cyber threats.

Supply chains offer a large attack surface that can be difficult to secure. LEO SV manufacturers rely on relatively cheap hardware and software services, which are often produced overseas with no transparency into their vulnerabilities or downstream supply sources. Software on these systems can be poorly documented and maintained. Large aerospace companies can have over 200 tier one suppliers and more than 12,000 suppliers in their second and third tiers (Hays). Cyber-security seeks to secure this large attack surface, resist attacks, and protect space assets to provide the desired outcomes of the space mission (Carlo & Veazoglou, 2020). It is against this large threat surface and very capable threat actors that this report seeks to provide value, to support space service providers and engineers.

Report Objectives

This report describes the threat and cyber-security landscape pertaining to LEO space systems. It presents an Evil Digital Twin (EDT) Framework, for use as a component of a broader Cyber-Jeopardy and Response (CY-JAR) concept. Specific adversarial use cases will be developed to emulate likely attack patterns to be applied against LEO constellations and systems. Principles, approaches and specific tools for the application of cyber-security to the LEO space system environment will be discussed, with the intention of informing long-term sovereign Australian satellite cyber-security, digital twin modelling and simulation capability.

A digital twin is an '…informational construct about a physical system… created as an entity on its own… linked with that physical system through the entire lifecycle of the system' (Kahlen, Flumerfelt & Alves, 2016). Digital twins can have different objectives (Katona, 2020). In the context of this report, the digital twin supports the prediction of system behaviour in a cyber-security context. An objective of this report is to identify what is required from a digital twin to adequately support cyber-security efforts. The knowledge gained through the twin should prepare LEO SVs and space systems for real-world missions.

This report seeks to apply an adversarial mindset and red teaming approach to the problem of cyber-security for LEO space systems. Red teaming is 'the independent application of a range of structured, creative and critical thinking techniques to assist the end user make a better informed decision or produce a more robust product' (Ministry of Defence, 2013, pp. 1- 5). Red teaming supports mental agility in complex environments and seeks to reduce blindspots and bias through multiple different perspectives (University of Foreign Military and Cultural Studies, 2019). The concept of an EDT is explored in this paper as a means of integrating a red teaming mindset with adversarial intelligence curated within the cyber- security community, to achieve enhanced outcomes for LEO space systems.

Adversaries will focus outside of the design space normally occupied by engineers and designers. As a result, traditional use cases, which seek to provide conformance parameters and provide boundaries of acceptable use, lie outside of the digital twin environment. The EDT incorporates a set of use cases and scenarios that take an opposite view to the traditional engineering and risk management approach; it is focused on an adversarial view. Cyber-security incidents and malicious events will often seek to break protocols and product designs and trigger unexpected behaviour. This presents a problem because digital twins are generally defined based on their protocols and designs, what is allowable and feasible within the design specifications.

To manage the risk of attack, designs must incorporate events outside of expected behaviours and use cases. This is the EDT. The EDT is critical to good cyber-security as it informs, predicts and emulates the adversary. The digital twin, without its evil opposite, may teach the wrong lessons if design is focused on user intentions only. The EDT allows for a space to plan specifically for aspects outside of the engineered space, emulating and modelling an intelligent, curious and resourced adversary.

Contribution

This report seeks to set the pre-conditions and enable follow up activities as part of the broader SmartSat CRC efforts to encourage a safe and secure space environment. This report is part one of two, working towards the following goals:

Vision: Enhance LEO space system resilience and reduce risk for Australian LEO operations through the effective application of an Evil Digital Twin, cyber-worthiness framework and CY-JAR model.

Enabler Activities:

- LEO operators identify relevant APTs and other cyber actors reported through open source means that have the capability and intent to attack LEO systems. These actors will form a threat actor library.
- LEO operators identify the TTPs employed by the threat actors included in the library.
- LEO operators identify crown jewels, critical systems and mission essential assets for protection using a space mission assurance assessment process. Security controls and efforts will be prioritised to protect these systems and assets.
- LEO operators undertake cyber threat intelligence monitoring, vulnerability management, threat modelling, penetration testing and research to maintain situational awareness of contemporary threats and forecast future trends.
- LEO operators report breaches and share intelligence sources to ensure a secure ecosystem for all space systems.
- LEO operators develop a Cybe-Jeopardy and Response (CY-JAR) capability within constellations to provide contextualised space domain awareness, using anomaly attribution and intelligent sense making as a defensive function.

Report Structure and Core Concepts

Part one of this report is structured around six integrated core concepts, depicted below in Table 1.

Table 1: Report Structure

Mission Assurance and Resilience
Risk and Cyber-Worthiness
The Digital Twin
The Evil Digital Twin
Adversary Behaviours

1. Mission Assurance and Resilience

'The approach we take is… to ensure that the operational missions can be executed to the maximal extent possible in the event of the most damaging cyber-attack…' (Snyder, Hart, Lynch & Drew, 2015).

1.1 Assurance

Space systems have defined tasks that contribute to a broader mission or set of mission objectives, depending on their payload and associated business, national or organisational outcomes. A focus on mission objectives is a key attribute of mission assurance. Mission assurance is a process that seeks to maintain confidence in mission success (Musman, Tanner, Temin, Elsaesser & Loren, 2011, pg 210) and mitigate deficiencies or vulnerabilities that could impact mission success (National Defense Industrial Association, 2008, pg 152). These definitions require an understanding of what constitutes mission success, how it is measured, and what is considered essential to the mission. The interaction between processes, procedures, tools and people determines the degree of assurance that exists for a space system and, consequently, the degree of confidence applicable to a specific mission (Vaughn Jr, Henning & Siraj, 2003).

Space Domain Mission Assurance refers to a process that ensures the benefits associated with a mission are achieved, based on specific critical performance functions that are considered mission essential. Mission assurance in the space domain is directly related to resilience, although resilience itself is not the objective. Mission assurance is an outcome of resilience (Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, 2015, pg 2). The importance of linking resilience to mission assurance is vital to a complete understanding of the concept. Although a single system can incorporate functions that contribute to its resilience, the overall concept of mission assurance should be seen from the perspective of the mission and the resilience across all systems that provide mission essential functions. The system of systems must be capable of fighting through attacks to conduct missions and achieve essential tasks, to provide mission assurance (Command, 2009).

The Space Domain Mission Assurance taxonomy depicted below in Figure 1 provides a means of categorising the functions that sit within its scope. Defensive Operations seek to interrupt the adversary kill chain or provide warning to support the defence of the system. Reconstitution replenishes denied or degraded functions to an acceptable level, in a similar way to the concept of responsive space (Jung & Vasen, 2021). Resilience supports the delivery of mission success with higher probability across a broader range of scenarios and threats. The delivery of additional resilience through non-space domain assets (such as aircraft) is out of the scope of resilience in the context of the space domain, although it can be seen as part of the overall multi-domain mission assurance model (Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, 2015, pg 3).

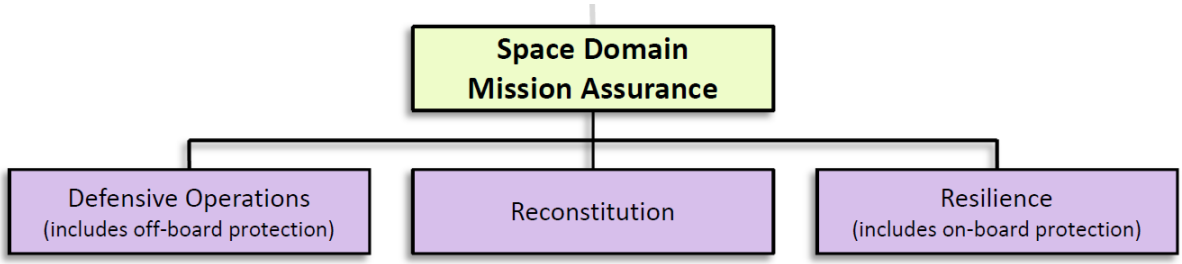


Figure 1 - Space Domain Mission Assurance Taxonomy

Understanding the mission and mission assurance is the underlying foundation for effective cyber-security. Space Domain Mission Assurance and effects-based planning in the LEO cyber environment seeks to clearly enunciate the end-state and desired missions of the LEO SV and supporting systems. A systems approach in this context consists of three parts:

- 'a problem space – what are the systemic interactions that cause the situation to exist?
- a solution space – what could I do as part of an orchestrated campaign to bring about a more favorable situation?
- a design space – what am I going to do to alter the prevailing conditions to those that comprise my desired end–state?' (Duczynski, 2004).

1.2 Resilience

Resilience is the ability for a system to provide mission essential functions despite hostile events and conditions. Resilience is a property of a system or architecture described through probability and/or confidence levels against functionality metrics and/or capability levels, based on a range of scenarios, events and/or threats (US Department of Defense, 2011).

Resilience focuses on core capabilities and their ability to provide a continued presence despite threats that interrupt those capabilities delivering services to other users and systems (R. W. Burch, 2019, pg 27). Five criteria have been developed to assess resilience of an architecture (US Department of Defense, 2011):

'1. Anticipated level of adversity
2. Functional capability goals necessary to support the mission
3. The risk that these goals may not be met at a given level of adversity
4. The severity of the functional shortfall to the mission; and
5. The time which the shortfall can be tolerated by the mission'

There is a relationship between robustness and resilience. Robustness relates to the amount of damage that can be sustained by a system, whereas resilience relates to the speed and level of recovery (Kott & Linkov, 2018). Those responsible for engineering and developing SVs and related space systems must consider a broad range of factors, including decisions relating to the space system trade space depicted in Figure 2 (below). Cost, performance and resilience must be traded to provide an affordable, mission-worthy and capable platform depending on the context of the mission (R. W. Burch, 2019). This trade space is a critical consideration in any discussion of space and cyber.

Figure 2 - Space System Trade Space (R. W. Burch, 2019)

Resilience can be described at a variety of levels including organisational, enterprise, tactical and operational missions, or functional levels. Specific systems can possess resilience, as can networks, architectures and systems of systems (R. W. Burch, 2019, pg 29). A higher-level view of resilience assessment, from the perspective of the capability lifecycle and system of system elements, is covered under the US DoD model of Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) (Dreyer, Langeland, Manheim, McLeod & Nacouzi, 2016). This lifecycle approach is managed in an Australian military context through the concept of Fundamental Inputs to Capability (FIC) (Commonwealth of Australia, 2012). The principle of these concepts is the role of the broader ecosystem, over time, to influence the full capability realisation and mission assurance of any system, be it in space, air, sea, cyber or on the ground.

Cyber-resilience at an organisational level is often described as a governance issue. Governance, in the context of cyberspace, refers to the decision rights and accountability that encourages desirable behaviours in the application of digital technology. Effective technology governance is particularly important to manage risk and rapid change, which are both significant features of the space environment (Westerman & Hunter, 2007). COBIT provides a variety of components and design factors, and is one type of governance framework designed specifically for information and technology sectors. It posits three principles for a governance framework (ISACA, 2019):

- Grounded in a conceptual model
- Flexible and able to adapt; and
- Compliant and aligned to relevant standards.

Decision frameworks are described as necessary to provide effective governance, including architecture and business requirements (Weill & Ross, 2004). Six principles of cyber- resilience from a governance perspective (World Economic Forum, 2021) include:

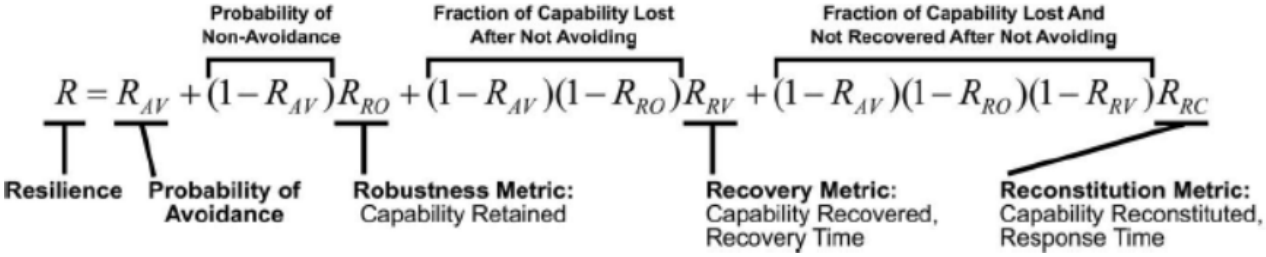
- Cyber-security is a strategic business enabler
- Understand the economic drivers and impact of cyber risk

- Align cyber-risk management with business needs
- Ensure organisational design supports cyber-security
- Incorporate cyber-security expertise into board governance; and
- Encourage systemic resilience and collaboration.

These high-level governance models need to be considered as part of an LEO space system solution and as considerations in running a space-service business or agency. However, at the engineering operational level, resilience needs to have a more focused approach that is both practical and measurable.

1.3 Resilience Quantification

There is a significant gap in knowledge pertaining to resilience and risk in cyber-security as it applies to the space domain. However, a notable publication that has sought to provide a quantitative approach to resilience is provided by R. Burch (2013) calculating resilience in the cyberspace environment. Resilience in this model, is the sum of the probability of avoidance combined with a series of metrics; robustness, recovery and reconstitution, as described in Equation 1:



Equation 1 - The Resilience Equation (R. Burch, 2013)

This equation is further explained through the flowchart depicted in Figure 3 (below). Where a threat is not avoided, a percentage of capability may be lost. A percentage of capability may subsequently be recovered and another percentage reconstituted. The total is the resilience calculation of the system (R. Burch, 2013, pg 76).

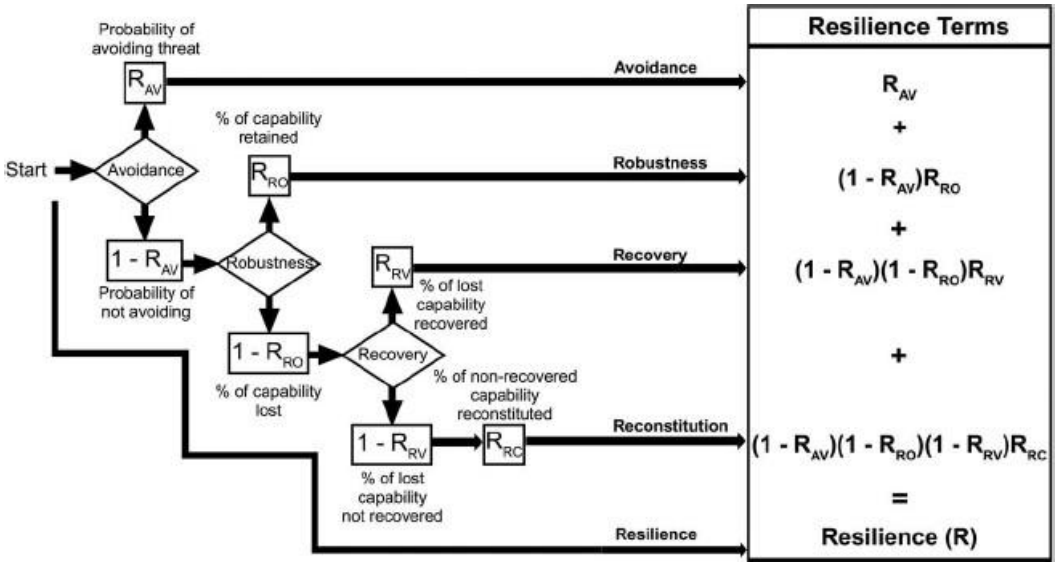


Figure 3 - Flowchart of Resilience Equation (R. Burch, 2013)

1.4 Crown Jewels Analysis

Crown Jewels Analysis is a process to identify the cyber-assets that are mission essential (MITRE Corporation, 2014). Identifying crown jewels and high value assets to facilitate an enhanced security posture is critical to ensure prioritisation of resources and defensive efforts. Given the limited resources available to an entire system or organisation, high value assets must be identified based on their connection to mission dependencies. Mission dependencies include the second and third order consequences associated with a failure of confidentiality, integrity or availability within those systems. Tools are available to support this planning activity, as a component of the threat modelling process, which can be documented as crown jewels or high value assets (Foreseeti, 2020). The modelling of crown jewels and their relationship to missions is depicted in Figure 4 (below), which has been adapted from the MITRE Systems Engineering Guide (MITRE, 2014).

