SMARTSAT
COOPERATIVE RESEARCH CENTRE

TECHNICAL REPORT 08

Satellite Cyber Resilience Whitepaper

Satellite Cyber Resilience Whitepaper

April 2022

ISBN:

This report should be cited as:
SmartSat 2022, Satellite Cyber Resilience Whitepaper, 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 Jordan Plotnek and Professor Jill Slay towards the authorship of this whitepaper.

Executive Summary

Contemporary cyber-attacks are increasing in frequency and sophistication with growing impacts such as large-scale privacy breaches, theft of intellectual property (IP), significant financial losses for businesses, and reputational damage. Cyber exploits can range from simplistic and opportunistic phishing campaigns to complex, covert and persistent attacks over time involving malicious actors with access to highly-skilled teams of hackers and advanced tools and resources.

The rapid commercialisation of space, and increased ease and lowering costs associated with launching satellites into space, has resulted in global supply chains of privatised satellite networks for commercial and military purposes. The Internet of Things (IoT) and associated connectivity with satellite networks has also created numerous vulnerabilities, which raises questions of how contemporary cyber-attacks could potentially impact satellites and the space security domain.

This whitepaper presents a novel Satellite Cyber Resilience Taxonomy derived from related contemporary space security and cyber-resilience literature. A taxonomy-guided research roadmap for SmartSat CRC is then proposed based on the identified literature gaps. The proposed research roadmap is based on four key satellite sub-systems: radio-link security; space hardware security; ground station security; and operations security, which are then further segmented and discussed according to the satellite resilience taxonomy.

Aims, Objectives & Impacts

The key aim of this whitepaper is to provide a literature review and research roadmap for satellite cyber-security resilience, to scope a SmartSat CRC research agenda and meet Commonwealth Milestones 1.3, 2.2 and 3.1.

Objectives for this whitepaper are:

- Identification of any previous research and development (R&D) activities that have been conducted in cyber-security and resilience of satellites
- Critical research review of most appropriate research agenda and outcomes to meet Commonwealth milestones
- Development of taxonomy for Satellite Cyber Resilience, including an understanding of Disaggregation, Distribution, Diversification, Deception, Protection and Proliferation; and
- Determination of a suitable technical framework, within which satellite cybersecurity and resilience research may be carried out.

Impacts that this whitepaper may have include:

- Improved understanding of cyber-security and resilience in a satellite context
- A common cyber-security taxonomy for CRC usage
- A technical research agenda in cyber-security and resilience for the CRC
- Contribution to the wider Australian space sector; and
- Enhancing CRC reputation in capabilities related to satellite cyber-security and resilience.

Table of Contents

1. Introduction

Contemporary cyber-attacks are increasing in frequency and sophistication, with growing impacts such as large-scale privacy breaches, theft of intellectual property (IP), significant financial losses for businesses, and reputational damage. Current attack vectors and attacker techniques are revealing trends and issues associated with cyber weaponry used by threat actors in contemporary breaches. Numerous reports and surveys from the Australian Cyber Security Centre (ACSC) and private companies, such as Cisco and Trustwave, have identified a multitude of malware trends and current issues, including ransomware crypto-worms, Advanced Persistent Threats (APT), Supply Chain Vulnerabilities (SCV), Distributed Denial of Service (DDoS) attacks, insider threat, trojans, and Internet of Things (IoT) botnets.

Cyber exploits can range from simplistic and opportunistic phishing campaigns to complex, covert and persistent attacks over time involving malicious actors with access to highly-skilled teams of hackers and advanced tools and resources. Many cyber-attack analysis models have been proposed in past research to assist in improving defender understanding of attack vectors and associated threat actor behaviour.

The rapid commercialisation of space, and increased ease and lowering costs associated with launching satellites into space, has resulted in global supply chains of privatised satellite networks for commercial and military purposes. The IoT and associated connectivity with Low Earth Orbit (LEO) satellite networks has also created numerous vulnerabilities, which raises questions of how contemporary cyber-attacks could potentially impact satellites and the space security domain more broadly.

This whitepaper presents a novel Satellite Cyber Resilience Taxonomy derived from related contemporary literature, and proposes a taxonomy-guided research roadmap for SmartSat CRC based on identified space systems cyber-resilience literature gaps.

Research Methodology

This whitepaper has been produced based on literature review, desktop study, secondary analysis of data, and input from SmartSat CRC expert focus groups.

Literature Review

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

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

This whitepaper focuses exclusively on the cyber-security and resilience of satellites, which falls under the space systems security dimension. Space systems security is defined as, ‘the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction’ (Plotnek and Slay, 2021a).

Satellite Cybersecurity can thus be understood as:

'…the ability to place and operate satellites outside Earth's atmosphere without external interference, damage or destruction due to cyber-attack.'

With definitional scope in mind, a collection of disparate papers relating to the domain of space systems security can be found.

The *Handbook of Space Security* (Schrogl, 2020) contains a broad collection of different papers that, together, provide a foundation for understanding the various aspects of the space security domain, including four chapters specifically related to space systems security. In the chapter entitled 'Definition and Status of Space Security', Antoni reviews the definitional history of space security and proposes a new definition (Antoni, 2020). Albeit consistent with historical definitional attempts, Antoni's definition conflicts with the contemporary understanding of space security as a three-dimensional domain (Mayence, 2010); a notion on which this whitepaper expands. Space resilience from a policy perspective is also examined, with a unified definition proposed, based on policies in use around the developed world (Peldszus, 2020), which is critically analysed further in Section 6.3. The final chapter of relevance to satellite cyber-resilience is the one entitled, 'Space and Cyber Threats' (Zatti, 2020), which discusses space-cyber policy from a European perspective. Despite the heavy policy focus, the chapter also contains valuable space systems security insights such as a detailed analysis of key satellite-specific cyber-security threats and technical countermeasures.