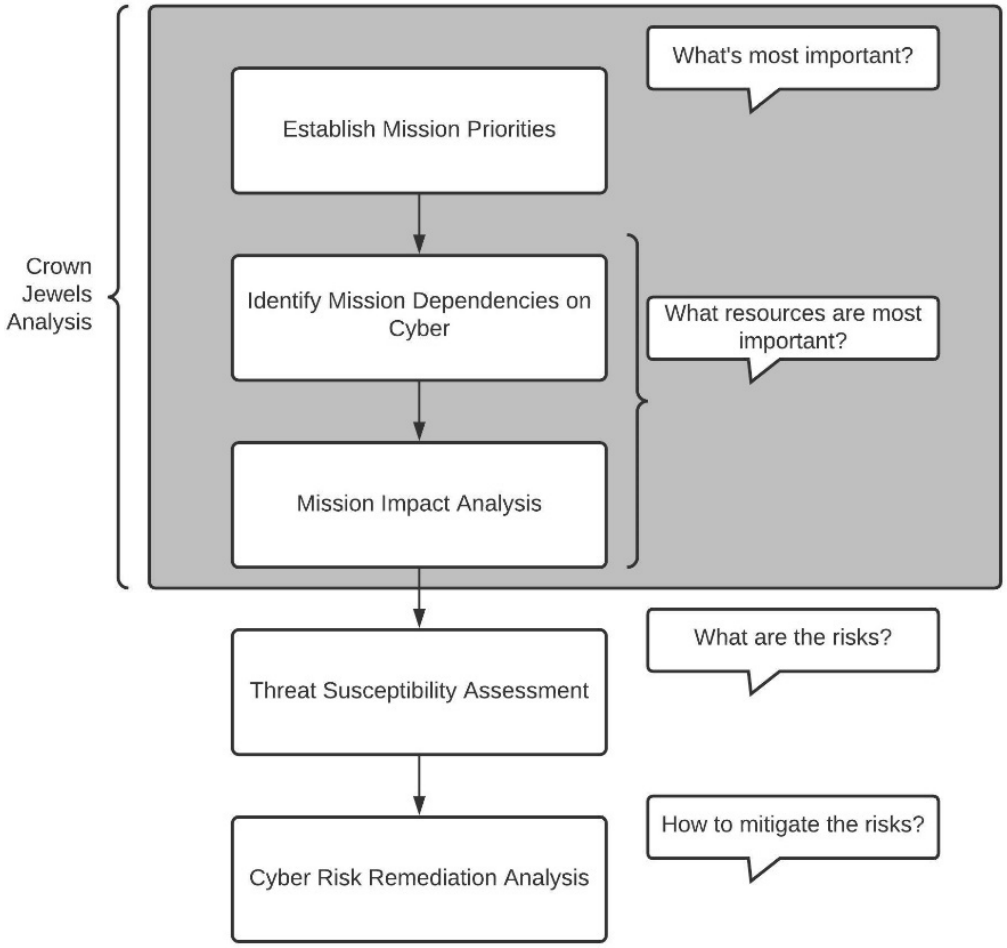


Figure 4 - Crown Jewels Analysis as part of the Mission Assurance Engineering Process (Adapted from MITRE, 2014, pg 168)

The function of a cyber-asset being compromised and the cascading impacts across assets, functionality, operational tasks and mission objectives are depicted through an example dependency map in Figure 5 (below).

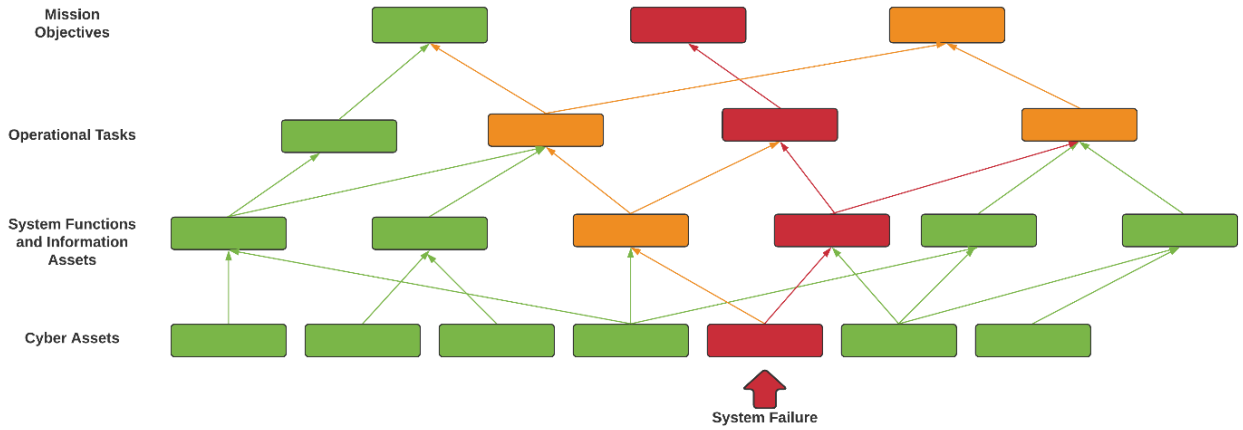


Figure 5 - Mission Dependency Mapping (Adapted from MITRE, 2014, p. 169)

The cascading impact of a single system failure arising from a cyber asset can be seen in red, whilst amber depicts a loss in capability but not a complete failure. Green represents unchanged capabilities. As depicted, a single failure can impact multiple mission objectives, through dependencies. However, security impacts do not necessarily result in mission failure, depending on the system in question and the type of security failure. For example, a short-term degradation of communications may not impact mission success at all, if the event occurs at a time when a satellite is not scheduled to transmit. Compromises to confidentiality may not lead to mission failure. An unclassified weather satellite may not require encryption on its weather payload broadcasts. On the other hand, a military operationally sensitive system may prioritise confidentiality over availability. These prioritisation decisions are driven by contextualisation of the space system mission, the services provided by the system, dependencies on other systems, the security requirements of the specific ecosystem under analysis, and how these factors align with adversary intent and goals.

The MITRE Cyber-Resilience Engineering Framework provides a structured approach to increasing resilience that is applicable to LEO missions. Eight objectives are provided, which are briefly explained below (MITRE Corporation, 2014):

1. **Understand.** Represent adversaries, their activities, mission dependencies, cyber-resources and their relationships
2. **Prepare.** Develop cyber-courses of action to respond to predicted cyber-attacks
3. **Prevent.** Avoid attack execution on cyber-resources
4. **Continue.** Maintain essential functions throughout an attack
5. **Constrain.** Limit the extent of the adversary actions and the damage sustained
6. **Reconstitute.** Redeploy cyber-resources to restore functionality
7. **Transform.** Change behaviour to prevent future attacks; and
8. **Rearchitect.** Change architecture to enhance cyber-resilience and adjust to a changing environment, in terms of adversary capabilities and intent, and emerging and legacy technologies.

The combination of mission assurance analysis, dependency mapping, and the application of the objectives described in the MITRE Cyber-Resilience Engineering Framework, provides a comprehensive approach to support a thorough understanding of mission-essential systems. The MITRE Cyber-Resilience Engineering Framework objectives align to many of the other models discussed throughout this report. Understanding the adversary and how to thwart their activities is a crucial part of the framework. Equally, the ability to transform and adapt systems to respond to a changing environment is central to achieving the objectives within the MITRE Cyber-Resilience Engineering Framework. Measuring impact is an important concept to developing an

understanding of mission assurance and cyber-security.

1.5 Impacts of Cyber Actions

Measures of Effectiveness (MoE) enable planners and engineers to develop metrics that support analysis of progress against identified missions. Reporting of the effect allows for comparison of observed events and measures with target states (Commonwealth of Australia, 2009). The relationships between behaviours, events, effects, missions, metrics, Measures of Performance (MoP) and MoE are essential parts of any model describing impacts on cyber, space, resilience and mission assurance. These different variables mean that context shapes the relevance of a system. A single LEO SV can be of negligible value unless it happens to be the only asset able to receive a signal of national significance.

Suddenly value and importance can change. However, this rare event may not be enough to justify significant changes in investment and security. Highly unlikely events may also be overlooked in risk and benefit assessments. Impact is highly contextual, making assessments reliant on experienced and skilled personnel.

Influence diagrams, ontologies and Bayesian methods have all been employed to manage mission assurance and effects-based planning through causal relationships (O'Sullivan & Turnbull, 2015). Duczynski (2004) provides a systems approach to effects-based planning. The Analyzing Mission Impacts of Cyber Actions (AMICA) framework advocates for different fidelity levels and threat classes to be used, and incorporates:

- TTPs, for both the attacker and defender
- Attack dynamics and subsequent mission impact; and
- Attack surface and resiliency.

Process modelling and graph modelling are core to the AMICA framework. Different simulation engines, scenarios, cyber-attack and defence models and mission models can be used to model workflow and process. This informs, and is informed by, parallel graph models that examine attack graphs, state models and mission effects. These models are then supported by visualisation and analysis tools with underlying data models, such as the one depicted below in Figure 6 (below) for CyGraph (Noel, 2015).

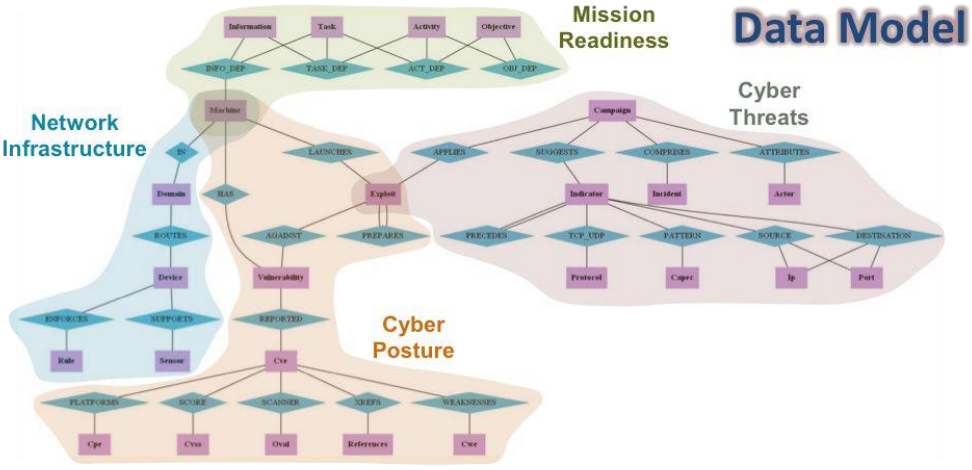


Figure 6 - CyGraph Data Model Visualisation

The use of data models, directed graphs, Bayesian models and ontologies is common throughout the industry, as they allow for rapid reuse, ingestion of new data sources and reusability. This type of approach has considerable functionality and utility, although it requires a larger upfront investment to develop, and regular commitment to maintain.

There are other methods available for assessing the mission impact of events and the resilience of systems. One such method is the RAND Project Resilience Assessment Process and Portfolio Option Reporting Tool (RAPAPORT) (Dreyer et al., 2016).

RAPAPORT is a methodology and Excel-based tool developed to support a US Air Force space resilience project, aligned to MITRE and US DoD lifecycle resilience doctrine. The tool assesses resilience interdependencies across the DOTMLPF lifecycle, using assessments against baseline and capability options, against defined threats.

Detailed impact models require an understanding of metrics and their relationships. These metrics can be broadly grouped into four perspectives: project manager, system engineer, mission assurance and threat. The relationship between these perspectives and their metrics is depicted in Figure 7 (below), adapted from D Bodeau et al. (2018).

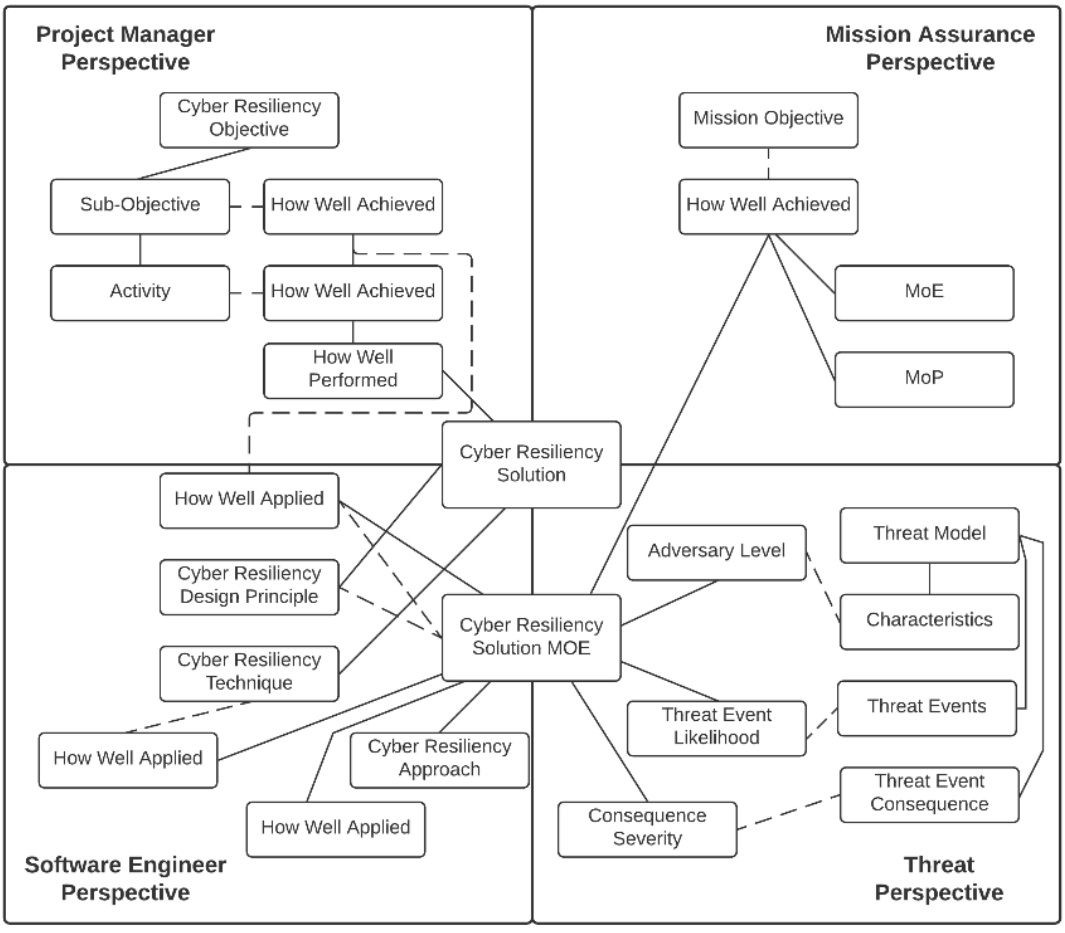


Figure 7 - Relationship of Cyber Resiliency Solution MoE to Other Metrics (D Bodeau, Graubart, McQuaid, & Woodill, 2018)

Mission-focused and effects-based cyber-security requires resilience. Resilience in this context is based on a prediction of the system's capacity to be impacted by a successful cyber-attack, survive through the incident, continue to provide a minimal level of mission-essential services throughout, then recover post-incident (Jakobson, 2013). The focus on the mission allows for prioritised defence decisions, with investment into proactive measures to reduce risk to those systems that are most important to mission success. Mission response is driven by resilience, which is focused on the causal links between mission, effects, crown jewels and the other systems enabling functionality in the space system. Mission response allows for risk-based decision-making, by enabling prioritisation of systems. However, cyber-enabled functions do complicate this simplification due to the capacity for lateral movement by adversaries.

Seemingly insignificant systems can be used to bypass defences, opening weak points and vulnerabilities for exploitation. Working around hard defensive points and then pivoting to the actual target is a standard method for cyber-attackers. This means that defence-in-depth should focus on hardening crown jewels and increasing resilience, but defence-in-breadth is important to provide sufficient coverage that adversaries cannot bypass protections through weak points in the overall architecture. Laser-like focus just on the mission and mission critical systems can indirectly undo excellent security controls, simply because adversary lateral movement has been enabled. Therefore, other approaches must be employed to enhance our understanding of the threat.

2. Risk and Cyber-worthiness

'More people are killed every year by pigs than by sharks, which shows you how good we are at evaluating risk' (Schneier cited in UcedaVelez & Morana, 2015).

2.1 Risk is Uncertainty

Risk refers to the positive or negative effect of uncertainty on objectives (International Standards Organisation, 2018). By reducing uncertainty, risk is also reduced. From a risk management perspective, understanding of the external and internal context of an organisation or system should increase understanding of the environment. Increased situational awareness should subsequently reduce uncertainty, which leads to a decrease in risk. Risk management is intended to protect value by applying controls that influence risk.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 describes the role of risk assessments to '…identify, estimate and prioritise risk' using risk factors, consisting of threat, vulnerability, likelihood and impact leading to risk (National Institute of Standards and Technology, 2012). A generic risk model presented in NIST SP800-30 is depicted in Figure 8 below).

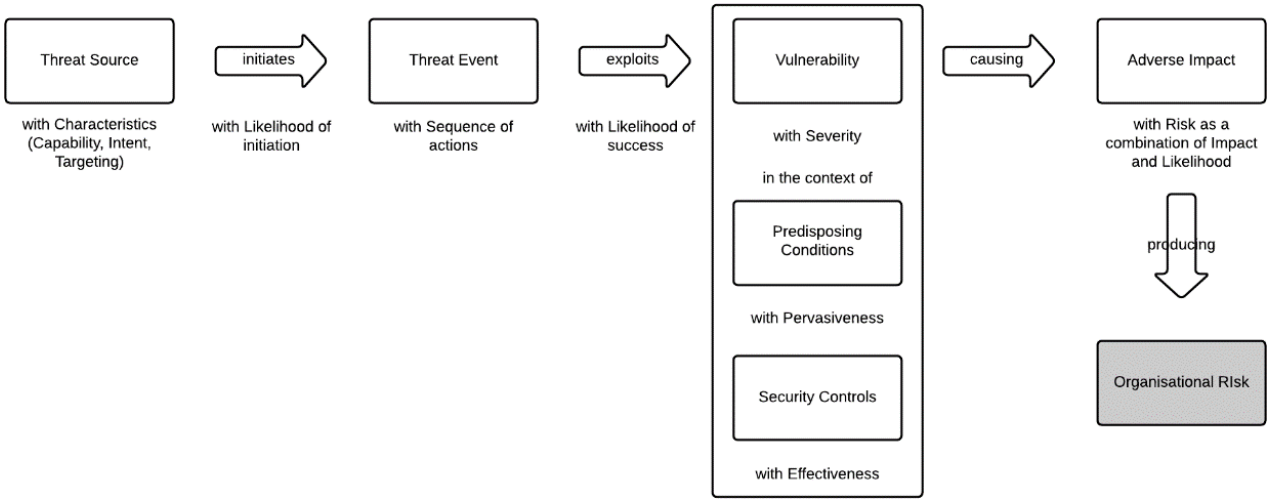


Figure 8 - SP800-30 Generic Risk Model (National Institute of Standards and Technology, 2012)

The model consistently displays the importance of the threat to assess risk. It is the threat source that exploits vulnerabilities. Indeed, most of the key risk factors in this model are based on threat actors, their methods, and the vulnerabilities they seek to target. This is not to say that such detail is mandatory in every sort of risk assessment, but it is intended to inform more accurate cyber-security assessments.

'Risk models differ in the degree of detail and complexity with which threat events are identified. When threat events are identified with great specificity, threat scenarios can be modelled, developed, and analysed. Threat events for cyber or physical attacks are characterised by the TTPs employed by threat sources adversaries. Understanding adversary-based threat events gives organisations insights into the capabilities associated with certain threat sources. In

addition, having greater knowledge about who is carrying out the attacks gives organisations a better understanding of what adversaries' desire to gain by the attacks.

'Knowing the intent and targeting aspects of a potential attack helps organisations narrow the set of threat events that are most relevant to consider' (National Institute of Standards and Technology, 2012).

An example of the type of risk assessment template recommended in SP800-30 National Institute of Standards and Technology, 2012) is provided below in Figure 9.

Threat Event	Threat Sources	Threat Source Chacteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

Figure 9 - SP800-30 Adversarial Risk Calculation Template (National Institute of Standards and Technology, 2012)

This guidance is reinforced by the advice provided in the United Kingdom (UK) for government cyber-threat intelligence reporting (Crown, 2019). The report advocates for more detail than has traditionally been provided in threat assessments, and a transition to more mature reporting outcomes. Specific differences between the approaches of the past and those advocated as mature are described in Table 2 (below).

Table 2: A Comparison of Past and Mature Cyber Threat Assessments

Past Threat Assessment	Mature Cyber-Threat Assessment
A wide range of threat actors are considered, regardless of functional relevance	Only threat actors with the capability and motivation to attack are assessed in detail
Threat actors are grouped in a course fashion	Specific threat groups are considered on a case-by-case basis, dependent on capability and motivation, and regardless of any formal label
Departmental assets are considered coarsely in terms of business impact	There is an in-depth understanding of the business, and critical business assets are considered individually with specific threat actors and attack scenarios considered
Threats such as Foreign intelligence Services are often discounted as being out of scope	There is recognition that most threat actor groups are using commercially available, detectable attacks and that intelligence on their capability is of value

This type of detailed understanding of specific threat actors and their capability and intent aligns to the risk assessment guidance produced by NIST over a decade ago. The requirement for 'in depth understanding of the business, and critical business assets are considered individually with specific threat actors and attack scenarios' certainly extends much further than current Australian National Audit Office (ANAO) cyber-security reporting obligations focused on the deployment of controls aligned to the Top 4 or Essential 8.

Quantitative approaches have been proposed to calculate risk, in a similar way to the calculations provided earlier for resilience. UcedaVelez and Morana (2015) provide a method for calculating residual risk. The calculation method includes Equation 2 below.

Risk (R) is the product of Threat Likelihood (TL), Vulnerability Exposure (VE) and Asset Value (AV).

R = TL x VE x AV

Inherent Risk (IR) is the product of the Threat Likelihood (TL), Ease of Exploitation (EE) and Asset Value (AV).

IR = TL x EE x AV

Risk Mitigation (RM) is the product of the Inherent Risk (IR) and the Control Effectiveness (CE). CE may be effective in both reducing likelihood and impact on the AV.

RM = IR x CE

Residual Risk (RR) is the IR reduced by Risk Mitigation (RM). RR = IR – RM

RR can also be factored as a function of CE. RR = IR x (1-CE)

The Liability (L) incurred by an exploit is a product of the probability of an exploit (P) and the business impact (I).

L = P x I

Equation 2 - Risk Equations

These equations provide a logical, quantitative basis for establishing a variety of risk ratings. There is an argument that they provide greater utility than some of the alternative qualitative approaches evident in the literature. Popular contemporary risk assessment tools and approaches have been criticised as flawed due to their use of Risk Matrices (RM) to support risk assessments in cyber-security.

'The perceived benefit of the RM is its intuitive appeal and simplicity. RMs are supposedly easy to construct, easy to explain, and easy to score. They even might appear authoritative and intellectually rigorous. However, the development of RMs has taken place completely isolated from scientific research in decision making and risk management… The ranking produced by RMs was shown to be unduly influenced by their design, which is ultimately arbitrary. No guidance exists regarding these design parameters because there is very little to say. A tool that produces arbitrary recommendations in an area as important as risk management… should not be considered an industry best practice' (Bratvold, Thomas, & Bickel, 2014).

Purdy has stated that risk management is not about risk registers at all, but about decision-making. He is very disparaging about the state-of-the-art of risk management.

'Understanding your assumptions and the uncertainties inherent in those assumptions is the key to making good decisions… In 1995 when we wrote the first Australian/New Zealand standard, we thought we were being really helpful by cutting in an appendix of the standard for indicative purposes only, a five by five matrix. It was the worst decision we ever, ever made. It wasn't intended to work, it was purely an illustration. It was just sort of this is what a matrix looks. And it wasn't the rating system, it was just a, a heap [of] numbers, you would call it now, as a way of pictorially representing risk in terms of consequence and liability. But of course, you know it then got transmogrified and turned into, well it's almost a religion now… I think we're starting to recognise that most of the decisions [that] remain the important ones, are in the area of complexity. And, and using a two dimensional matrix to deal with complexities, it's, it's like trying

to fly paper plane to the moon. It can't work out. It's just not gonna take off. The way we have to approach things such as complex decision making within the project environment, requires a totally different skill set. A different paradigm entirely. Things aren't two-dimensional matrices and risk registers, they're absolutely irrelevant. And we're not talking about a small number. Most of the decisions you have to make, involve an element of complexity' (Sidorenko, 2021).

Explaining risk and threats in a more approachable and practical way has also garnered attention online, through conversations about 'everyday threat modelling' and the relationship with risk assessments.

The security scenario of being 'sucker-punched in the face' helps to understand the basic concepts of risk, as depicted in Figure 10 (below).

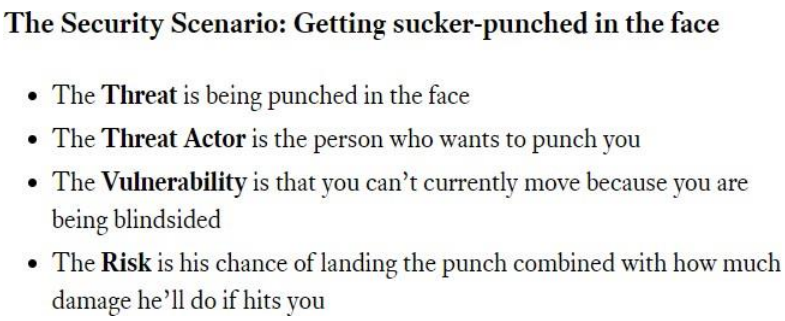


Figure 10 - Everyday Threat Modelling Security Scenario

In this instance, risk is much more than a scenario and the threat; it includes the chance of the scenario occurring and the impact if it happens. The context of the risk and the threat is a significant part of the calculus of risk because it informs why the risk is worthwhile; the reason the risk exists, and why it is worth taking action. It also informs how much should be invested in treating the risk. For example, a threat actor could vary greatly between a prize fighter and a child. This simple change can have a significant impact on the outcome of the assessment (Miessler, 2021). The utility of this scenario has been enhanced with a full taxonomy and numerous Twitter additions (Ellis, 2021).

Hubbard contends that an entirely different approach is needed to effectively assess risk, based on probability metrics that are easier to quantify and calibrate. 'The fact that simple scoring methods are easy to use, combined with the difficulty and time delay in tracking results with respect to reality, means that the proliferation of such methods may well be due entirely to their perceived benefits and yet have no objective value' (D. Hubbard & Evans, 2010). Bias in variation of risk assessments is addressed in Hubbard's approach through using calibration tools to understand confidence intervals associated with the people making the risk assessments, and the likelihood that their assessments are predictive.

Decomposition consists of assessing events based on probabilities of confidentiality, integrity and availability impacts with bounded confidence intervals. An example is provided in Table 3 (below). This approach has merit, but is not necessary sufficient to deal with the mission impact rather than direct financial loss associated with an attack on an SV.

Table 3 - Cyber-Security Risk Decomposition Example

No.	Event Name	Prob. Event Will Happen (Annual)				If event occurs, Conf/Int occurs	If event occurs, Availability occurs	90% interval for CI (Confidentiality/ Integity)		Confidence interval for A (Availability)				Expected Loss from Conf/Int	Expected Loss from Availability	Actual Scenario Outcome, Conf/Int	Actual Scenario Outcome, Availability	Final Result
								Lower Bound	Upper Bound	Duration of Outage (hours)		Cost per hour ($)						
1	Event 1	2%	20%	50%	30%	0	1	$ 110,000	$ 2,200,000	2.00	4.00	$ 6,100	$ 61,000	$ 7,447	$ 1,140	$ -	$ 8,277	$ 8,277
2	Event 2	5%	20%	30%	50%	1	0	$ 10,000	$ 50,000	0.50	2.00	$ 150	$ 450	$ 882	$ 12	$ 7,985	$ -	$ 7,985
3	Event 3	10%	50%	10%	40%	1	0	$ 20,000	$ 400,000	0.25	1.25	$ 3,500	$ 17,500	$ 12,186	$ 278	$ 69,741	$ -	$ 69,741

The use of expert assessments of percentages remains subject to considerable variation and presents problems baselining a common scoring system between engineering and cyber-security teams. This challenge has been studied by D. W. Hubbard and Seiersen (2016). Calibration is conducted through activities to estimate the ability for participants who are conducting risk assessments to quantify their own uncertainty. Quizzes are used to understand and assess uncertainty. This is intended to address the overconfidence evident in the risk assessment community (D. W. Hubbard & Seiersen, 2016, pg 143).

Limited data pertaining to cyber-security hampers risk assessments. Information gaps stem from multiple causes, ranging from corporate drivers to not disclose events for commercial and legal reasons, through to inadequate collection methods. The use of statistical and mathematical approaches described in this report provide a means of addressing the problem without significant information. Additional confidence in risk assessments can be achieved through the use of Bayesian techniques, consisting of network diagrams of observable states described as nodes, supported by a set of probabilities for each node (Pollino & Henderson, 2010).

The risk community has provided little guidance to organisations around reducing the impact of sophisticated adversaries. Looking at the state of cyber-security in 2021, it is evident that existing approaches are insufficient to match the capabilities of threats. Publications such as SP800-30 by NIST have advocated for an adversarial, threat-focused approach, with a detailed understanding of defenders' architecture, for over a decade. In addition, they have implored organisations and communities to define risk models appropriate to their view of risk, including: 'which risk factors must be considered, which factors can be combined, which factors must be further decomposed, and how assessed values should be combined algorithmically' (National Institute of Standards and Technology, 2012, pg 16).

Risk assessment applications to cyber-security are limited by the integrated and interdependent nature of digital systems and their architecture, which may respond in unpredictable ways due to a variety of loosely and tightly connected socio-technical systems. The existence of many loosely coupled systems with limited visibility outside of the technical domain means that risk assessments often lack the technical depth to understand and assess the cyber-threat. However, a stronger link between the concepts and literature pertaining to risk and resilience may enhance the situation. Resilience has been proposed as a risk response, to residual risks and emerging threats (Kott & Linkov, 2018). Residual risk remains after risk treatments have been applied. Resilience, by covering the recovery and reconstitution of capabilities aligned to the mission, is accounting for the residual risk that individual controls and risk mitigations may not address. The concept that resilience deals with residual risk aligns to a requirement for more agile and responsive depth to space systems. This recognises that static risk approaches are unlikely to provide long-term success over the full lifecycle of many systems.

2.2 Cyber-worthiness

Cyber-worthiness seeks to address the regulation of cyber-security for platforms and systems such as SVs by placing a focus on the ability of a system or platform to operate safely and effectively within a contested cyber environment. In this context, cyber-worthiness has been viewed as the possession of an acceptable level of cyber resiliency (Fowler & Sitnikova, 2019). However, cyber-worthiness potentially extends further than resilience. It may also refer to the design choices and decisions inherent in system configuration and the threats modelled against the chosen architecture.

'Lex Informatica' refers to the difference between a system built from code and a physical system. Whilst physical systems are regulated through natural laws, which are consistent between systems, the regulation of cyberspace through code and architecture creates a complicated and varying landscape that continually changes between instances. The '…code sets the rules… it regulates behaviour in this space; it determines what's possible here, and what's not possible' (Lessig, 2002, pg 5). Network architecture can change in moments from the command line, whereas a physical object is generally modified through a systematic and planned process (Lessig, 1996; Reidenberg, 1997). The environment within whicha cyber-enabled device or network is operating can change into entirely unexpected and new forms depending on how it is configured and utilised. This is further complicated through the wide variety of network architectures and protocols that can be utilised by an adversary to design workarounds and defeat system protections. There is a distinct difference between a system accredited using a risk-based technical and business approach, which establishes a static baseline of security using policy, and a system designed to be resilient in a contested and hostile operating environment.

In the context of LEO SVs, increasing resilience will not necessarily increase cyber-worthiness. For example, increasing the distribution of a satellite constellation will increase overall resilience. It will not necessarily increase cyber-worthiness; indeed, it may reduce the cyber-worthiness of the system. 'The mass production of satellites for a proliferated constellation could easily result in the cyber vulnerabilities of any particular satellite replicating across a network, making it easier to attack the entire architecture' (Hallex & Cottom, 2020). The cheap and minimalist design approach, rewarded in commercial arrangements for LEO missions, would be to develop the same sort of SVs on scale with maximum reuse of componentry and software. This approach may lead to a homogenous system of systems and limited degeneracy, increasing resilience but degrading cyber-worthiness.

LEO system architecture, without sufficient planning, could be vulnerable to attacks of a kind that traditional satellite planning has not yet needed to consider. Cyber-attacks are more likely to be successful against such constellations, as the larger number of targets increases the potential for a platform to be misconfigured or unpatched. Homogenous constellations may offer significant redundancy from kinetic or physical threat, but they may only slow a cyber-attack, at best, as it hops across network connections and infects the constellation.

They would certainly complicate the task of threat hunting. In contrast, multi-layered and diverse architectures may increase cyber-worthiness, as the constellation will become less homogenous. A different type of resilience can be achieved with degeneracy. However, degeneracy also increases the attack surface by adding more complexity and different options to attackers.

In a complex network, a single weak point may be sufficient to reduce the cyber-worthiness of the entire constellation. There are different mitigations to reduce this risk, but each has its own

challenges – such as the difficulty of monitoring LEO traffic when bandwidth is precious, and where fast orbits may result in intermittent communication. Monitoring increases the security effort required to maintain a network; a maintenance burden that may exist for years.

Encryption, the mainstay of LEO security, may also reduce the speed of detection and prevent effective remediation of an attack that is pivoting between nodes of a constellation. In some cases, encryption can be a strong ally to an attacker, as it can mask the nature of communication between systems. These are all risks that must be considered in advanced LEO constellation configurations.

2.3 Cyber-security for Road Vehicles

The relationship between LEO SV cyber-security and road vehicles is not immediately obvious. However, road vehicles have been subjected to decades of regulation and possess strict safety controls with globally enforced standards. Although the development of digitally-enabled road vehicles has not been without cyber-security issues, the regulatory aspects have received considerable attention in the last five to ten years. *International Standards Organisation (ISO) 21434* remains in draft at the time of writing this report, but it has a strong pedigree inherited from the *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061_201601* (SAE International, 2016). J3061 provides guidance for cyber-security of digitally-enabled vehicles and ISO 21434 builds upon J3061 with a developed approach to cyber-security risk management, which has been supported by automotive industry engagement, communities of practice, data sharing, and the development of tools over several years.

These standards have been further reinforced through the drafting of *ISO 24089 Road Vehicle Software Update Engineering* (International Standards Organisation, 2021) and the release of *United Nations (UN) Regulation 155* (United Nations, 2021). *UN Regulation 155* provides a high-level approach to certification and compliance activities, including a list of threats, vulnerabilities, attack methods and corresponding mitigations, as well as the requirement for the threat analysis to consider possible attack impacts (effects). This approach provides for consistent standardisation of vehicle cyber-security certification and therefore fits at least some of the parameters of a cyber-worthiness approach. However, cyber-worthiness is a feature of the system lifecycle and *'…*is not static – it must be developed and then maintained as the situation and mission evolves*'* (Romanych, 2005, pg 29). There is a significant risk in providing lists of attack methods and focusing on compliance. However, *UN Regulation 155* does not stand in isolation, as it builds on the guidance provided for the vehicle industry in ISO 21434.

ISO 21434 incorporates a model specifically to manage the product development and Software Development Life Cycle (SDLC) process. This aligns to the view of 'Security as Code' demonstrated in the Development Security Operations (DevSecOps) philosophy. The utilisation of DevSecOps ensures security is integrated naturally as part of the software development and operational cycle, reducing vulnerabilities and supporting agile development approaches with a solid understanding of security (RedHat, 2021).

An example of the ISO 21434 approach as it applies specifically to the product development process is depicted in Figure 11.