A second key text in this domain is the book by Georgescu et al. entitled '*Critical Space Infrastructures: Risk, Resilience and Complexity*' (Georgescu, 2019). The book provides a comprehensive understanding of space infrastructure but is decidedly lacking in its discussion of cyber-security issues. Georgescu also contributes a chapter of the same theme to the *Handbook of Space Security* (Georgescu, 2020).

A whitepaper by the United States Office of the Assistant Secretary of Defense for Homeland Defense & Global Security entitled '*Space Domain Mission Assurance: A Resilience Taxonomy*' (US DoD, 2015) gets particular attention among space resilience advocates. However, the proposed resilience taxonomy is detached from tangential resilience literature and thus lacks a solid academic foundation. Additionally, and surprisingly, the whitepaper does not acknowledge the security landscape, with 'cyber' not earning a single mention.

In 2016, Housen-Couriel published a paper on '*Cybersecurity Threats to Satellite Communications*' with the goal of establishing a typology of state actor responses. However, it is focused on international law and thus does not adequately address satellite cyber-security or resilience from a technical perspective. The paper does, however, identify five stages of satellite operations, which is a security-relevant model for conceptualising the satellite lifecycle (Housen-Couriel, 2016):

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

A Chatham House research paper by Livingstone and Lewis takes a high-level approach to space cyber-security, discussing topics such as cyber-threats and risks to satellite infrastructure, as well as challenges and trends in the industry (Livingstone and Lewis, 2016). Although valuable in contextualising the issue of satellite cyber-security, the paper is directed toward a general audience and is therefore not based on published taxonomies.

Finally, a comprehensive paper by Pavur and Martinovic details the cyber-security threats to satellites and examines over 100 significant satellite hacking incidents over the past 60 years (Pavur and Martinovic, 2020). The paper identifies four sub-domains to which satellite cyber-security applies:

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

A few other papers touch on the subject but are specific to niche technologies or formal methods, hence they do not adequately lay the foundation for future satellite security and resilience research (Hannan, 2018; Ikitemur, 2020; Kallberg, 2012; Kang, 2018; Santamarta, 2014).

It is important to note that this literature review was only conducted across open source English resources, not only skewing the threat context to a Western bias, but also excluding any additional or conflicting research that may exist within classified archives.

The research conducted in support of this whitepaper is currently under review for publishing, but can largely be attributed to Plotnek and Slay (Plotnek and Slay, 2021a; Plotnek and Slay, 2021b).

2. Space Resilience Taxonomy

2.1 Critical Space Infrastructure

Critical infrastructure is defined slightly differently by each jurisdiction (Critical Five, 2014). However, it generally refers to any infrastructure on which society has a critical dependency and which, if disrupted, could cause significant and potentially catastrophic consequences to the safety or security of that society (Council, 2004).

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

Many critical infrastructure systems rely on satellites for vital functions like time, location, guidance, communications and sensory data. Everything from guided munitions to air traffic control and banking to emergency services depends heavily on satellites to function safely and effectively. Satellites also provide vital services, data and imagery to government agencies and civilian populations who could all be significantly impacted in the case of an event, potentially triggering mass panic or fear. Hence it can be understood that catastrophic consequences, including potential loss of life, are sure to follow any major disruptions to satellite infrastructure; a clear case for its criticality to society (Georgescu et al., 2019).

2.2 Critical Infrastructure Resilience

Having established that satellites are indeed critical infrastructure, we can now look to other domains of critical infrastructure resilience to identify commonalities and define a satellite-specific approach that is grounded in published literature. There are many different types of critical infrastructure, each with its own peculiarities and approach to resilience, so it is useful to limit the comparative analysis to cyber-physical systems (CPS) only. A CPS includes any system that converts electronic signals to physical actions, such as a satellite receiving control signals.

Some of the most prominent Critical Cyber-Physical Infrastructure (CCPI) domains include energy, water and wastewater, manufacturing, and transportation. Of these domains, the energy sector stands out in the literature as having invested the most resources into their understanding of resilience (Fraccascia et al., 2018). Power systems also share the most similarities with space systems, such as: aging infrastructure; continuous availability requirements; remote and inaccessible components; vast distance coverage; centralised control; vulnerability to cascading failures; and complex inter-system dependencies. It therefore makes sense to leverage power systems resilience literature in establishing a baseline understanding for satellite cyber-resilience.

Prior to circa 2016, power systems resilience was used interchangeably with other terms, such as reliability, recoverability, availability, robustness and risk (Roege et al., 2014). However, the concept is now distinctly understood as the recurring ability of a system to anticipate, survive, sustain, recover from and adapt to high-impact low-frequency (HILF) events (Plotnek and Slay, 2021c). This can be contrasted to reliability engineering, which focuses on a system's ability to continue operations despite low-impact high-frequency (LIHF) events such as routine disruptions or common errors (Albasrawi et al., 2014). HILF events are also sometimes referred to as black swan events, defined by Gholami et. al as a rare 'unknowable' event with unforeseen or unobserved consequences upon random occurrence, such as the 9/11 attacks or Stuxnet (Gholami et al., 2018). Gholami et. al also make a distinction between black swan and grey swan events, where a grey swan is a metaphor for an 'unknown' or partially predictable, high-impact and rare event, such as a natural disaster.

Besides the definitional confusion historically surrounding the concept of resilience, some other problem areas are also signposted in the literature. One such trend was noted to be a transitioning away from purely technical and mathematically-derived resilience formulas towards an inclusive approach more comparable to risk analysis (Plotnek and Slay, 2021c). The key factor in this transition is the increasing recognition of incalculable socio-technical impacts on resilience. Examples of such 'human' aspects that may factor into the resilience equation include processes, procedures and management (Kwasinski, 2016), social wellbeing post-event (Liu et al., 2016), human-machine interfaces (HMI) in the control loop (Genge et al., 2015), and human behaviour and bureaucracy in times of emergency (Eisenberg et al., 2014).