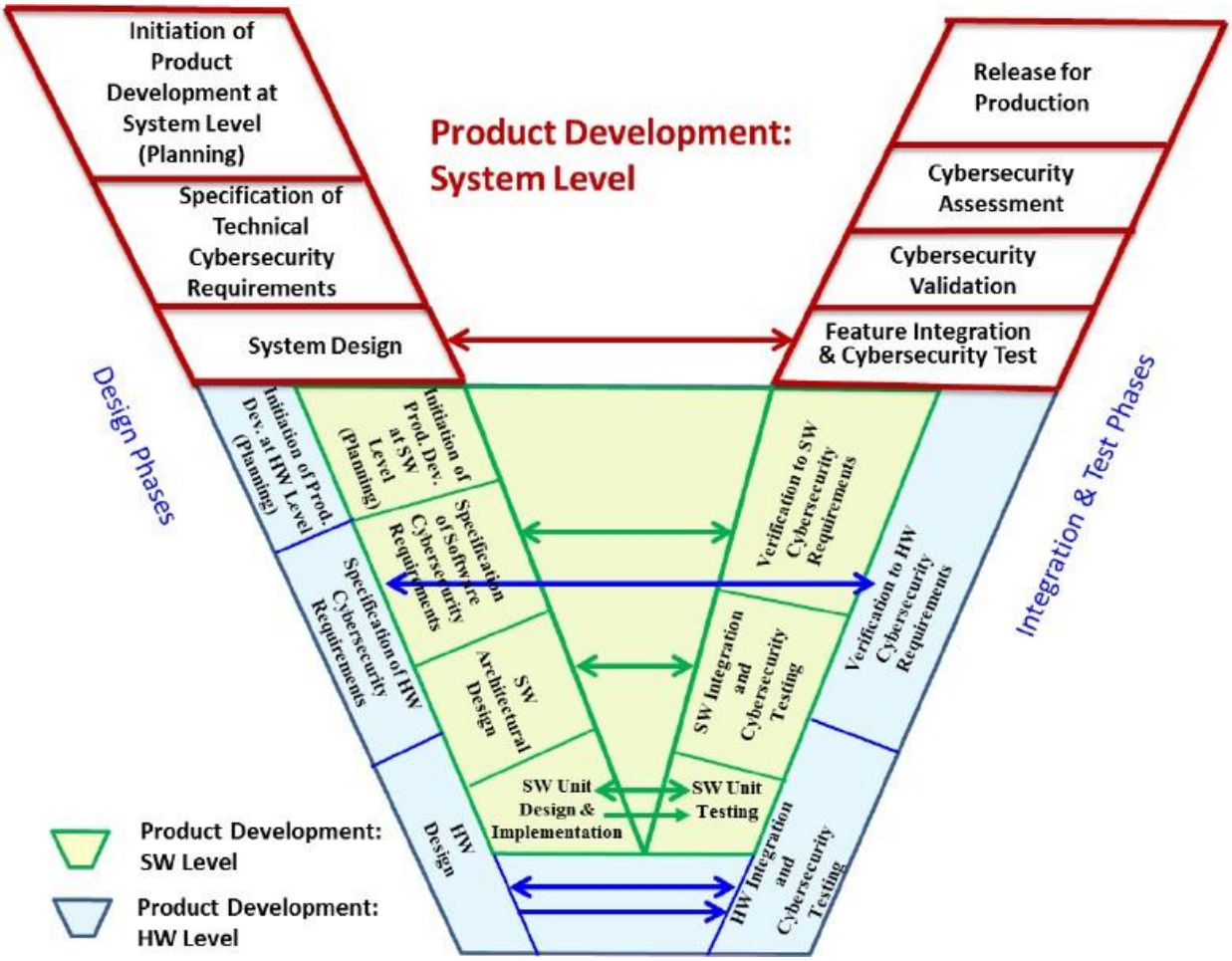


Figure 11 - ISO21434 Cyber-security integration into the Product Development Process

The incorporation of product development increases the requirement for supporting planning and artefacts. For example, a production control plan is recommended within the Standard. Such a plan would have the potential to significantly enhance the cyber-security controls applied during the design and development of LEO space systems, if implemented by well-trained and motivated cyber-security professionals in conjunction with the engineers and project managers overseeing LEO system production.

ISO 21434 could be seen as inspiration or exemplar for establishing an early model of what an LEO cyber-worthiness framework may look like, with some additional developments and modification. The incorporation of a resilience calculation model, as presented earlier within this report, and detailed digital twin and evil twin models could be added.

3. The Digital Twin

3.1. A Model of the Space Domain

'Basic digital twins encompass any kind of real-world data point that is digitally replicated for the purposes of keeping track or making predictions, and some of the most sophisticated digital twins include detailed 3D models which are like the computer- generated special effects we've seen for decades in movies' (Tordable, 2021).

Different models of space system architectures exist, including the one depicted in Figure 12 below (R. Burch, 2013). In this example, different segments are used including space, launch, control, user and network. This report utilises a model of the space domain to support the development of an experimental approach. The full model will be introduced later in this chapter.

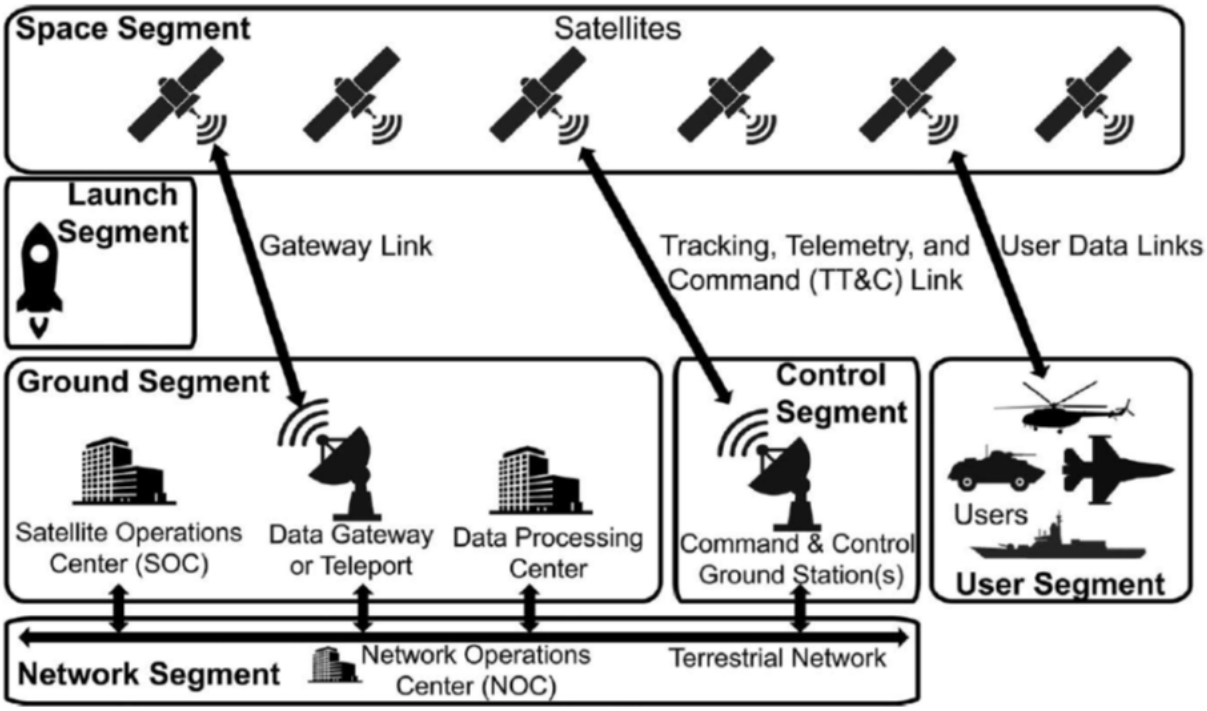


Figure 12 - Key Components of a Space System Architecture (R. Burch, 2013)

The specific components and networking arrangement to support a space solution can vary greatly, depending on a variety of factors. LEO constellations bring their own challenges due to their dynamic network topology, reducing the opportunity to apply traditional routing approaches (Hussein & Hanani, 2016). Self-configuring network solutions will be required to support the flexibility and mobility inherent of future LEO mega-constellations (Yang, 2018).

Digital Twins simulate space systems and their functions, and require many different components to successfully replicate real space systems and SVs. NASA, the European Space Agency, and civilian organisations provide a broad array of simulation and software solutions for space systems.
For example, mesh communication software (NASA, 2021a), debris modelling (NASA, 2019b), orbit visualisation (LeoLabs Inc, 2021), and performance behaviour (European Space Agency, 2005).

The Small Spacecraft Virtual Institute provides an array of useful tools for managing space missions for small SVs (NASA, 2021b). This includes trajectory design, mission control, radiation analysis, project management and other mission management software.

Information on different SV and space system technologies to support the development of digital twins is available through a variety of sources. This includes the NASA report on *State of the Art of Small Spacecraft Technology* (NASA, 2020) and books that describe specific software and hardware solutions in use on SVs (Sebestyen, Fujikawa, Galassi & Chuchra, 2018). *The RocketLab Payload User Guide* (RocketLab, 2020), *SpaceWire Standard* (European Cooperation for Space Standardisation, 2014), *Software Engineering Handbook for flight and ground systems* (European Cooperation for Space Standardisation, 2013), *OpenLST radio design* (Planet, 2021), and a multitude of academic papers and publications provide insights for those who are building digital twins of satellite systems, as well as those researching for nefarious attack vectors and researching communication and security protocols in order to defeat them.

Running different simulations requires a federation of systems to work together. Simulation federations offer an approach that maximises best-of-breed simulation options, providing versatility for digital twin creation. The Space Reference Federation Object Model (SpaceFOM) provides guidance on the use of High Level Architecture (HLA) Run Time for distributed simulation. SpaceFOM considers aspects such as the management of time and entity attributes, including dynamic data sharing between different simulation systems and entities. SpaceFOM has been used for a variety of simulation scenarios, including Model, Processor and Hardware-in-the-Loop testbeds and simulations using various sensors and software systems (Moller et al., 2019).

3.2. A Common Generic Model of an LEO Space System Digital Twin

Table 4 and Figure 13 below depict potential generic versions of LEO SV and supporting system architectures, which can be developed into representative digital twin systems for testing purposes. These generic versions do not create a security, safety or intellectual property risk for satellite operators. However, they do allow for the testing of principles and approaches to determine appropriate methodologies and models that can subsequently support real systems in the future. These models will be used more extensively in Part Two of this report, and are presented here as a baseline for further development.

Table 4: Common Generic LEO Space-System Cyber-Security Digital Twin Testbed Sub-systems

LEO Vehicle		Ground Station	Launch Vehicle	Launch Site
Bus System	**Payload System**			
Command and Data Handling (BCDH)	Payload Processing Module (PPM)	Encryption and Certificate Management (GECM)	Launch Vehicle Software Stack (LCSS)	Launch Control Software Stack (SCSS)
Electrical Power System (BEPS)	Payload Sensor Systems (PSS)	Application Programming Interfaces (GAPIs)	Propulsion System (LPS)	Fuel System (SFS)
Telemetry and Tracking (BTT)	Payload Data Storage (PDS)	Directory Services (GDS)	Avionics and Telemetry (LAT)	Launch Site Management System (SMS)
Communication Subsystem (BCS)	Payload Antenna Array (PAA)	Ground Control Network (GCN)	Launch Vehicle Communications System (LCS)	Encryption & Certificate Management (SECM)
Attitude Determination and Control System (BADCS)	Mission Systems (PMS)	Flight Control Software Stack (GFCSS)	Fuel System (LFS)	Application Programming Interfaces (SAPIs)
Thermal Control (BTC)	Payload System User (PSU)	Cloud Services (GCS)	Electric Pump System (LEPS)	Directory Services (SDS)
Services Control (BSC)	Payload System Admin (PSA)	Human Social Network (GHSN)	Launch Vehicle User (LSU)	Cloud Services (SCS)
Bus System User (BSU)	Payload System Network (PSN)	Ground Station User (GSU)	Launch Vehicle Admin (LSA)	Launch Site User (LSU)
Bus System Admin (BSA)		Ground Station Admin (GSA)	Launch Vehicle Network (LVN)	Launch Site Admin (LSA)
Bus System Network (BSN)		Ground Station Network (GSN)		Launch Site Network (LSN)

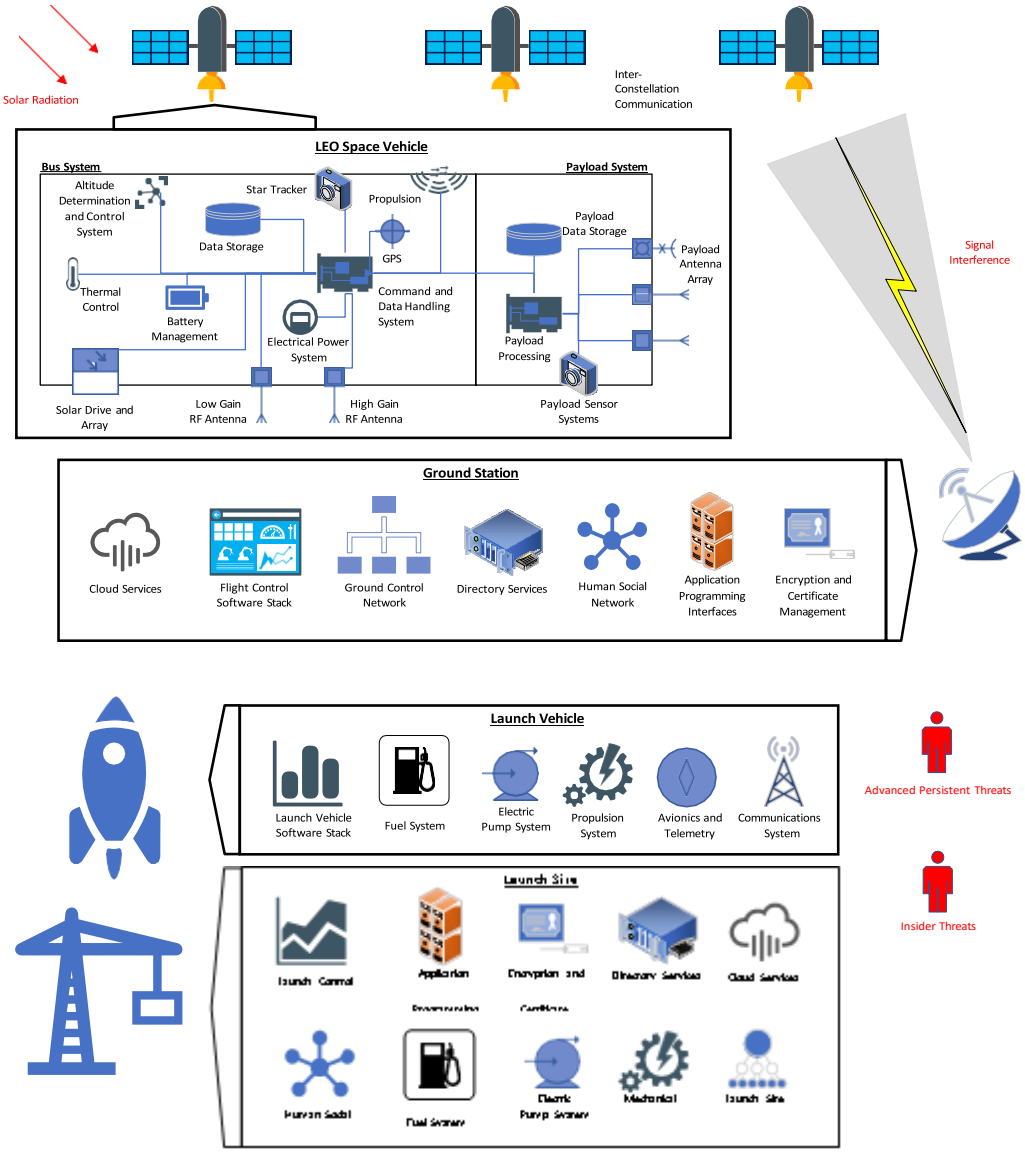


Figure 13 - Common Generic LEO Space-System Cyber-Security Digital Twin Testbed High Level Architecture

3.3. Part Two of this Report

The common generic model presented above will be utilised in Part Two to develop a cyber-security Digital Twin. This Digital Twin will subsequently be used to demonstrate the utility of the EDT and provide examples of the various assessment processes recommended to secure LEO space systems from cyber-attack.

4. The Evil Digital Twin

'This is what I call a target rich environment' (Maverick, in the movie, 'Top Gun').

4.1 LEO Space Systems as Targets

The EDT is designed to provide a means of testing and evaluating LEO SVs and systems from an adversarial perspective, concentrating on the threat as the key actor in a cyber-attack. The EDT supports the prediction of system behaviour in a cyber-security context to prepare LEO SVs and space systems for real-world missions. Digital twins are generally defined based on their protocols and designs; what is allowable and feasible within the design specifications. To manage the risk of attack, designs must incorporate events outside of expected behaviours and use cases. This is the EDT. This sort of thinking is evident throughout the threat modelling approaches in the cyber-security body of literature discussed throughout this report, including the application of misuse cases (UcedaVelez & Morana, 2015) such as the type depicted in Figure 14 below.