Another hurdle of which to be aware in the quest for understanding space resilience is how the definition will drive resilience measurement and monitoring. Resilience is measured against a specified threat event, and so metrics should be considered from the outset (Bie et al., 2017; Chanda and Srivastava, 2015). Power systems resilience literature displays a tension between top-down and bottom-up approaches to metrics. This issue has led to many competing definitions, each with only a slightly different threat or event focus. For example, some power systems resilience definitions attempt a top-down approach where they generalise the threat (e.g. make no distinction between natural or man-made disasters) and end up with non-specific or unmeasurable metrics (Kwasinski, 2016; Dessavre et al., 2015; Friedberg et al., 2017). Others attempt a bottom-up approach with multitudes of differing definitions specific to precise threat events leading to disparate and disorganised definitions (Gholami et al., 2018; Panteli et al., 2017). Both approaches inevitably lead to the continuous reinvention of resilience and its definitional attributes, creating confusion and reducing the effectiveness of the term.

To avoid this issue, it is important to ensure that the proposed satellite cyber-resilience definition is broad enough to be relevant to any viable HILF threat to satellite resilience, but specific enough to ensure that every resilience practitioner in the domain can use common language for effective communication. This approach treats resilience not as a binary state, but as a system characteristic with various nuanced facets that can be measured under specified circumstances (Jackson and Fitzgerald, 2016).

2.3 Space Resilience Taxonomy

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

The definitional variance of space resilience is made clear in the *Space Security Handbook* chapter entitled 'Resilience of Space Systems: Principles and Practice', in which Peldszus reviews global space resilience policies to gain an understanding of how policy makers, systems analysts and operators define the term in practice (Peldszus, 2020). Peldszus then proposes a unified definition of space systems resilience based on the findings.

Although valuable for policymakers, a more reliable strategy for technical resilience would be to propose a definition grounded in taxonomy. As discovered in earlier sections, system resilience is a function of anticipating, surviving, sustaining, recovering from and adapting to HILF events. Additionally, resilience should account for socio-technical factors and be broad enough to allow for tailoring to each specialist sub-domain's metric measurement needs.

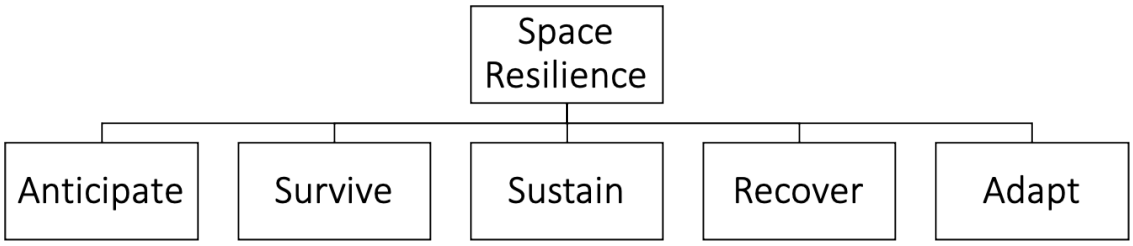

Figure 1 - Space resilience taxonomy (Plotnek and Slay, 2021b)

Before attempting to define resilience for satellites, it is helpful to understand space resilience from a taxonomical perspective. This aids in breaking down the problem of resilience into smaller focus areas for easier measurement and management, as demonstrated in Figure 1 above.

The space resilience taxonomy at Figure 1 can be applied to satellite cyber-resilience, where (Plotnek and Slay, 2021b):

- Anticipate refers to the satellite system's resilience-enhancing mechanisms in place to prevent, detect and avoid HILF cyber events
- Survive refers to the satellite system's resilience-enhancing mechanisms in place to mitigate, absorb and withstand the impacts of the HILF cyber event
- Sustain refers to the satellite system's resilience-enhancing mechanisms in place to contain any impacts and preserve core functions during a HILF cyber event

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

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

These five taxonomical categories can also be understood as phases within an indefinitely recurring resilience cycle, as per Figure 2 below. The residual impact seen in this figure refers to the post-event impact after resilience-enhancing mechanisms have mitigated the impacts of a HILF event. As shown, the residual impact can both weaken overall system resilience as well as going on to cause impacts external to the satellite, such as to the wider mission or social wellbeing.

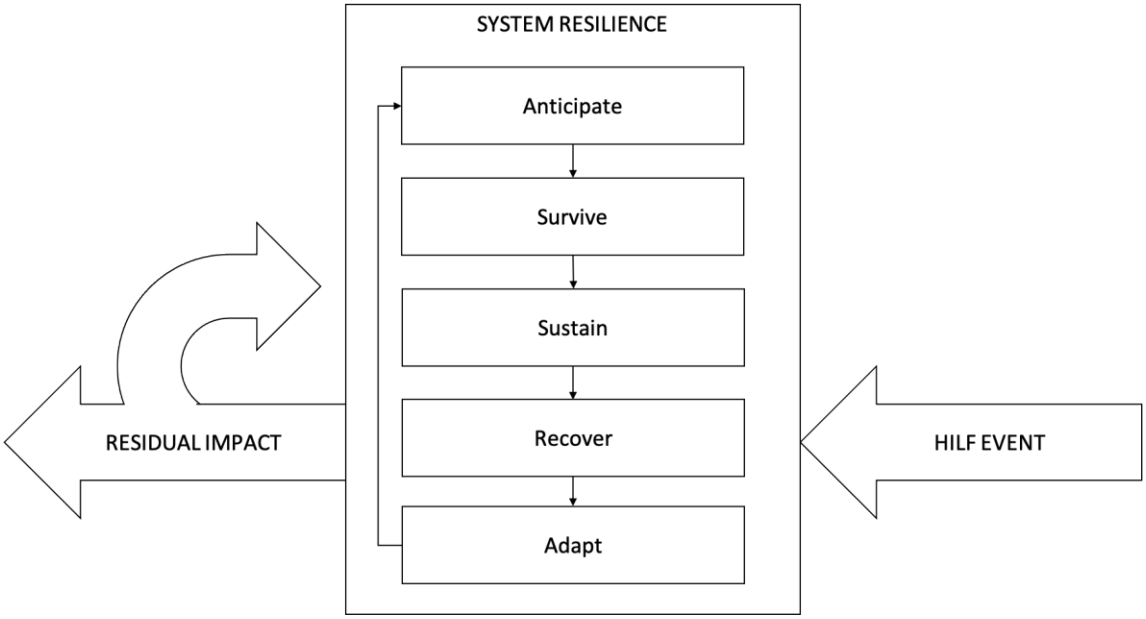

Figure 2 - Resilience cycle in response to High-Impact Low-Frequency (HILF) threats (Plotnek and Slay, 2021b)

With a novel resilience taxonomy and a clear understanding of how each resilience aspect cyclically interacts in a space context, space resilience can be defined as:

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

3. Satellite Cyber Resilience

Based on the space resilience definition established in Section 2, satellite cyber-resilience can be defined as:

'…the recurring ability of a satellite system, including all sub-components and supporting functions, to anticipate, survive, sustain, recover from and adapt to high-impact low frequency cyber events.'

In the above definition, a 'cyber event' can be understood as any unexpected and undesired HILF threat to a satellite system by way of either malicious attack or negligent malpractice by a cyber threat actor. Cyber threats interfere with the confidentiality, integrity or availability of satellite systems through the manipulation of data and code, and can be broken down into three components:

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

The threat actor is the person or organisation behind the attack, and can be assessed by considering their capability to conduct an attack versus their intent behind the attack. The threat vector refers to the vulnerable point of entry used by the threat actor to successfully carry out the attack; for example, if a ground system is air-gapped (i.e. not connected to any network) then the threat vector may be a flash drive. Finally, the attack itself is the exploit used by the threat actor to achieve their objectives and cause the desired impact; for example, malware or spoofing. In the case of malpractice, the threat actor can cause an adverse impact without malicious intent.

This is visually summarised in Figure 3 below, whereby the threat vector is the actor's entry to the satellite system, eventually resulting in an impact that extends back to the operational environment.

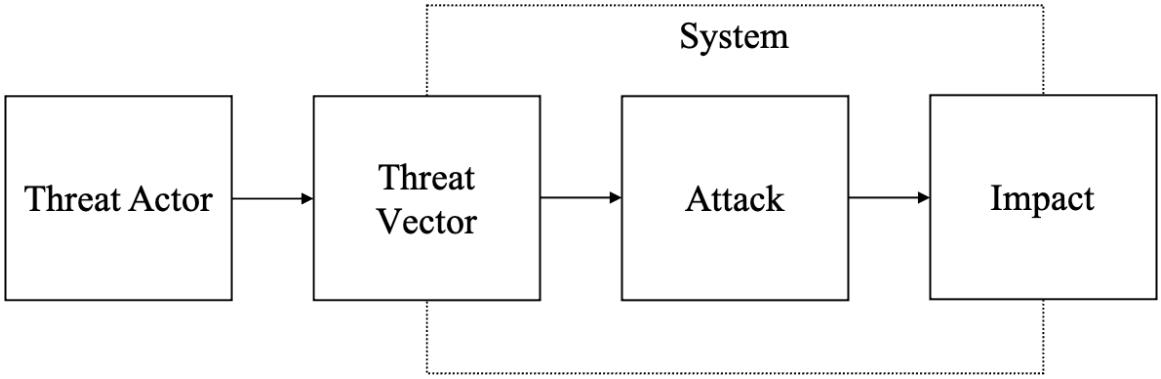

Figure 3 - Anatomy of a targeted threat (Plotnek and Slay, 2021)

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

- nation-state
- terrorist
- criminal group; or
- individual (e.g. insider threats, hacktivists, or bored teenagers).

Sometimes, hacktivism occurs on a larger scale (e.g. Anonymous) and can be treated as a separate category, conforming to neither terrorist nor criminal motivations. Bradbury et al. broke these high-level categories down further and provided satellite-specific examples in Figure 4 below (Bradbury et al., 2020).

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

Figure 4 - Threat actor examples (Bradbury et al., 2020)

As Figure 4 demonstrates, each actor type has their own intent (i.e. goals & motivations) and capability (i.e. capabilities, environment, resources) that drives their decision-making process

when considering the carrying out of a cyber-attack against satellite infrastructure. Pavur and Martinovic produced a similar yet simpler version of this threat actor table, expanding beyond just cyber-security considerations in Figure 5 (below).

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

Figure 5 - Summary of Satellite Threat Actors (Pavur and Martinovic, 2020)

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

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

Each of these components can be accessed via a myriad of different threat vectors, such as through ground segments, supply chains, unsecured communications links and countless other avenues. Bradbury et al. propose a handy reference architecture for assessing satellite threat vectors and attack surfaces in their 2020 IEEE Aerospace Conference paper (Bradbury et al., 2020).

4. Research Roadmap

4.1 Space Trends and Projections

Before designing a research roadmap, it is important to consider current space trends and projections to best allocate resources. From colonies on Mars to space hotels and deep-space exploration, there is no shortage of ideas to keep humanity driving forward in this domain. The first space race cemented space systems as critical infrastructure for progressing life on earth. The second space race is shifting the focus from government to commercial interests, with significant headway already being made to secure space as a viable human arena in its own right.