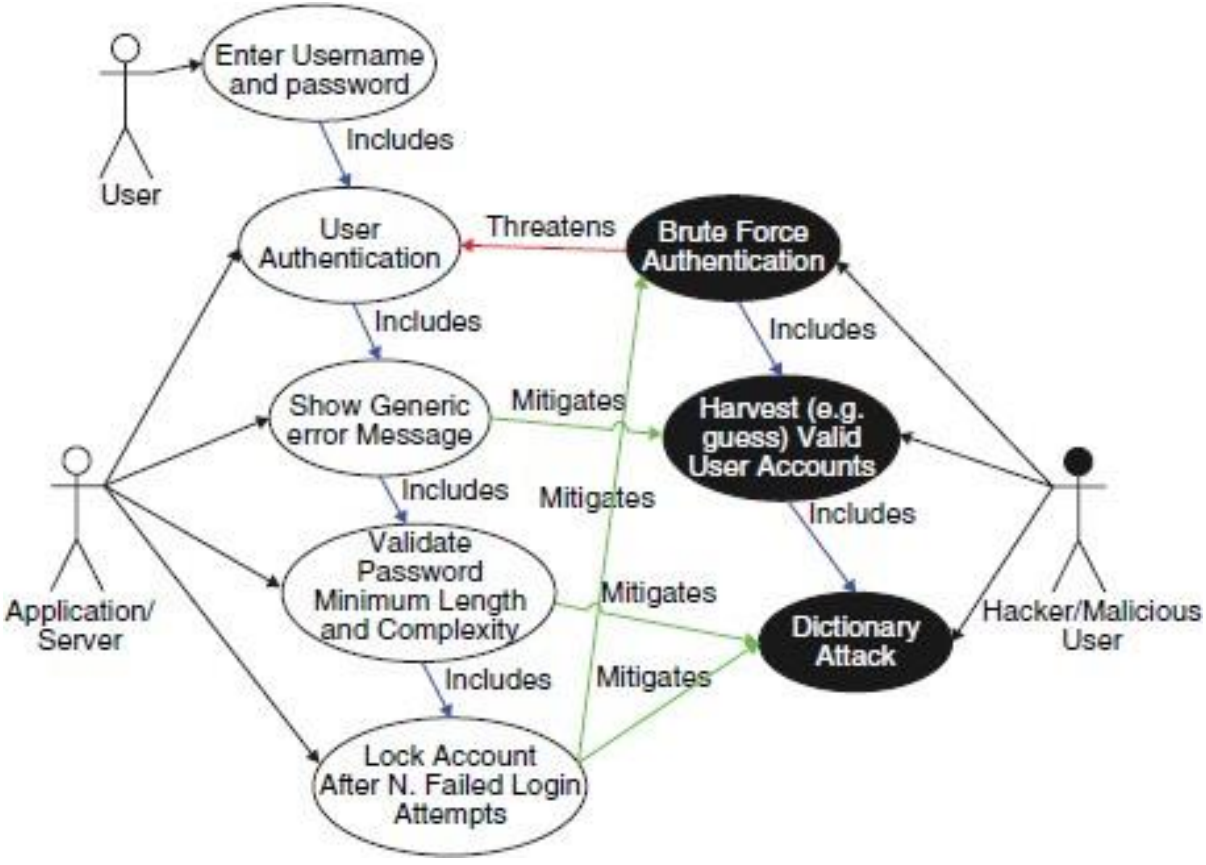


Figure 14 - Use and Misuse Case of User Logon with Mitigation Mappings (UcedaVelez & Morana, 2015)

Misuse cases are one method of focusing on threat actor intent and TTPs. Cyber Prep is another approach that focuses on threats and their relationship to system controls and defences (Deb Bodeau & Graubart, 2016). Cyber Prep involves adversary profile development and a move away from compliance thinking to an advanced threat-orientated risk management mindset.

Adversaries are modelled based on specific characteristics, including their intent, targets and capabilities. Organisational strategies are then used to defend against these threats, including governance, operational processes, architecture and engineering. Cyber Prep defines a relationship between the adversary and defender structure, as depicted in Figure 15 below.

Figure 15 - Cyber Prep Comparison of Adversary and Organisational Strategy (Deb Bodeau & Graubart, 2016)

The Cyber Prep model demonstrates the view that adversaries are a significant driver of security strategy, including the development of governance, operations and engineering. The EDT is an extension of this thinking; the adversary is critical to good cyber-security. The EDT informs, predicts, and emulates the adversary. The digital twin, without its evil opposite, could teach the wrong lessons if design is focused on user intentions only. The EDT is a critical part of the design space and represents a rapidly evolving part of the hostile environment against which space systems must be engineered to operate. EDT allows for planning outside of the traditional engineered space, emulating and modelling an intelligent, curious and resourced adversary.

4.2 Cyber-Jeopardy and Response (CY-JAR)

CY-JAR provides space domain awareness using anomaly attribution and situational awareness. Making sense of the environment allows for defensive functions to identify jeopardy and respond in an intelligent way. The ability for LEO SVs to independently respond to threats will be a significant step towards mission resilience and the delivery of trusted autonomous SV operations.

The introduction of jeopardy and response functions to a wide range of threats in LEO platforms is logical, given the increasing risks inherent in SV operation, the increased traffic in space, and the ever-growing satellite constellations moving at great speed in orbit around Earth.

*'*Persons in the loop for satellite systems operations slow response times due to the risk of making the situation worse. This can extend the outage time… One method of improving response times is to embed greater autonomy and cognitive functions in the system itself. A smart system can more efficiently self-monitor and quickly respond to suspicious or outright threatening conditions... [an] issue is determining what level of policy authority these systems are given, and how much trust is imparted to faithfully execute operators' wishes, particularly in contested environments. These concerns must be addressed if future space systems are to fully embrace complex cognitive autonomous features*.'* (R. Burch, 2013, pg 171).

The challenge of the convergence of space and cyber and the development of a CY-JAR solution is that existing cyber-security dictums and assumptions are not always true for specific SVs, such as LEO constellations.

'Ultimately, space systems are much more than mere 'computers in the sky'. Well-regarded terrestrial security practices often fail to transfer to space systems for unintuitive reasons which require a wide breadth of expertise to overcome. The result is that relatively little work, especially within systems security, has been conducted on space technologies' (James Pavur & Martinovic, 2020, pg 5).

The evolving nature of adversary capabilities also needs to be considered in the LEO context. SVs with multi-year lifespans should consider future risks. For example, quantum communications solutions are likely to degrade the security capabilities of traditional cryptographic-based protection and potentially make many existing encryption controls obsolete (Unal, 2019).

Despite the broad promulgations relating to the space threat, there remains a view that 'space is a sanctuary*'* (McLeod et al., 2016). The traditional focus of satellite security has been based on the dictum of 'security through obscurity'. An example of the prevalent view on cyber-security in space, which reinforces the security through obscurity notion, is provided by the NATO Joint Air Power Competence Centre, which contends that in the instance of a cyber-attack:

'…the primary aim is not the takeover of the satellite by the attacker. The objective is primarily the suppression of their services. To protect communications between the ground stations and the spacecraft, high end, encrypted communication is used to create the best possible protection against any kinds of cyber-attacks' (Vasen 2021).

This thinking is also reflected through industry channels. The Utah State University Conference on Small Satellites in 2018 received a research recommendation to adopt a 'policy that, for those cubesats and smallsats that have propulsion, that the industry adopt a 'no encryption, no fly' rule' (Foust, 2018).

Encryption is a useful means of providing one form of defence to a platform's communication system. However, encryption provides a single means of defending an SV and is not relevant to all forms of cyber-attack. Indeed, encryption can be used to facilitate some forms of attack and support undetected manoeuvre between systems where intrusion detection has been employed. Space systems software and networks are susceptible to cyber-attack, despite cryptographic protection (Pawlikowski, Loverro & Cristler, 2013). The means of encryption deployment, security applied to private keys, and a host of other factors, can degrade the effectiveness of encryption as a security solution. Encryption is a viable defensive control, but it is just one. Although a system may be 'hard to clone and attack, it is the way in which they are used that compromise

the security of the entire system… security is all about context… it is a mistake to treat a problem in isolation, as it is likely to lead to broken systems' (Drimer, 2009).

Space system leaders, risk managers and engineers need to embrace the security design practices recommended by the Open Web Application Security Project (OWASP), one of which includes the mantra that 'the security of a mechanism should not depend on the secrecy of its design or implementation' (OWASP, 2020). Satellite Communications attacks have been demonstrated on numerous occasions in a non-malicious environment using limited resources (Barrett, 2019; J. Pavur, 2020; James Pavur & Martinovic, 2020; Santamarta, 2014). Developing repeatable, robust security approaches is vital as the space industry continues to grow and expand into the future. New space opportunities include the launch of mega-constellations, vastly increasing the number of SVs and ground stations in use. As opportunities grow, the attack surface and possibilities for malicious actors, which are already numerous, will increase (James Pavur & Martinovic, 2020).

Despite some arguments to the contrary, obscurity as a broad concept is fading through the increasing numbers and total value of the space sector, the increasing international competition between nation states, the increasing sophistication of non-state actors, and the interconnected nature of cyberspace and the space industry, combined with the low cost of entry for malicious actors. The rapid growth of the sector, increased access to the technologies involved in satellite systems, and increasing integration of commonly employed civilian systems that are not as bespoke as they once were (admittedly with some customisation), all mean that obscurity is not the answer (James Pavur & Martinovic, 2020). This reality is already evident outside of the space sector and has been demonstrated through a wide variety of cyber-security compromises and breaches across many different industries. Rather than relying on security through obscurity and encryption, the industry should embrace security through threat-driven resilience.

A significant difference in the cyber-security approach for space systems and terrestrial cyber-security leading practice is evident within some of the literature, due to the specific nuances of SV operations and environmental conditions. For example:

'…it is hard to detect if an adverse effect was due to a cyber-attack or a natural phenomenon. Thus, measures should be prepared for byzantine failures, where the adverse effect is recognized, measured, and treated without emphasizing the root cause of the error' (Kang, 2018).

This approach is understandable given the hostile environment and the likelihood of bit-flips. However, failure to identify potential adversaries and their associated TTPs can provide an opportunity for persistence by the attacker. Indeed, the standard redundancy measure of restoration through Field Programmable Gate Array (FPGA) reboot is unlikely to be a successful strategy if such a reboot simply provides an adversary another opportunity to conduct the same attack, without fear of new security controls being applied. In fact, the reboot process could be utilised to increase the attack surface by rolling back previously applied patches. Patching is further complicated in mesh networks across constellations, where communication solutions and dynamic links impact patch sharing and broadcast between SV nodes.

Ground station compromise provides a large attack surface due to the extensive human network and terrestrial system connections associated with their function. These risks remain despite the use of security controls, security tools and the integration of Security Operations Centres (SOCs). Ground stations are a central component of space operations and as the connection between

deployed SV and terrestrial networks, they are a key vector for attack. For example, commercial ground stations have been identified as potential vectors for attack on US government space systems (Economic and Security Review Commission, 2011).

The interconnected nature of space systems is amplified by the increasingly hybridised nature of the space ecosystem. Left-of-launch attacks generally refer to cyber-attacks on ballistic missiles and missile defence systems in a military context, conducted prior to launch. However, the principles shared between left-of-launch attacks on military systems and space launch vehicles are extensive. Pre-emptive attacks on launch vehicles, launch sites, supporting systems and supply chains all offer adversaries an opportunity to disrupt and potentially destroy space assets (Lewis & Unal, 2019). For example, the destruction of a single launch vehicle can have an extensive impact on the resupply of SVs to a constellation, with a broad attack surface. The variety of different attack surfaces available throughout the life of a space system presents a complex, wicked problem to engineers and operators seeking to defend these systems and provide mission assurance. Rather than focus purely on desktop assessments of risk, it is necessary to construct life-like representations and digital twin testbeds to test assumptions and support the development of innovative and new solutions to these security problems. Small, sovereign launch capabilities will increase the opportunities for adversaries to conduct left-of-launch attacks, as the network defences available for smaller operators are likely to be more modest than many existing large-scale launch providers. Australia is developing launch services such as Southern Launch (Southern Launch, 2021) and Gilmore Space Technologies (Gilmore Space, 2021) that will be capable of servicing LEO SVs. Rocket Labs are able to provide a more mature launch and production capability in the Southern Hemisphere, from New Zealand (Rocket Labs, 2020).

5. Adversary Behaviours

‘I keep warning you. Doors and corners, kid. That's where they get you’ (Corey, 2013).

5.1 Understanding Adversary Behaviours

Space threat assessments provide a high-level and strategic view of threat actors and their cyber activities that could lead to space mission disruption (Harrison et al., 2020). However, these approaches do not provide a means of understanding specific adversary behaviours, and such a high-level analysis provides little in the way of actionable intelligence. There are a variety of models available to understand adversary TTPs. A core element of understanding adversary behaviours is the pyramid of pain depicted in Figure 16 below.

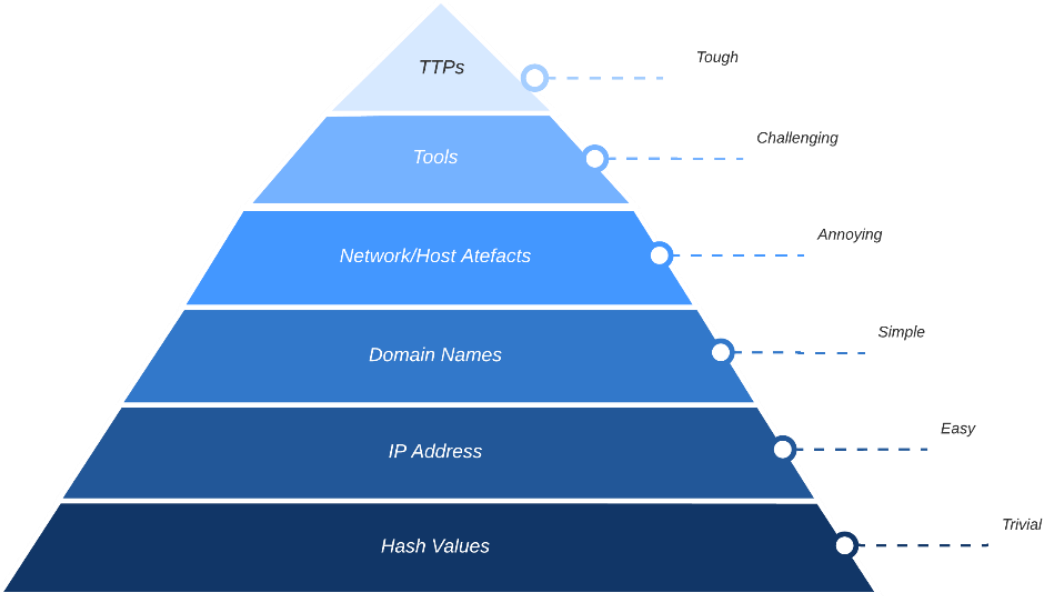


Figure 16 - The Pyramid of Pain

The pyramid of pain describes the increasing difficulty involved for an adversary to change indicators and warnings related to their behaviours. On the one hand, changing hash values and IP addresses at the bottom of the pyramid is easy. Changing tools and TTPs at the top of the pyramid is more challenging. This means that defenders should, wherever possible, seek to understand the behaviours of their adversaries at the top of the pyramid. Hash values and IP addresses are still valuable and support operational activities, such as updating monitoring systems using intelligence feed data and blocking known attacks. However, they are relatively simple for threat actors to alter and bypass these controls.

The TTPs employed by adversaries can be described in different ways depending on the model employed by defenders. Industry applies different language depending on the model utilised. The Lockheed Martin Cyber Kill Chain is one example of a seven-step process often used to describe threat behaviours and TTPs (Lockheed Martin, 2015). The Diamond Model of Intrusion Analysis is used to support cyber intrusion analysis and deconstruct the elements of intrusion events (Caltagirone, Pendergast & Betz, 2013). The Diamond Model comprises four features: adversary,

infrastructure, capability and victim; together with several meta-features related to intrusion events. The Diamond Model is also supported by six axioms. These axioms provide an excellent start point for cyber-security teams to baseline their understanding of adversary behaviours and a means of building a common lexicon and foundational agreement on threats to LEO systems (Caltagirone et al., 2013):

1. 'For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result.
2. There exists a set of adversaries (insiders, outsiders, individuals, groups, and organizations) which seek to compromise computer systems or networks to further their intent and satisfy their needs.
3. Every system, and by extension every victim asset, has vulnerabilities and exposures.
4. Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result.
5. Every intrusion event requires one or more external resources to be satisfied prior to success.
6. A relationship always exists between the Adversary and their Victim(s) even if distant, fleeting, or indirect.'

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a powerful knowledge base of adversary TTPs. This has been the most successful recent model for common agreement across industry, which provides sufficient detail and information to support practical measures to defend networks and hunt threats (MITRE, 2021d). The high-level ATT&CK tactics are mapped below in Figure 17.

Tactic Reference	ATT&CK Tactic	Description – The adversary is trying to…
TA0043	Reconnaissance	gather information they can use to plan future operations.
TA0042	Resource Development	establish resources they can use to support operations.
TA0001	Initial Access	get into your network.
TA0002	Execution	run malicious code.
TA0003	Persistence	maintain their foothold.
TA0004	Privilege Escalation	gain higher-level permissions.
TA0005	Defense Evasion	avoid being detected.
TA0006	Credential Access	steal account names and passwords.
TA0007	Discovery	figure out your environment.
TA0008	Lateral Movement	move through your environment.
TA0009	Collection	gather data of interest to their goal.
TA0010	Exfiltration	steal data.
TA0011	Command and Control	communicate with compromised systems to control them.
TA0040	Impact	manipulate, interrupt, or destroy your systems and data.

Figure 17 - High Level MITRE ATT&CK Tactics (MITRE, 2021)

MITRE Tactics are further decomposed into techniques and sub-techniques, which form an extensive curated knowledge base about contemporary adversary behaviours. MITRE navigator is a web-based repository available for research and low-overhead analysis (MITRE, 2021e). The MITRE ATT&CK workbench extends on and syncs with the MITRE ATT&CK knowledge base. The ATT&CK workbench provides customised instances of MITRE ATT&CK for different community requirements and the ability to share extensions across the community (Center for Threat Informed Defense, 2021). The ATT&CK workbench will be used to support Part Two of this report. The collection arising from Part Two of this report is intended to be deployed on the ATT&CK workbench for sharing across the SmartSat CRC community.

MITRE ATT&CK data is available in common data standards such as *Structured Threat Information Expression (STIX) 2.0* (MITRE, 2021c). MITRE ATT&CK has also been used to develop an understanding of attacks on machine learning solutions, such as the Adversarial Threat Landscape for Artificial-Intelligence Systems (MITRE, 2021a). The Common Attack Pattern Enumeration and Classification (CAPEC) is also maintained by MITRE, although it rests outside of the ATT&CK taxonomy. CAPEC is useful in understanding adversary behaviours, although the focus is on application security rather than the broader ATT&CK focus on network defence and adversary lifecycles to support network exploits. Fortunately, CAPEC is mapped to the ATT&CK taxonomy so the two approaches can be used together (MITRE, 2021b).