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

Alongside the rapid evolution of satellite systems also comes all kinds of new threats. Talk of cyber warfare, cyber terrorism and cybercrime are increasing, and so are the capabilities of motivated threat actors (Plotnek and Slay, 2021d). Both cyber and electronic weapons are becoming more effective and accessible by the day, with at least 120 different countries already invested in cyber warfare capabilities (McAfee, 2005). Additionally, the United States has officially approved the establishment of a Space Force (Farley, 2020), and many other countries are likely to follow suit – events that will undoubtedly impact the space security domain.

Mass-scale environmental and political events may also impact humankind's reliance on satellites, potentially causing unforeseeable impacts. For example, hazardous asteroids heading for earth (O'Neill and Handal, 2021) or the growing threat of climate change, both of which are tracked and assessed using satellite infrastructure – a reliance that may evolve and become more critical as time goes on. Another example might be a third eruption of world warfare. Military equipment has become increasingly reliant on satellite technology and such a situation may over-burden aging infrastructure and cause Denials of Service (DoS) in critical moments.

4.2 Research Opportunities

Pulling together the different research threads identified throughout this whitepaper paints a picture of the current state of space systems security as a domain, and highlights areas needing further development, as shown below in Figure 6. As can be seen, we currently have a preliminary understanding of attack surfaces, threats and actors, as well as past events and future predictions, which are not shown in the diagram.

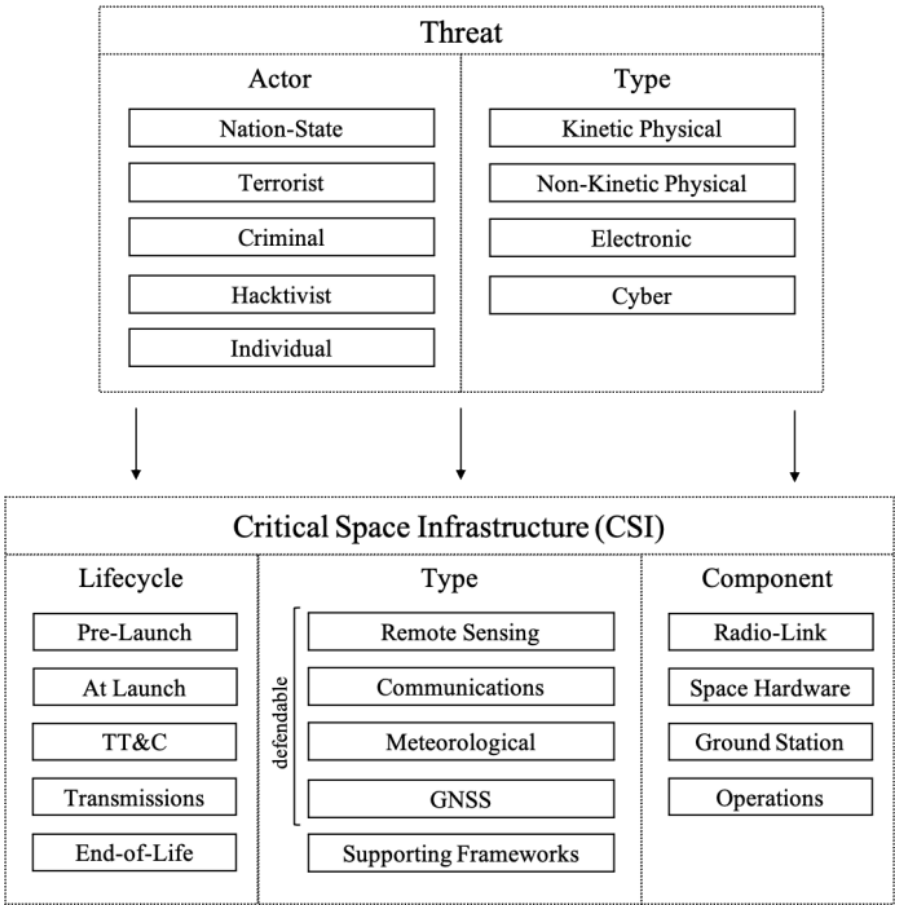

Figure 6 - Threats to Critical Space Infrastructure (CSI) broken down into taxonomical sub-categories as per available literature (Plotnek and Slay, 2021a)

With a clear idea of the current state of the literature it becomes easier to see a path forward. However, just because research on certain problems happens to exist does not necessarily mean that those questions that have been asked are the most important ones to be asking.

4.3 Research Roadmap

A satellite cyber resilience research roadmap can help SmartSat CRC researchers by mapping out the domain and providing a comprehensive scoping guide for research planning and prioritisation.

The first step in preparing a research roadmap is to break the satellite cybersecurity domain down into manageable blocks. Table 1 below provides a cross-mapping of satellite components (Pavur and Martinovic, 2020) to the space resilience taxonomy (Figure 1) and designates a sub-section that outlines each research area. This method ensures that each satellite component is considered against every stage of cyber-resilience, providing full-spectrum coverage of the problem of satellite cyber-security and resilience.

Table 1: Satellite cyber-security and resilience research roadmap broken down by component and resilience phase

	Radio-Link	Space Hardware	Ground Station	Operations
Anticipate	6.3.1.1	6.3.2.1	6.3.3.1	6.3.4.1
Survive	6.3.1.2	6.3.2.2	6.3.3.2	6.3.4.2
Sustain	6.3.1.3	6.3.2.3	6.3.3.3	6.3.4.3
Recover	6.3.1.4	6.3.2.4	6.3.3.4	6.3.4.4
Adapt	6.3.1.5	6.3.2.5	6.3.3.5	6.3.4.5

In the following sub-sections, the four satellite components (i.e. columns of Table 1) will be defined at each of the five phases of the resilience cycle (i.e. rows of Table 1), such that:

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

Finally, researchers should consider the impact and frequency of cyber-threats when scoping resilience research. Resilience is concerned primarily with high-impact low frequency events, whereas reliability engineering is focused on low-impact high-frequency events.

4.3.1 Satellite Radio-Link Resilience

More than two-thirds of historical satellite incidents relate to attacks on the radio-link (i.e. RF communications). Besides jamming attacks, which are generally considered electronic attacks and not cyber-attacks, most historical radio-link attacks are either eavesdropping, signal injection or signal spoofing (Pavur and Martinovic, 2020). This is not to say that other types of cyber-attacks will not affect radio-links in the future; something that should be pre-emptively considered by researchers.

The following subsections leverage the space resilience taxonomy to define the parameters of a perfectly cyber-secure and resilient satellite radio-link subsystem. Each statement should be interpreted as a hypothetical ideal and can be used as a baseline to scope future research questions and programs in this domain.

4.3.1.1 Anticipate

A resilient satellite radio-link sub-system should be able to anticipate (i.e. prevent, detect and avoid) cyber-attacks.

4.3.1.2 Survive

A resilient satellite radio-link sub-system should be able to survive (i.e. mitigate, absorb and withstand) cyber-attacks.

4.3.1.3 Sustain

A resilient satellite radio-link sub-system should be able to sustain operations during cyber-attacks by containing impacts and preserving core functions.

4.3.1.4 Recover

A resilient satellite radio-link sub-system should be able to recover (i.e. respond, restore operations and ‘bounce back’) from cyber-attacks.

4.3.1.5 Adapt

A resilient satellite radio-link sub-system should be able to adapt to its threat environment by incorporating resilience enhancements from lessons learned.

4.3.2 Satellite Hardware Resilience

Satellite payloads are often highly bespoke proprietary systems that are tailored specifically to the designated mission. Despite the research challenges this poses, the increased use of Commercial off-the-shel (COTS) components is making research in this domain more accessible.

Four common attack surfaces that should be considered for deployed satellite systems were identified in Section 3 (Wheeler et al., 2018):

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

Pavur and Martinovic also suggest that satellite cyber-security research should include space-side sub-systems such as onboard computing, telemetry, positioning and navigation, propulsion and reaction control, thermal control, power management and mission payload (Pavur and Martinovic, 2020).

The following sub-sections leverage the space resilience taxonomy to define the parameters of a perfectly cyber-secure and resilient satellite hardware sub-system, including the attack surfaces identified above. Each statement should be interpreted as a hypothetical ideal and can be used as a baseline to scope future research questions and programs in this domain.

4.3.2.1 Anticipate

A resilient satellite hardware sub-system should be able to anticipate (i.e. prevent, detect and avoid) cyber-attacks.

4.3.2.2 Survive

A resilient satellite hardware sub-system should be able to survive (i.e. mitigate, absorb and withstand) cyber-attacks.

4.3.2.3 Sustain

A resilient satellite hardware sub-system should be able to sustain operations during cyber-attacks by containing impacts and preserving core functions

4.3.2.4 Recover

A resilient satellite hardware sub-system should be able to recover (i.e. respond, restore operations and 'bounce back') from cyber-attacks.

4.3.2.5 Adapt

A resilient satellite hardware sub-system should be able to adapt to its threat environment by incorporating resilience enhancements from lessons learned.

4.3.3 Satellite Ground Station Resilience

Ground station systems are generally comparable to other terrestrial computing systems and hence do not face the same unique challenges that other satellite subsystems face. Usually, a ground station will consist of RF communications equipment to communicate with the satellite, and a computer that runs specialist satellite communications software. Most historical ground station incidents have been deemed by-products of general untargeted intrusions (Pavur and Martinovic, 2020).

Nevertheless, there are several aspects of satellite ground station resilience that are noteworthy from a space security research perspective. Perhaps most importantly, the ground station marks the security boundary between the satellite's maintainable ground components and its inaccessible space components. Secondly, satellite ground systems are often located in remote and unmanned locations, thereby increasing the system's vulnerability to cyber-attacks that exploit physical access. Finally, satellite ground stations are often internet-connected for remote access, which then holds potential to expose the deployed space system to internet-based threats.

The following sub-sections leverage the space resilience taxonomy to define the parameters of a perfectly cyber-secure and resilient satellite ground station subsystem. Each statement should be interpreted as a hypothetical ideal and can be used as a baseline to scope future research questions and programs in this domain.

4.3.3.1 Anticipate

A resilient satellite ground station sub-system should be able to anticipate (i.e. prevent, detect and avoid) cyber-attacks.

4.3.3.2 Survive

A resilient satellite ground station sub-system should be able to survive (i.e. mitigate, absorb and withstand) cyber-attacks.

4.3.3.3 Sustain

A resilient satellite ground station sub-system should be able to sustain operations during cyber-attacks by containing impacts and preserving core functions.

4.3.3.4 Recover

A resilient satellite ground station sub-system should be able to recover (i.e. respond, restore operations and 'bounce back') from cyber-attacks.

4.3.3.5 Adapt

A resilient satellite ground station sub-system should be able to adapt to its threat environment by incorporating resilience enhancements from lessons learned.

4.3.4 Satellite Operations Resilience

Satellite system resilience should be considered across each of the five phases of satellite operations identified in Section 1 (Housen-Couriel, 2016), with each having its own operational requirements and vulnerabilities:

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

In addition to the above, Georgescu et al. (Georgescu, 2019) suggest that a taxonomy can be used to divide satellite operations into five key mission-oriented categories:

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

The following sub-sections leverage the space resilience taxonomy to define the parameters of perfectly cyber-secure and resilient satellite operations. Each statement should be interpreted as a hypothetical ideal and can be used as a baseline to scope future research questions and programs in this domain, with reference to the points above.