5.2 Enhancing security through adversary behaviours

MITRE recommends a specific approach to developing defensive recommendations through an understanding of adversary behaviours. The employment of this model is a focused adversarial technique conducted through the following steps (MITRE cited in Cybrary, 2021):

1. 'Determine Adversary Priority Techniques and Sub-Techniques;
2. Research how Adversary Priority Techniques and Sub-Techniques are used;
3. Research Defensive Options Related to Technique;
4. Research Organisational Capabilities and Constraints;
5. Determine Specific Trade-offs; and
6. Make Defensive Recommendations'.

Having established a Threat Library by identifying specific threat actors who have the requisite capability and intent to target a LEO system, the cyber-defence team undertake a process to determine the various ATT&CK Matrix techniques and sub-techniques likely to be employed, then research and understand precisely how these techniques and sub-techniques are used at a technical level. Techniques are researched in parallel with MITRE Shield, to explore the defensive options available to mitigate these techniques, including the employment of non-technical security controls. Making this information actionable then requires an analysis of the restrictions, constraints and opportunities available, given the architecture and resources involved in the defended system. Trade-offs are determined and defensive recommendations are developed. These should be integrated into a defined governance and risk management process, to ensure appropriate trade-offs are made and risk is accepted at the right level.

The development of formalised and detailed processes as part of adversary emulation is evident in a recent pilot program for the Australian financial industry. The Cyber Operational Resilience Intelligence-led Exercises (CORIE) pilot program seeks to provide in-depth adversary emulation reconnaissance and attacks on financial industry networks, supported by threat intelligence providers (Council of Financial Regulators, 2020). These CTI providers are certified to perform analysis on real-world threats targeting the financial industry, and develop threat intelligence reports and targeting reports covering TTPs and open-source intelligence available to adversaries that could be used to target and penetrate systems (including dark web sources). This information is then used to inform long-term red teaming and penetration testing activities and reporting.

The Space Information Sharing and Analysis Center (Space ISAC) is a US non-profit established to support threat data sharing (Space ISAC, 2021) with enterprise and small business membership options. The sharing model is depicted in Figure 18 below.

Figure 18 - Space ISAC Partner Information Sharing Model

The Space ISAC was reported to meet initial operating capability in February 2021, using a partner organisation and platform (Cyware) to share threat intelligence (Underwood, 2021). The Cyber Security Centre of Excellence at the European Space Security and Education Centre is a European alternative, providing an industry hub for cyber and space activities including educational activities. The project formally commenced in 2017 and concluded in 2019, although it appears to remain active in Belgium (European Space Agency, 2020a).

Malware Information Sharing Platform and Threat Sharing (MISP) is a threat information sharing platform. MISP is most powerful as a collaboration tool, offering a means of sharing threat TTP sightings and correlations (Computer Incident Response Center, 2021). These sharing tools and standards are not tailored for the Australian space industry, but an example of what is possible is the automotive industry. The development of strong standards and regulation has come about in this industry by sharing information and data. Examples include the Automotive Security Research Group (ASRG) with 5882 members (ASRG, 2021) and the OPEN format for eXchanging Security Analysis Models (openXSAM) (openXSAM, 2021).

5.3 Defending Against Adversary Behaviours

MITRE Shield (MITRE, 2021f) is built upon the ATT&CK framework, but with a focus on cyber-defence. MITRE Shield is a knowledge base, providing a range of options from cyber=deception to adversary engagement operations, with the intention to support countermeasure employment and intelligence gathering on adversaries. Table 5 below provides the high-level defensive tactics described in MITRE Shield.

Table 5: MITRE Shield High-level Tactic Descriptions

Tactic Reference	Shield Tactic	Description
DTA0001	Channel	Guide an adversary down a specific path or in a specific direction.
DTA0002	Collect	Gather adversary tools, observe tactics, and collect other raw intelligence about the adversary's activity.
DTA0003	Contain	Prevent an adversary from moving outside specific bounds or constraints.
DTA0004	Detect	Establish or maintain awareness into what an adversary is doing.
DTA0005	Disrupt	Prevent an adversary from conducting part or all of their mission.
DTA0006	Facilitate	Enable an adversary to conduct part or all of their mission
DTA0007	Legitimise	Add authenticity to deceptive components to convince an adversary that something is real.
DTA0008	Test	Determine the interests, capabilities, or behaviours of an adversary.

The Shield Active Defence Matrix is depicted in Figure 19 below. This matrix provides additional information to high-level MITRE Shield Tactics. For example, adversary group mappings are included in the MITRE Shield knowledge base with mappings to Opportunities, Techniques, and Use Cases to support defenders in adopting defensive techniques to counter adversary TTPs (Goffin, 2020).

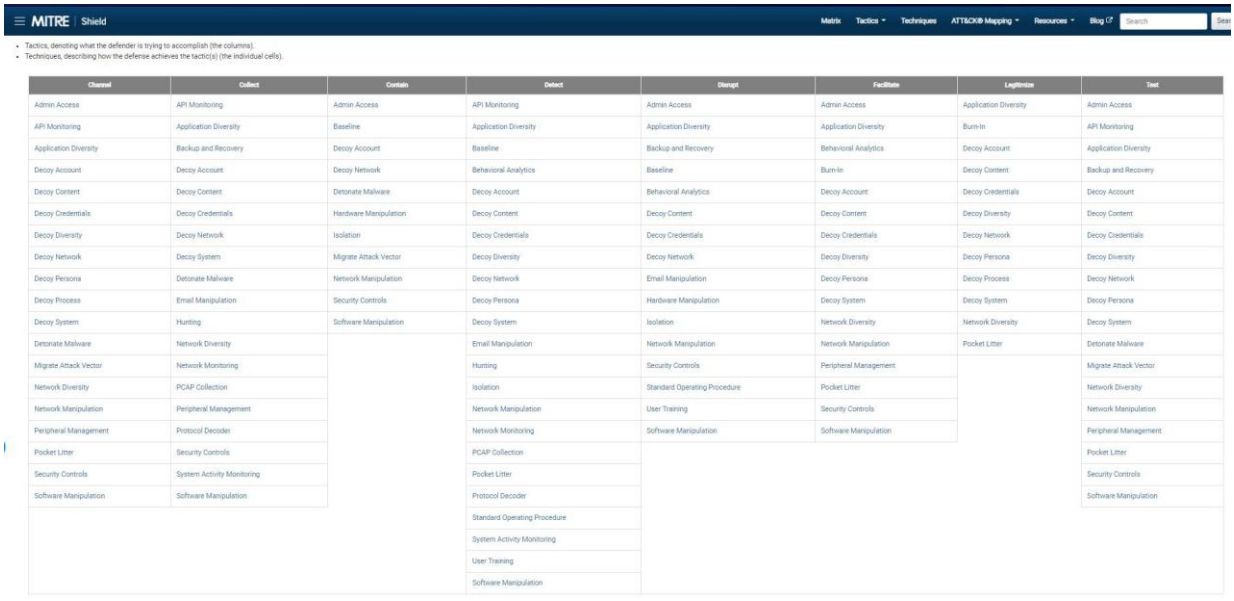


Figure 19 - Shield Active Defence Matrix

Extending on both MITRE ATT&CK and Shield, the MITRE's D3FEND framework provides a technical set of defensive countermeasures that complements the ATT&CK framework.

D3FEND 'illustrates the complex interplay between computer network architectures, threats, and cyber countermeasures… [enabling defenders to] tailor defences against specific cyber threats, thereby reducing a system's potential attack surface. As a result, D3FEND will drive more effective design, deployment, and defence of networked systems writ large' (NSA, 2021).

D3FEND includes an ontology, provided in json, owl and ttl formats. The ontology performs the role of translation between the offensive and defensive MITRE models as depicted in Figure 20 below.

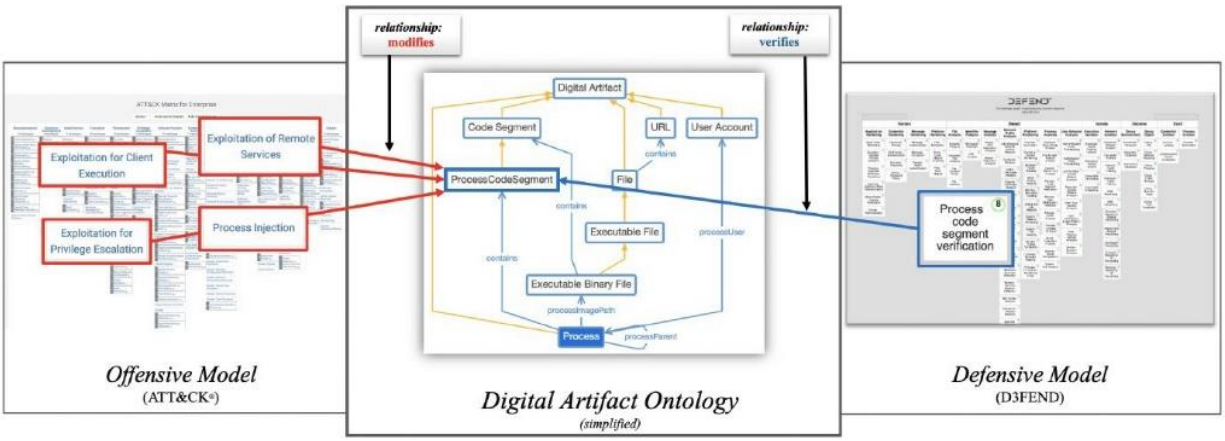


Figure 20 - Mapping via Inference Through the Digital Artifact Ontology (Kaloroumakis & Smith, 2021, p9)

MITRE is not the only repository of tools and frameworks to support cyber-security practitioners. The NIST Cybersecurity Framework consists of five functions, providing a model with sufficient depth to support the development of practical cyber-security solutions. The functions are (National Institute of Standards and Technology, 2018):

- Identify – Obtain situational awareness of cyber-security systems, people, assets, data and capabilities.
- Protect – Employ safeguards to limit or contain the impact of a potential cyber-security event.
- Detect – Identify the occurrence of cyber-security events.
- Respond – Take action to respond to a detected cyber-security incident.
- Recover – Undertake timely recovery to normal operations to reduce the impact from a cyber-security incident.

The NIST Functions decompose into categories, subcategories and references, with a wide variety of underlying data and models to support users. An example of this decomposition of information as part of the NIST Functions is provided in Figure 21 below.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 21 - NIST Framework for Improving Critical Infrastructure Cybersecurity (National Institute of Standards and Technology, 2018)

Advantages of the NIST Framework is commonality with a broad range of other frameworks, models and standards, including ISO 27001, as well as training material and supporting references. The NIST Cybersecurity Framework provides a means of managing security functions against corresponding security controls. However, it does not map these controls against the adversary TTPs directly.

The NIST Framework places a large focus on detection, response and recovery from the perspective of cyber-security controls. However, LEO systems do not appear to feature many controls aligned to these categories. Engineering and production activities generally focus on the identify and protect categories. However, response and recover functions provide recovery, and must be planned and resourced for the entire space system, from ground station networks through to SVs.

Detection, response and recovery is pertinent to the degree of supervisory control LEO system operations and security teams have over the constellation and networks. Adversaries can operate at any time of the day or night. Breakout times are a metric for adversary time to move laterally between hosts on a compromised network from their initial access. Breakout times average at just 4 hours and 37 minutes (Crowdstrike, 2021). Given that a ground station team is unlikely to have a persistent connection to all SVs in their constellation at all times (due to orbits), there are likely to be periods of time where an SV is essentially 'on its own' in space, or dependent on other nodes in the constellation for its communications. This offers an opportunity to adversaries, because operators are unlikely to detect attempts to gain control of the SV. In the event of an

attack, LEO space systems need to have a detection, response and recovery capability. Conducting threat hunt is difficult enough in a terrestrial environment. Undertaking a threat hunt across an LEO constellation would be extremely difficult without preparation. For example, the presence of cyber-defence-specific network taps and onboard detection capabilities able to perform rapid updates in the event of a detected threat should be seen as critical LEO SV constellation capabilities. Cloud-delivered ground stations and services potentially reduce the issue of poor connectivity coverage, but they bring their own risks and attack surface. These issues will be explored further in Part Two of this report, as enablers of the CY-JAR concept.

5.4 Threat Models

Threat modelling is a *'*strategic process aimed at considering possible attack scenarios and vulnerabilities within a proposed or existing application environment for the purpose of clearly identifying risk and impact levels' (UcedaVelez & Morana, 2015). A wide variety of threat modelling approaches and toolsets exist. This report does not seek to provide an exhaustive list, as other authors have already performed such analysis (Selin, 2019; N. Shevchenko, 2018; Nataliya Shevchenko, Chick, O'Riordan, Scanlon & Woody, 2018). However, to inform the reader and provide an understanding of the context of threat modelling, this report describes two of the more advanced techniques.

Threat Assessment and Remediation Analysis (TARA) is part of the MITRE Mission Assurance Engineering process, focused on assessing cyber-vulnerabilities and associated countermeasures. When supported by an appropriate crown jewels analysis and catalogue data, TARA allows engineers to evaluate and improve the security posture of systems during the acquisition and development process. TARA consists of three models (Wynn, 2014):

1. Cyber Threat Susceptibility Analysis (CTSA) – Develop cyber model of the system, followed by identification and ranking of attack vectors and risk assessment
2. Cyber Risk Remediation Analysis (CRRA) - Identify plausible mitigations and select countermeasures based on utility and cost; and
3. Knowledge Management (KM) – Develop catalogue content to support the CTSA and CRRA models. This model includes the prioritisation of information needs, identification and evaluation of data, and updates to the catalogue.

The TARA model relies on catalogued content. Where this exists and is appropriate, the model offers efficiencies. However, this may also be a limitation where applicable content does not exist.

The Process for Attack Simulation and Threat Analysis (PASTA) seeks to emulate threats and their means of conducting attacks, to improve the security posture of systems under analysis. The threat model imitates real TTPs and toolsets and develops test cases for detailed risk-based modelling, which are contextually useful for the system being defended. Mitigations and countermeasures are developed, focusing on the threats, TTPs and risks identified throughout the PASTA process (UcedaVelez & Morana, 2015). PASTA consists of seven stages depicted in Figure 22 below.

Stage	Description	Activities
1	**Definition of Objectives**	• Document business requirements. • Define security/compliance requirements. • Define the business impact. • Determine the risk profile.
2	**Definition of the Technical Scope**	• Enumerate software components. • Identify actors and data sinks/source • Enumerate system-level services. • Enumerate third party infrastructure. • Assert completeness of secure design.
3	**Application Decomposition and Analysis**	• Enumerate all application use cases. • Document data flow diagrams. • Security functional analysis and the use of trust boundaries.
4	**Threat Analysis**	• Analyse the overall threat scenario. • Gather threat information from internal threat sources. • Gather threat information from external threat sources. • Update the threat libraries. • Threat agents to assets mapping. • Assignment of the probablistic values for identified threats.
5	**Weakness and Vulnerability Analysis**	• Review/correlate existing vulnerabilities. • Identify weak design patterns in the architecture. • Map threats to vulnerabilities. • Provide context risk analysis based upon threat-vulnerability.
6	**Attack Modelling and Simulation**	• Analyse the attack scenarios. • Update the attack library/vectors and the control framework. • Identify the attack surface and enumerate the attack vectors. • Assess the probability and impact of each attack scenario. • Derive a set of cases to test existing countermeasures. • Conduct attack driven security tests and simulations.
7	**Risk Analysis and Management**	• Calculate the risk of each threat. • Identify countermeasures and risk mitigations measures. • Calculate the residual risks. • Recommend strategies to manage risks.

Figure 22 - PASTA Stages and Activities

The PASTA process is extensive. A variety of different models, tables and use cases are developed throughout the process to defend a system. A threat model stack is created, including threat motivations, targets, attack vectors, vulnerabilities and impacted assets. Impact is considered both in terms of technical and business affects. PASTA uses various methods to test for vulnerabilities, ranging from source code review to penetration testing. Various system mapping and categorisation systems are available to analysts. PASTA maps to the NIST SP-800 risk assessment process, as depicted in Figure 23 below.