4.3.4.1 Anticipate

Resilient satellite operations should be able to anticipate (i.e. prevent, detect and avoid) cyber-attacks.

4.3.4.2 Survive

Resilient satellite operations should be able to survive (i.e. mitigate, absorb and withstand) cyber-attacks.

4.3.4.3 Sustain

Resilient satellite operations should be able to sustain operations during cyber-attacks by containing impacts and preserving core functions.

4.3.4.4 Recover

Resilient satellite operations should be able to recover (i.e. respond, restore operations and ‘bounce back’) from cyber-attacks.

4.3.4.5 Adapt

Resilient satellite operations should be able to adapt to their threat environment by incorporating resilience enhancements from lessons learned.

Conclusion

The past 60 years have seen space transform from an arena for politics to a critical infrastructure on which all of society heavily depends. Considering the newfound global appetite for space development and the rapidly expanding threat environment, a need for a better understanding of satellite cyber resilience has emerged.

This whitepaper has established a contextualised foundation for satellite cyber-security and resilience drawn from existing cross-disciplinary literature on the subject. It proposed a novel space systems resilience taxonomy and definition, derived from existing critical infrastructure resilience literature.

Satellite cyber-security was defined as the ability to place and operate satellites outside Earth's atmosphere without external interference, damage or destruction due to cyber-attack. Space resilience was defined as the recurring ability of a space system, including all sub-components and supporting functions, to anticipate, survive, sustain, recover from and adapt to high-impact low frequency events. Taxonomically space resilience was broken down into five categories – Anticipate, Survive, Sustain, Recover and Adapt – towards which different space technologies, such as cybersecurity features, can contribute to increase overall system resilience. It was also noted that resilience assessments should account for socio-technical factors, such as in-the-loop Human-Machine Interfaces (HMI) and residual impacts on society.

Finally, the whitepaper painted a picture of the current state of space systems security research and drew from this to design a satellite cyber-resilience research roadmap for SmartSat CRC. The proposed research roadmap is based on four key satellite sub-systems: radio-link security, space hardware security, ground station security, and operations security; which are then further segmented and discussed according to the satellite resilience taxonomy.

References

Sheehan, M., 2015. Defining Space Security, in: Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., Giannopapa, C. (Eds.), Handbook of Space Security. Springer, New York, United States of America, pp. 7–21.

Mayence, J.-F., 2010. Space security: transatlantic approach to space governance, in: Robinson, J., Schaefer, M., Schrogl, K.-U., von der Dunk, F. (Eds.), Prospects for Transparency and Confidence-Building Measures in Space. ESPI, Vienna, Austria, p. 35.

Plotnek, J., Slay, J., 2021a. A new dawn for space security. TBA, Australia.

Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., Giannopapa, C. (Eds.), 2015. Handbook of Space Security. Springer, New York, United States of America.

Antoni, N., 2015. Definition and Status of Space Security, in: Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., Giannopapa, C. (Eds.), Handbook of Space Security. Springer, New York, United States of America, pp. 9–33.

Peldszus, R., 2020. Resilience of Space Systems: Principles and Practice, in: Schrogl, K.-U. (Ed.), Handbook of Space Security. Springer, New York, United States of America, pp. 127–143.

Zatti, S., 2015. Space and Cyber Threats, in: Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., Giannopapa, C. (Eds.), Handbook of Space Security. Springer, New York, United States of America, pp. 245–263.

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

Georgescu, A., 2020. Critical Space Infrastructures, in: Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., Giannopapa, C. (Eds.), Handbook of Space Security. Springer, New York, United States of America, pp. 227–244.

US Department of Defense, 2015. Space Domain Mission Assurance: A Resilience Taxonomy. Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, United States.

Housen-Couriel, D., 2016. Cybersecurity threats to satellite communications: Towards a typology of state actor responses. Acta Astronautica 128, 409–415. https://doi.org/10.1016/j.actaastro.2016.07.041

Livingstone, D., Lewis, P., 2016. Space, the Final Frontier for Cybersecurity? Chatham House.

Pavur, J., Martinovic, I., 2020. SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research. eprint arXiv:2010.10872.

Hannan, N., 2018. An Assessment of Supply-Chain Cyber Resilience for the International Space Station. The RUSI Journal 163, 28–32. https://doi.org/10.1080/03071847.2018.1469249

Ikitemur, G., Karabacak, B., Igonor, A., 2020. A Mixed Public-Private Partnership Approach for Cyber Resilience of Space Technologies, in: Space Infrastructures: From Risk to Resilience Governance, NATO Science for Peace and Security Series - D: Information and Communication Security. IOS Press, pp. 120–130.

Kallberg, J., 2012. Designer Satellite Collisions from Covert Cyber War. Strategic Studies Quarterly 6, 124–136.

Kang, M., Hopkinson, K., Betances, A., Reith, M., 2018. Mitigation of Cyber Warfare in Space Through Reed Solomon Codes. Presented at the 13th International Conference on Cyber Warfare and Security, ACPI, Washington DC, United States.

Santamarta, R., 2014. SATCOM Terminals: Hacking by Air, Sea, and Land. IOActive, United States of America.

Plotnek, J., Slay, J., 2021b. Laying the groundwork for space systems resilience. TBA, Australia.

Critical Five, 2014. Forging a Common Understanding for Critical Infrastructure. Critical Five, New Zealand.

European Council, 2004. Communication from the Commission to the Council and the European Parliament: Critical infrastructure protection in the fight against terrorism. Commission of the European Communities, Brussels, Belgium.