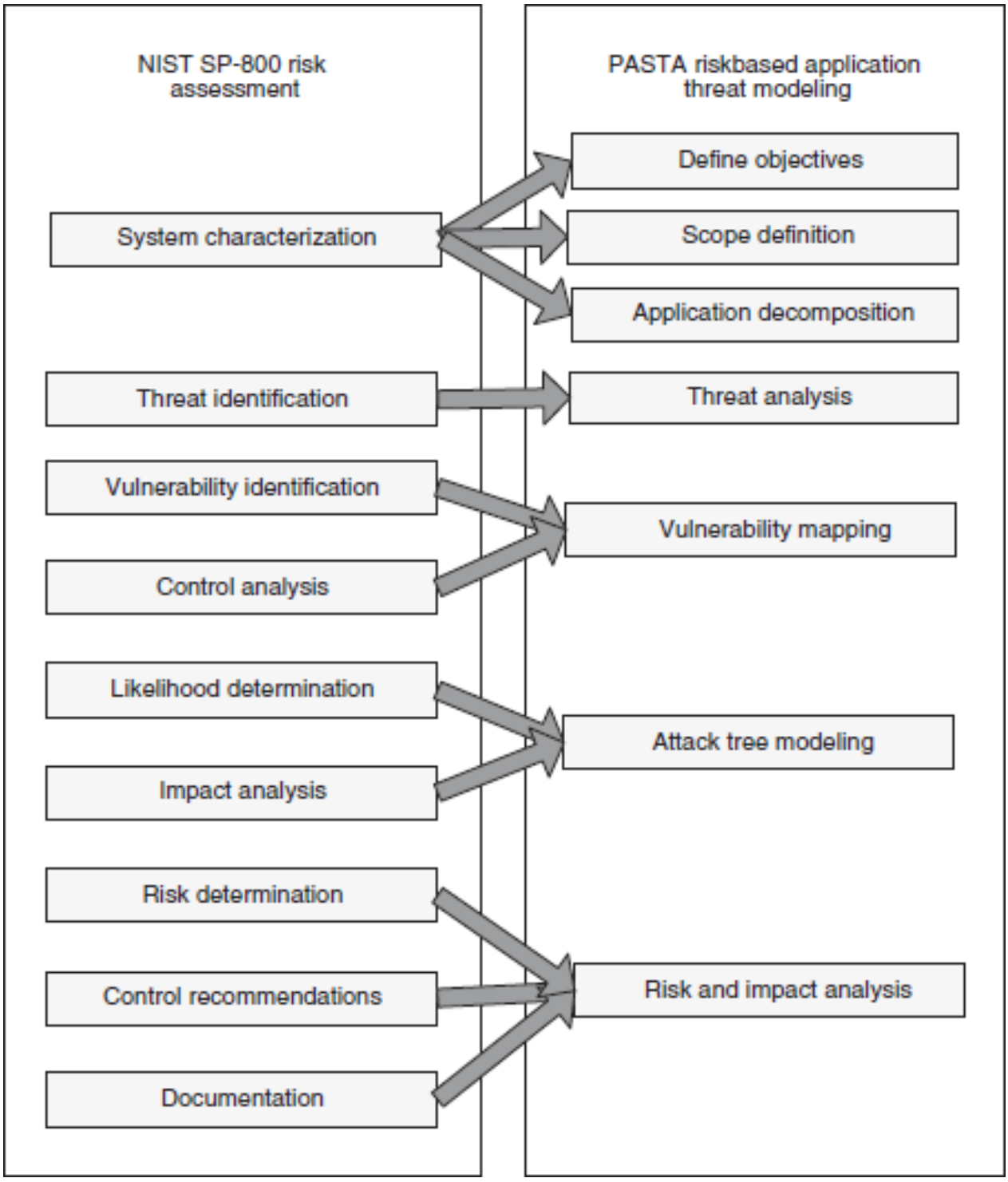


Figure 23 – NIST Risk Assessment to PASTA Mapping

A completed PASTA example of an attack tree, with countermeasures, is provided in Figure 24 below. This example demonstrates the tree commencing with the asset, which represents a target to the adversary, with the branching out use cases, threats, abuse cases, vulnerabilities, attack patterns, impacts and countermeasures.

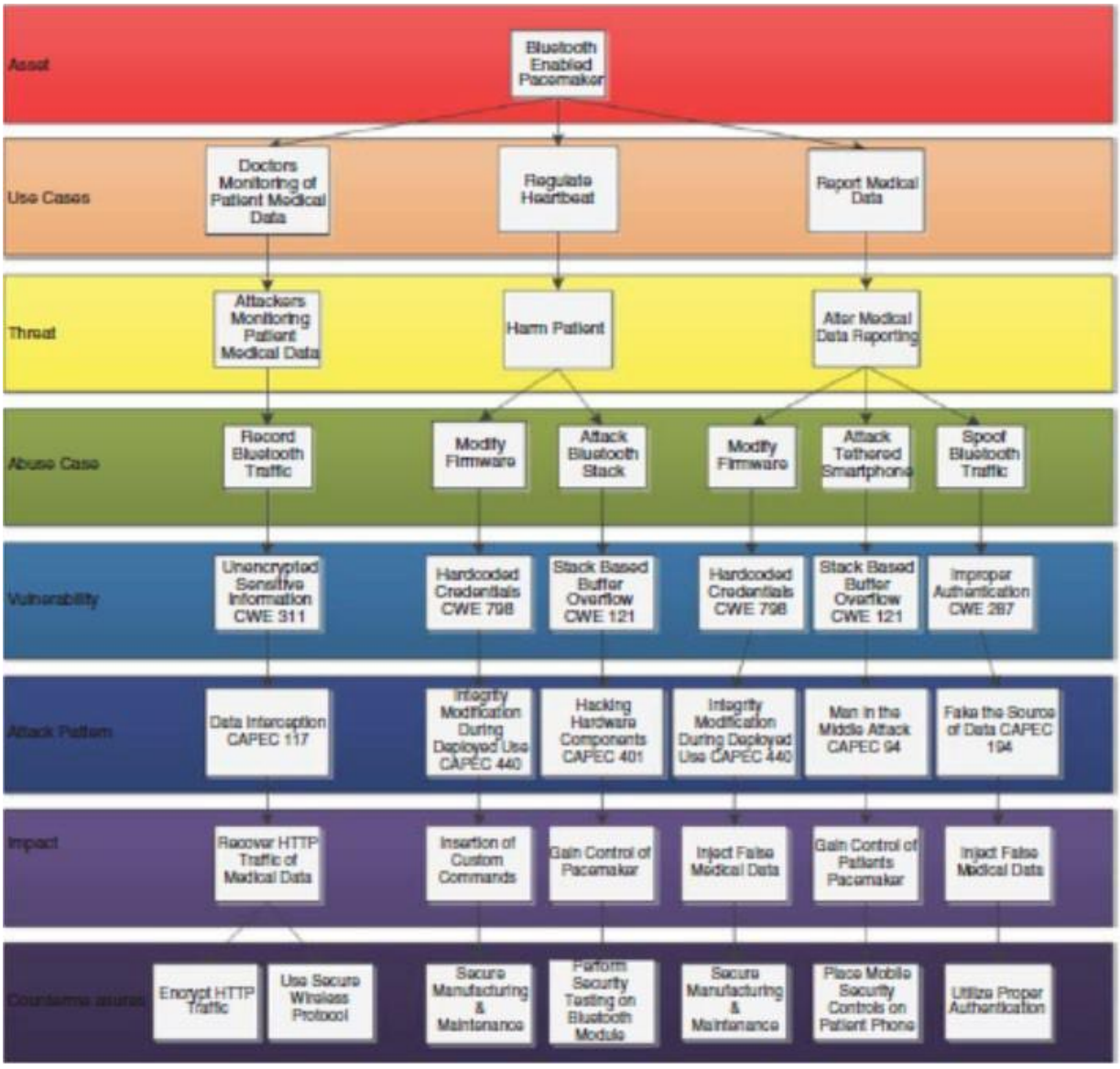


Figure 24 - PASTA Completed Attack Tree

Threat models such as TARA and PASTA provide a repeatable technique for mapping adversary behaviours to system functions and countermeasures. The use of a structured technique to support efficient and effective analysis of cyber-security risks against LEO space systems is critical, to enhance the quality of the risk assessment outcomes and increase resilience. The practical application of these techniques will be explored in more detail in Part Two of this report.

Conclusion

‘Secure encryption seems to be the most plausible response to cyberthreats to space assets, although it has its limits. Some security is better than no security – as long as the experts know what that security is capable of providing and what its limitations are. Part of the problem appears to be that neither the cyber community nor the space community understands the security requirements and vulnerabilities of each other’s domain’ (Livingstone & Lewis, 2016).

This report is the first of two parts commissioned by SmartSat CRC through the University of South Australia, seeking to enhance the state of the art in cyber-security solutions for LEO space systems. The aim of this two-part series is to establish a Cyber-Jeopardy and Response (CY-JAR) Concept for ongoing development and subsequent deployment into the LEO space operational environment. The EDT is a first conceptual step in developing an advanced CY-JAR capability.

This first part of the report has provided an overview and analysis of the body of knowledge pertaining to the concept of the evil twin, and the supporting concepts of mission assurance, resilience, risk, and cyber-worthiness as a means of enhancing the security posture of LEO systems. This report outlines a variety of frameworks, models and approaches pertaining to cyber-security, to inform long-term sovereign Australian satellite cyber-security, digital twin modelling and simulation capability.

The Evil Digital Twin Methodology

The author has formulated an approach using the frameworks, models, tools and processes described throughout this report. The EDTM is proposed below, across twenty steps.

1. Collect intelligence.
The collection of intelligence involves the development of a collection plan, with formalised collection methods and procedures to protect both the intelligence team and the integrity of the data collected. Intelligence sharing arrangements and tools should be agreed, including external data sources and internal procedures. Intelligence gaps should be identified for further development. Intelligence collection should include threat and friendly data relevant to securing the LEO systems. Priority Intelligence Requirements should be developed, sorted, catalogued and answered. Continuous intelligence collection approaches should be established based on the lifecycle of both threats and defended systems.

2. Develop a Threat Library.
Conduct an Adversary Threat Assessment and develop a Threat Library of all threat actors of interest with information available through threat reporting, including tool sets and malware employed that could be a significant threat to any component of the space system.

3. Develop a Threat TTP Matrix.
Using the MITRE ATT&CK Framework and other adversary behaviour models, build a Threat TTP Matrix. Undertake further research on TTPs within the matrix.

4. Collect architectural and system information of space systems and assets.

Develop a clear and consistent view of the system architecture, and a bill of materials pertaining to software and hardware. Document relevant protocols and networking connections.

5. Build a Digital Twin.
Develop a digital twin using simulation systems and/or a replication of the satellite systems, with a methodology to support testing, data collection, data storage and Verification, Validation and Accreditation (VV&A) as appropriate.

6. Develop vulnerability models for all space systems including:
- LEO SVs
- LEO constellation
- Space system (ground station, terrestrial network); and
- Users, roles, and identity management.

7. Conduct Threat Modelling.
Undertake threat modelling using shared toolsets, to ensure consistency and coverage of agreed threats and vulnerabilities. Align vulnerabilities with system assets and architecture. Confirm overlap of Threat TTPs with vulnerable systems.

8. Record a Baseline.
Using the digital twin, understand what is considered 'normal' (or expected) behaviour and build models of the system under various operational conditions where a cyber-attack is not occurring. This will support future testing as well as the detection of unusual behaviour.

9. Develop an Initial Mission Resilience Sub-System Crosswalk.
Conduct a crosswalk of each sub-system against the MITRE Mission Resilience Engineering framework, to determine both defence-in-depth and defence-in-breadth coverage at a sub-system level.

10. Develop a Crown Jewels and Mission Assessment.
Undertake a crown jewels assessment and map mission-essential functions and systems to support prioritisation.

11. Conduct Impact Analysis.
Determine the impact of specific adversarial targets if they are achieved. Map prior threat modelling and crown jewels assessment results to likely adversary targets and threat surface. Utilise this mapping to review high-value vulnerabilities, entry and egress points into and out of major systems, lateral movement paths, adversary countermeasures to security controls, and likely points for privilege escalation to support TTPs.

12. Conduct security testing using the Digital Twin.
Undertake hands-on penetration testing and experimentation with the digital twin to test assumptions and confirm TTPs.

13. Conduct Countermeasure Research and Analysis.
Develop additional security controls and mitigations, including resilience and recovery measures as required, to enhance the overall security of the LEO space system. Maintain a focus on mission assurance capabilities and hardening of systems. Ensure an understanding of impact on system functionality is considered; security can reduce usability.

14. Conduct Desktop Quantitative Resilience Assessment.

Undertake a desktop quantitative resilience assessment to confirm the desired changes to the system value-add, and contribute to the overall resilience of the LEO space system.

15. Undertake a Cyber-worthiness Design Principles Review.
Conduct a cyber-worthiness design principles review using the following points (Ormrod, Slay, & Ormrod, 2021):

- Identify the crown jewels – protect the mission and dependent services
- Fail safe and gracefully - default to a secure state with alerts
- Avoid security through obscurity – embrace open design principles;Implement Role Based Authentication Controls (RBAC) – separate duties
- Provide minimum privilege by default – make escalation hard for the attacker
- Reduce the attack surface - identify vulnerabilities early
- Harden architecture - layer security controls
- Provide incident response capabilities – aligned to predicted adversary profiles
- Embed resilient systems and practices - the spacecraft must be its own root of recovery; and
- Identify and protect the weakest links in the security system – prioritise risks and controls.

16. Improve and update the system.
Iterate back through the system architecture, design and digital twin setup to enhance security using identified countermeasures. Review any impact on system effectiveness and efficiency. Update and enhance the security of the system. Review documentation and golden images. Refresh security documentation and assessments developed to date, including threat models.

17. Conduct security testing using Digital Twin.
Undertake another hands-on penetration test and experiment with the digital twin to test assumptions and confirm the effectiveness of the new controls.

18. Record a new Baseline.
Using the digital twin, understand what is considered ‘normal’ behaviour and build models of the system under various operational conditions where a cyber-attack is not occurring. This will support future testing as well as the detection of unusual behaviour.

19. Undertake Risk Governance Review.
Provide senior management with a full risk assessment and document residual risks for governance review and endorsement.

20. Iterate.
Continuously undertake the process, beginning from intelligence collection (1) through to governance review (19). Just as the adversary evolves, the security controls employed on LEO space systems must keep up with the threats and not be allowed to languish.

The Evil Digital Twin Methodology (EDTM) is a hybrid method, built upon the literature and key concepts presented within this report. The EDTM will be used in Part Two of this report, which will seek to conduct a proof-of-concept activity to secure a generic model of a LEO space system, to test assumptions. In addition, Part Two will provide a worked example of a cybersecurity solution, using a generic model and proof of concept LEO space system, as a precursor to the CY-JAR concept.

References

Abbany, Z. (2018). SpaceX's Starlink satellite internet: It's time for tough talk on cyber security in space. Retrieved from https://www.dw.com/en/spacexs-starlink-satellite- internet-its-time-for-tough-talk-on-cyber-security-in-space/a-42678704

ASRG. (2021). Automotive Security Research Group. Retrieved from https://www.asrg.io/

Australian National Audit Office. (2021). *Cyber Security Strategies of Non-Corporate Commonwealth Entities*. Canberra, ACT.: Commonwealth of Australia, Retrieved from https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities

Australian Space Agency. (2019). *Advancing Space: Australian Civil Space Strategy 2019 – 2028*. Canberra: Commonwealth of Australia, Retrieved from https://publications.industry.gov.au/publications/advancing-space-australian-civil- space-strategy-2019-2028.pdf

AWS. (2020). AWS Ground Station. Retrieved from https://aws.amazon.com/ground-station/ Bardin, J. (2013). Chapter 89 - Satellite Cyber Attack Search and Destroy. In *Computer and Information Security Handbook (Third Edition)* (pp. 1173–1181).

Barrett, M. (2019). The Air Force Will Let Hackers Try to Hijack an Orbiting Satellite. Retrieved from https://www.wired.com/story/air-force-defcon-satellite-hacking/

Bodeau, D., & Graubart, R. (2016). *Cyber prep 2.0: Motivating organizational cyber strategies in terms of threat preparedness*. Retrieved from

Bodeau, D., Graubart, R., McQuaid, R., & Woodill, J. (2018). Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods (MTR 180314). *The MITRE Corporation, Bedford, MA*.

Bratvold, R. B., Thomas, P., & Bickel, J. E. (2014). The Risk of Using Risk Matrices. *SPE economics & management, 6*(2), 056-066. doi:10.2118/166269-PA

Burch, R. (2013). A Method for Calculation of the Resilience of a Space System. In (pp. 1002-1007): IEEE.

Burch, R. W. (2019). *Resilient space systems design : an introduction*. [S.l.]: S.l. : CRC PRESS.

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. Retrieved from

Carlo, A., & Veazoglou, N. (2020). *ASAT Weapons: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era*. Paper presented at the Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).

Center for Threat Informed Defense. (2021). ATT&CK Workbench Frontend. Retrieved from https://github.com/center-for-threat-informed-defense/attack-workbench-frontend

Cheng, J., & Harrington, R. (2017). 12 of the smartest things Elon Musk has said about the future of our planet. *Business Insider Australia.* Retrieved from https://www.businessinsider.com.au/elon-musk-future-quotes-2017-3?r=US&IR=T

Command, U. A. F. S. (2009). The United States Air Force Blueprint for Cyberspace. *Colorado Springs, CO*.