Fraccascia, L., Giannoccaro, I., Albino, V., 2018. Resilience of Complex Systems: State of the Art and Directions for Future Research. Wiley Hindawi 2018, 1–44. https://doi.org/10.1155/2018/3421529

Roege, P.E., Collier, Z.A., Mancillas, J., McDonagh, J.A., Linkov, I., 2014. Metrics for Energy Resilience. Energy Policy 72, 249–256. https://doi.org/10.1016/j.enpol.2014.04.012

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

Albasrawi, M.N., Jarus, N., Joshi, K.A., Sarvestani, S.S., 2014. Analysis of Reliability and Resilience for Smart Grids, in: 2014 IEEE 38th Annual Computer Software and Applications Conference. IEEE, pp. 529–534. https://doi.org/10.1109/COMPSAC.2014.75

Gholami, A., Shekari, T., Amirioun, M.H., Aminifar, F., Amini, M.H., Sargolzaei, A., 2018. Toward a Consensus on the Definition and Taxonomy of Power System Resilience. IEEE Access 6, 32035–32053. https://doi.org/10.1109/ACCESS.2018.2845378

Kwasinski, A., 2016. Quantitative Model and Metrics of Electrical Grids' Resilience Evaluated at a Power Distribution Level. Energies 9, 93. https://doi.org/10.3390/en9020093

Liu, C.-C., McArthur, S., Lee, S.-J., 2016. Smart Grid Handbook. John Wiley & Sons, Chichester, UK.

Genge, B., Kiss, I., Haller, P., 2015. A System Dynamics Approach for Assessing the Impact of Cyber Attacks on Critical Infrastructures. Elsevier International Journal of Critical Infrastructure Protection 10, 3–17. https://doi.org/10.1016/j.ijcip.2015.04.001

Eisenberg, D.A., Park, J., Kim, D., 2014. Resilience Analysis of Critical Infrastructure Systems Requires Integration of Multiple Analytical Techniques. Urban Sustainability and Resilience 15.

Bie, Z., Lin, Y., Li, G., Li, F., 2017. Battling the Extreme: A Study on the Power System Resilience. Proceedings of the IEEE 105, 1253–1266. https://doi.org/10.1109/JPROC.2017.2679040

Chanda, S., Srivastava, A.K., 2015. Quantifying Resiliency of Smart Power Distribution Systems with Distributed Energy Resources, in: 2015 IEEE 24th International Symposium on Industrial Electronics (ISIE). IEEE, pp. 766–771. https://doi.org/10.1109/ISIE.2015.7281565

Dessavre, D.G., Ramirez-Marquez, J.E., Barker, K., 2015. Multidimensional Approach to Complex System Resilience Analysis. Elsevier Reliability Engineering & System Safety 149, 34–43. https://doi.org/10.1016/j.ress.2015.12.009

Friedberg, I., McLaughlin, K., Smith, P., Wurzenberger, M., 2017. Towards a Resilience Metric Framework for Cyber-Physical Systems, in: 4th International Symposium for ICS & SCADA Cyber Security Research 2016. https://doi.org/10.14236/ewic/ICS2016.3

Panteli, M., Mancarella, P., Trakas, D.N., Kyriakides, E., Hatziargyriou, N.D., 2017. Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems. IEEE Transactions on Power Systems 32, 4732–4742. https://doi.org/10.1109/TPWRS.2017.2664141

Jackson, M., Fitzgerald, J.S., 2016. Resilience Profiling in the Model-Based Design of Cyber-Physical Systems. 14th Overture Workshop.

Ormrod, D., Slay, J., Ormrod, A., 2021. Cyber-Worthiness and Cyber-Resilience to Secure Low Earth Orbit Satellites. Presented at the 16th International Conference on Cyber Warfare and Security, Academic Conferences Limited, p. 257.

McLeod, G., Nacouzi, G., Dreyer, P., Eisman, M., Hura, M., Langeland, K.S., Manheim, D., Torrington, G., 2016. Enhancing Space Resilience Through Non-Materiel Means (Technical Report No. AD1085075). RAND Project Air Force Santa Monica, Santa Monica, United States of America.

Straub, J., 2014. Building space operations resiliency with a multi-tier mission architecture. Sensors and Systems for Space Applications VII 9085. https://doi.org/10.1117/12.2050175

Naser, M.Z., Chehab, A.I., 2018. Materials and design concepts for space-resilient structures. Progress in Aerospace Sciences 98, 74–90. https://doi.org/10.1016/j.paerosci.2018.03.004

Phillips, D.M., Mazzuchi, T.A., Sarkani, S., 2018. An architecture, system engineering, and acquisition approach for space system software resiliency. Information and Software Technology 94, 150–164. https://doi.org/10.1016/j.infsof.2017.10.006

Bradbury, M., Maple, C., Hu, Y., Ugur, I.A., Cannizzaro, S., 2020. Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures, in: 2020 IEEE Aerospace Conference. Presented at the 2020 IEEE Aerospace Conference, IEEE, USA, pp. 1–20. https://doi.org/10.1109/AERO47225.2020.9172785

Wheeler, W.A., Cohen, N., Betser, J., Ewart, R.M., 2018. Cyber Resilient Flight Software for Spacecraft, in: AIAA SPACE and Astronautics Forum and Exposition. American Institute of Aeronautics.

Plotnek, J., Slay, J., 2021d. Cyber terrorism: A homogenized taxonomy and definition. Computers & Security 102, 102145.

McAfee, 2005. McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet. McAfee.

Farley, R., 2020. Space Force: Ahead of Its Time, or Dreadfully Premature? CATO Institute Policy Analysis 904.

O'Neill, I.J., Handal, J., 2021. https://www.jpl.nasa.gov/news/nasa-analysis-earth-is-safe-from-asteroid-apophis-for-100-plus-years. NASA Jet Propulsion Laboratory.

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