Commonwealth of Australia. (2009). *ADDP 3.14 Targeting*. Commonwealth of Australia, Retrieved from http://www.defence.gov.au/foi/docs/disclosures/021_1112_Document_ADDP_3_14_Targeting.pdf

Commonwealth of Australia. (2012). Defence Capability Development Handbook 2012. Retrieved from https://www.defence.gov.au/publications/DefenceCapabilityDevelopmentHandbook2012.pdf

Computer Incident Response Center. (2021). MISP Project - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. Retrieved from https://www.misp-project.org/
Corey, J. S. (2013). *Abaddon's Gate*: Orbit.
Council of Financial Regulators. (2020). Cyber Operational Resilience Intelligence-led Exercises (CORIE) - Pilot Program Guideline v1.1. Retrieved from https://www.cfr.gov.au/publications/policy-statements-and-other-reports/2020/corie- pilot-program-guideline/pdf/corie-framework-guideline.pdf
Crowdstrike. (2021). The Myth of Part-time Hunting, Part 1: The Race Against Ever- diminishing Breakout Times. Retrieved from https://www.crowdstrike.com/blog/the- myth-of-part-time-threat-hunting-part-1/
Crown. (2019). *Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts v2.0*.
Cybrary. (2021). MITRE ATT&CK Defender (MAD) ATT&CK Cyber Threat Intelligence Certification Training. Retrieved from https://www.cybrary.it/course/mitre-attack- defender-mad-attack-for-cyber-threat-intelligence/
Defence Science and Technology Group. (2020). Star Shots - Resilient Multi-Mission Space.
Retrieved from https://www.dst.defence.gov.au/strategy/star-shots/resilient-multi- mission-space
Dreyer, P., Langeland, K. S., Manheim, D., McLeod, G., & Nacouzi, G. (2016). *RAPAPORT (Resilience Assessment Process and Portfolio Option Reporting Tool): Background and Method*. Retrieved from
Drimer, S. (2009). Security for volatile FPGAs. Retrieved from https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-763.pdf
Drozhzhin, A. (2020). Russian-speaking cyber spies exploit satellites. *Kaspersky Daily*. Retrieved from https://www.kaspersky.com.au/blog/turla-apt-exploiting- satellites/9771/
Duczynski, G. (2004). *Effects-Based Operations: A Guide for Practitioners*. Retrieved from https://www.hsdl.org/?view&did=454767
Economic and Security Review Commission. (2011). Report to Congress of the US-China Economic and Security Review Commission. Retrieved from https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf
Ellis, C. (2021). The Bar Fight Risk Taxonomy. 27 June 2021,. Retrieved from https://cje.io/2021/06/27/the-bar-fight-risk-taxonomy/
European Cooperation for Space Standardisation. (2013). Software engineering handbook. ECSS-E-HB-40A. Retrieved from https://ecss.nl/hbstms/ecss-e-hb-40a-software-engineering-handbook-11-december-2013/
European Cooperation for Space Standardisation. (2014). SpaceWire Standard Revision Draft D Issue 1.0. ECSS-E-ST-50-12CRev1. Retrieved from http://spacewire.esa.int/WG/SpaceWire/SpW-WG-Mtg22-SupportDocuments/ECSS- E-ST-50-12C-Rev1%20Draft%20D%20v0.3.pdf
European Space Agency. (2005). Galileo service volume simulator available for download. Retrieved from https://www.esa.int/Applications/Navigation/Galileo_service_volume_simulator_available_for_download
European Space Agency. (2020a). CSCE - Cyber Security Centre of Excellence and supporting technologies. *Telecom Artes 4.0 Programme,.* Retrieved from https://artes.esa.int/projects/csce
European Space Agency. (2020b, 30 Mar 2020). Types of orbits. Retrieved from https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits#LEO
Falco, G. (2018). *The vacuum of space cybersecurity*.
Federal Communications Commission. (2021). *In the Matter of Space Exploration Holdings, LLC Request for Modification of the Authorization for the SpaceX NGSO Satellite System* Washington, D.C.: Federal Communications Commission, Retrieved from https://docs.fcc.gov/public/attachments/FCC-21-48A1.pdf

Foreseeti. (2020). Selecting High Value Assets. Retrieved from https://docs.foreseeti.com/docs/selecting-high-value-assets
Foust, J. (2018). “No encryption, no fly” rule proposed for smallsats. Retrieved from https://spacenews.com/no-encryption-no-fly-rule-proposed-for-smallsats/
Fowler, S., & Sitnikova, E. (2019). *Toward a framework for assessing the cyberworthiness of complex mission critical systems* IEEE.
Gilmore Space. (2021). Gilmore Space Technologies. Retrieved from https://www.gspacetech.com/
Goffin, M. (2020). Introducing MITRE Shield Adversary Group Mappings. Retrieved from https://medium.com/mitre-shield/introducing-mitre-shield-adversary-group-mappings-b1e095381dae
Hallex, M. A., & Cottom, T. S. (2020). Proliferated Commercial Satellite Constellations - Implications for National Security. *JFQ 97, 2nd Quarter 2020*.
Harrison, T., Johnson, K., Roberts, T. G., Way, T., & Young, M. (2020). *Space threat assessment 2020*: Center for Strategic and International Studies (CSIS).
Hays, S. Takeaways from Special Senate Hearing on CMMC and DIB Cybersecurity. Retrieved from https://info.summit7systems.com/blog/cmmc-senate-hearing?hs_amp=true
Hubbard, D., & Evans, D. (2010). Problems with scoring methods and ordinal scales in risk assessment. *IBM Journal of Research and Development, 54*(3), 2:1-2:10. doi:10.1147/JRD.2010.2042914
Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Hoboken, New Jersey: Hoboken, New Jersey : Wiley.
Hussein, M., & Hanani, A. (2016). Routing in IP / LEO Satellite Communication Systems : Past , Present and Future. Retrieved from https://fada.birzeit.edu/bitstream/20.500.11889/4353/1/2-5icssc_2016.pdf
International Standards Organisation. (2018). ISO 31000: Risk Management - Guidelines.
International Standards Organisation. (2021). ISO/CD 24089 - Road vehicles — Software update engineering. Retrieved from https://www.iso.org/standard/77796.html
ISACA. (2019). COBIT 2019 Introduction and Methodology. Retrieved from https://www.isaca.org/resources/cobit
Jakobson, G. (2013). *Mission-centricity in cyber security: Architecting cyber attack resilient missions*. Paper presented at the International Conference on Cyber Conflict, CYCON, Estonia, Tallinn.
Jung, W., & Vasen, T. (2021). Responsive Space for NATO Operations. Retrieved from https://www.japcc.org/responsive-space-for-nato-operations/
Kahlen, F. J., Flumerfelt, S., & Alves, A. (2016). Transdisciplinary perspectives on complex systems: New findings and approaches.
Kang, M. (2018). Mitigation of cyber warfare in space through reed solomon codes. *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018,*.
Katona, Z. (2020). A flexible LEO satellite modem with Ka-band RF frontend for a data relay satellite system. *International Journal of Satellite Communications and Networking*.
Kott, A., & Linkov, I. (2018). *Cyber Resilience of Systems and Networks*. Cham, SWITZERLAND: Springer International Publishing AG.
Kramer, M. (2007). *Knowing Thy Enemy: Decisionmaking of Regional Adversaries.* Paper presented at the Seventh Annual Herzliya Conference Washington D.C.
LeoLabs Inc. (2021). Low Earth Orbit Visualization. *LeoLabs Platform for Operators and Developers.* Retrieved from https://platform.leolabs.space/visualization
Lessig, L. (1996). Reading the constitution in cyberspace. *Emory LJ, 45*, 869.
Lessig, L. (2002). *The Future of Ideas: The Fate of the Commons in a Connected World. Random House. New York. USA.*
Lewis, P., & Unal, B. (2019). The Destabilizing Danger of Cyberattacks on Missile Systems. Retrieved from https://www.chathamhouse.org/2019/07/destabilizing-danger-cyberattacks-missile-systems
Livingstone, D., & Lewis, P. (2016). *Space, the Final Frontier for Cybersecurity?* : Chatham House. The Royal Institute of International Affairs.

Lockheed Martin. (2015). Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
Mann, A. (2021). Starlink: SpaceX's satellite internet project. Retrieved from https://www.space.com/spacex-starlink-satellites.html
Marc, A. (2011). Why Software Is Eating The World. *The Wall Street journal. Eastern edition*.
McDowell, J. (2021). Jonathan's Space Pages - Starlink Statistics. Retrieved from https://planet4589.org/space/stats/star/starstats.html
McLeod, G., Nacouzi, G., Dreyer, P., Eisman, M., Hura, M., Langeland, K. S., . . . Torrington, G. (2016). *Enhancing Space Resilience Through Non-Materiel Means*: RAND Corporation.
Microsoft. (2020). Azure Orbital Retrieved from https://azure.microsoft.com/en- au/services/orbital/
Miessler, D. (2021). Explaining Threats, Threat Actors, Vulnerabilities, and Risk Using a Real-World Scenario: Exploring an analogy used to explain security concepts. 03 May 2021,. Retrieved from https://danielmiessler.com/blog/explaining-threats-threat- actors-vulnerabilities-and-risk-using-a-real-world-scenario/
Ministry of Defence. (2013). Red teaming guide 2nd Ed.
MITRE. (2014). Systems Engineering Guide. Retrieved from https://www.mitre.org/publications/technical-papers/the-mitre-systems-engineering- guide
MITRE. (2021a). ATLAS - Adversarial Threat Landscape for Artificial-Intelligence Systems. Retrieved from https://github.com/mitre/advmlthreatmatrix
MITRE. (2021b). CAPEC - Common Attack pattern Enumeration and Classification. Retrieved from https://capec.mitre.org/about/attack_comparison.html
MITRE. (2021c). Cyber Threat Intelligence Repository of MITRE ATT&CK® and CAPEC catalogs expressed in STIX 2.0 JSON. Retrieved from https://github.com/mitre/cti
MITRE. (2021d). MITRE ATT&CK Matrix. Retrieved from https://attack.mitre.org/ MITRE. (2021e). MITRE ATT&CK Navigator v4.3. Retrieved from https://mitre-attack.github.io/attack-navigator/
MITRE. (2021f). MITRE Shield. Retrieved from https://shield.mitre.org/
MITRE Corporation. (2014). The MITRE Systems Engineering Guide. Retrieved from https://www.mitre.org/publications/technical-papers/the-mitre-systems-engineering- guide
Moller, B., Gray, T., Kay, S., Kisdi, A., Buckley, K., & Delfa, J. (2019). Experiences from the SISO SpaceFOM at the European Space Agency.
Musman, S., Tanner, M., Temin, A., Elsaesser, E., & Loren, L. (2011). *A systems engineering approach for crown jewels estimation and mission assurance decision making*. Paper presented at the 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), .
NASA. (2019a). Explore - NASA Small Spacecraft Strategic Plan. Retrieved from https://www.nasa.gov/sites/default/files/atoms/files/smallsatstrategicplan.pdf
NASA. (2019b). LEGEND : 3D/OD Evolutionary Model. *Astromaterials Research & Exploration Science Orbital Debris Program Office,*. Retrieved from https://orbitaldebris.jsc.nasa.gov/modeling/legend.html
NASA. (2020). State of the Art of Small Spacecraft Technology. Retrieved from https://www.nasa.gov/smallsat-institute/sst-soa-2020
NASA. (2021a). NASA Open Source Software. Retrieved from https://code.nasa.gov/ NASA. (2021b). Small Spacecraft Virtual Institute. Retrieved from https://www.nasa.gov/smallsat-institute/space-mission-design-tools
National Defense Industrial Association. (2008). National Defense Industrial Association Engineering for System Assurance v1.0. Retrieved from http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf
National Institute of Standards and Technology. (2012). *NIST Special Publication 800-30: Guide for Conducting Risk Assessments*. National Institute of Standards and Technology,
National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity v1.1. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Noel, S. (2015). CyGraph: Cybersecurity Situational Awareness That's More Scalable, Flexible & Comprehensive. Retrieved from https://neo4j.com/blog/cygraph- cybersecurity-situational-awareness/
NSA. (2021). NSA Funds Development, Release of D3FEND. Retrieved from https://www.nsa.gov/news-features/press-room/Article/2665993/nsa-funds- development-release-of-d3fend/
O'Sullivan, K., & Turnbull, B. (2015). The cyber simulation terrain: Towards an open source cyber effects simulation ontology.
Office of the Assistant Secretary of Defense for Homeland Defense & Global Security. (2015). *Space Domain Mission Assurance: A Resilience Taxonomy : a White Paper*: Office of the Assistant Secretary of Defense for Homeland Defense & Global Security.
Office of the Director of National Intelligence. (2021). Annual Threat Assessment of the US Intelligence Community. Retrieved from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
openXSAM. (2021). An OPEN format for eXchanging Security Analysis Models. Retrieved from https://openxsam.io/
Ormrod, D., Slay, J., & Ormrod, A. (2021). *Cyber-Worthiness and Cyber-Resilience to Secure Low Earth Orbit Satellites.* Paper presented at the ICCWS 2021 16th International Conference on Cyber Warfare and Security.
Ormrod, D., & Turnbull, B. (2016). The cyber conceptual framework for developing military doctrine. *Defence studies, 16*(3), 270-298. doi:10.1080/14702436.2016.1187568
Pavur, J. (2020). Whispers Among the Stars Perpetrating (and Preventing) Satellite Eavesdropping Attacks. Retrieved from https://www.blackhat.com/us-20/briefings/schedule/index.html#whispers-among-the-stars-a-practical-look-at-perpetrating-and-preventing-satellite-eavesdropping-attacks-19391
Pavur, J., & Martinovic, I. (2020). SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research.
Pawlikowski, E., Loverro, D., & Cristler, T. (2013). *Resiliency and Disaggregated Space Architectures*. Retrieved from
Planet. (2021). GitHub - OpenLST/openlst Retrieved from https://github.com/OpenLST/openlst
Pollino, C. A., & Henderson, C. (2010). Bayesian networks: A guide for their application in natural resource management and policy. *Landscape Logic, Technical Report, 14*.
RedHat. (2021). What is DevSecOps? Retrieved from https://www.redhat.com/en/topics/devops/what-is-devsecops
Reidenberg, J. R. (1997). Lex informatica: The formulation of information policy rules through technology. *Tex. L. Rev., 76*, 553.
Rocket Labs. (2020). Rocket Labs USA. Retrieved from https://www.rocketlabusa.com/missions/completed-missions/
RocketLab. (2020). Launch: Payload Users Guide. Version 6.5. Retrieved from https://www.rocketlabusa.com/assets/Uploads/Rocket-Lab-Launch-Payload-Users- Guide-6.5.pdf
Romanych, M. (2005). Operationalizing OPSEC. *IO Sphere, Summer 2005*. Retrieved from http://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C2_Operationalizing_OPSEC.pdf
SAE International. (2016). Cybersecurity Guidebook for Cyber-Physical Vehicle Systems *J3061_201601.* Retrieved from https://www.sae.org/standards/content/j3061_201601/ Santamarta, R. (2014). SATCOM terminals: Hacking by air, sea, and land.
Sebestyen, G., Fujikawa, S., Galassi, N., & Chuchra, A. (2018). Spacecraft Software. In *Low Earth Orbit Satellite Design* (pp. 115-125). Cham: Springer International Publishing.
Selin, J. (2019). Evaluation of threat modeling methodologies.
Shaw, J. (2019). Air Force: SSA is no more; it's 'Space Domain Awareness. Retrieved from https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness/
Sheftick, G. (2020). Army looks to leverage 'low Earth orbit' satellites. Retrieved from

https://www.army.mil/article/233587/army_looks_to_leverage_low_earth_orbit_satellit es
Shevchenko, N. (2018). Threat Modeling: 12 Available Methods. Retrieved from https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/
Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat modeling: a summary of available methods*. Retrieved from
Sidorenko, A. (2021). The most amazing risk management interview... ever... *LinkedIn.* 28 June 2021. Retrieved from https://www.linkedin.com/pulse/most-amazing-risk- management-interview-ever-alexei-sidorenko-crmp-1f/
Snyder, D., Hart, G. E., Lynch, K. F., & Drew, J. G. (2015). *Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems: Guidance for Where to Focus Mitigation Efforts*: RAND Corporation.
South Australian Auditor-Generals Department. (2021). *ICT vulnerability management in South Australian public sector entities*. Adelaide, SA.: South Australian Government, Retrieved from https://www.audit.sa.gov.au/Portals/0/Documents/Audit%20Reports/2020-21/Other/Report%2010%20of%202021%20-%20ICT%20vulnerability%20management%20in%20South%20Australian%20public%20sector%20entities.pdf
Southern Launch. (2021). Southern Launch. Retrieved from https://southernlaunch.space/about
Space ISAC. (2021). Space ISAC - Information Sharing and Analysis Center. Retrieved from https://s-isac.org/
Theohary, C. (2020). Defense Primer: Cyberspace Operations. *Congressional Research Service, 15 Dec 2020*. Retrieved from https://fas.org/sgp/crs/natsec/IF10537.pdf
Tordable, J. (2021). Doubling Down On Insights With Digital Twins. *Forbes.* Retrieved from https://www.forbes.com/sites/googlecloud/2021/06/25/doubling-down-on-insights- with-digital-twins/?sh=199bbaf82ced
UcedaVelez, T., & Morana, M. M. (2015). *Risk centric threat modeling*: Wiley Online Library. Unal, B. (2019). Cybersecurity of NATO's Space-based Strategic Assets. *Chatham House,*.
Retrieved from https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf
Underwood, K. (2021). ISAC Ventures Into Space Information Sharing. Retrieved from https://www.afcea.org/content/isac-ventures-space-information-sharing
United Nations. (2021). Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. *Addendum 154 – UN Regulation No. 155,*(22 January 2021). Retrieved from https://unece.org/sites/default/files/2021-03/R155e.pdf
University of Foreign Military and Cultural Studies. (2019). *The Red Team Handbook* United States Army, Retrieved from https://community.apan.org/wg/tradoc-g2/ufmcs-red- team-central/m/red-team-handbook/276147/download
US Department of Defense. (2011). FACT SHEET: Resilience of Space Capabilities. Retrieved from https://archive.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf
US Department of Defense. (2020). Defense Space Strategy Factsheet. Retrieved from https://media.defense.gov/2020/Jun/17/2002317392/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_FACTSHEET.PDF
US DoD. (2020). JP3-14 Space Operations. Retrieved from https://fas.org/irp/doddir/dod/jp3_14.pdf
US Whitehouse. (2020). Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems. Retrieved from https://www.whitehouse.gov/presidential-actions/memorandum-space-policy- directive-5-cybersecurity-principles-space-systems/
Vasen , T. (2021). *Resiliency in Space as a Combined Challenge for NATO*. Kalkar, Germany.: NATO
Vaughn Jr, R. B., Henning, R., & Siraj, A. (2003). *Information assurance measures and metrics-state of practice and proposed taxonomy.* Paper presented at the System Sciences,

2003. Proceedings of the 36th Annual Hawaii International Conference on.
Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*: Harvard Business Press.
Westerman, G., & Hunter, R. (2007). *IT risk: turning business threats into competitive advantage*: Harvard Business School Press Boston.
World Economic Forum. (2021). *Principles for Board Governance of Cyber Risk*. Geneva, Switzerland
Wynn, J. (2014). *Threat assessment and remediation analysis (tara)*. Retrieved from Yang, X. (2018). Low Earth Orbit (LEO) Mega Constellations – Satellite and Terrestrial
Integrated Communication Networks. Retrieved from http://epubs.surrey.ac.uk/850382/1/Xin Yang - PhD Thesis.pdf

USER INFORMED INDUSTRY DRIVEN RESEARCH POWERED

SMARTSAT
COOPERATIVE RESEARCH CENTRE

Building Australia's Space Industry

Australian Government
Department of Industry, Science, Energy and Resources

AusIndustry
Cooperative Research Centres Program

SmartSat CRC Head Office:
Lot Fourteen, Level 3, McEwin Building
North Terrace, Adelaide, SA

info@smartsatcrc.com
smartsatcrc.com