Security Challenges when Space Merges with Cyberspace

This position paper provides an analysis of threat landscape and emerging security challenges in the new space era and outlines technological and policy issues that need to be tackled in developing cyber security solutions for advancing the space industry for Australia.

1. Introduction

There is an escalation of security attacks in the space with the increasing challenges in the intersection of cyber security and space security. With the increasing commercialization and militarization of space sector, cyber security for space infrastructures will pose major challenges in the future [1]. Many of the world's critical infrastructures are heavily dependent on space-based assets, for their daily functioning. Critical terrestrial infrastructures such as communications, air transport, maritime trade, financial services, weather monitoring and defence, rely on space systems such as satellites, ground stations and communication links at the national, regional, and international level [2]. The compromise of space infrastructures will have a dramatic impact on the critical services on which our way of life on the earth depends on.

Space systems are how vital information is communicated to keep the power grid synchronized and the stock-market transactions are timed. Should the availability of such timing become impacted, the economy could be crippled, potentially leading to shortages of food, water, medicine, and commodities. Moreover, global navigation services, such as the Global Positioning System (GPS) that are used for trans-oceanic shipping and in daily civilian travel depend on space infrastructures. Satellites provide aerial coverage to view areas struck by natural disasters, enable live reporting of events, and provide information for organizing coordination of international relief efforts. We can even say that space systems have been the basis for the asymmetric warfare deterrence strategies that have helped to keep the different spheres of influence (such as US, Russia, Europe, and China) relatively peaceful so far.

Current trend is for the space sector to grow even faster in the future [3], with the space capabilities becoming more and more commercially competitive, driven by falling costs of launch and rapid technology developments. Despite the space industry's sophistication and the increasing dependency on the space infrastructures, cyber security issues are somewhat under recognized by the infrastructure providers and policymakers alike; they tend to lag developments in other high-technology sectors. In this article, we examine the current threat landscape of space infrastructures and security challenges and outline the issues that need to be tackled in the formulation of cyber security solutions for space as well as provide recommendations for developing a policy framework for space security.

Space Systems

Space systems are assets that either exist in suborbital or outer space or ground control systems, including facilities used in launching these assets [4]. Space systems are usually divided into three technological and operational segments namely the ground segment, the space segment, and the link segment. The space segment comprises groups of satellites in orbit (as well as launch vehicles designed to release satellites into space). A satellite contains a payload, the equipment designed to carry out the satellite's function, and a bus, which houses the payload and remaining satellites systems. The

link segment consists of the transmission channels between the satellite and the ground station, as well as between satellites. The ground segment consists of all the ground elements of space systems and allows command and control, and management of space objects such as satellites as well as the data arriving from the payload and delivered to the users. All these segments can be exposed to a range of cyber threats.

Space organizations are organizations that build, operate, maintain, or own space systems. Space systems, however, are somewhat more complex than terrestrial digital infrastructures from a technology development, ownership, and management perspective. Cyber vulnerabilities pose serious risks not just for space-based assets themselves but also for ground-based critical infrastructures. From a technology perspective, it is easy to imagine an attacker attempting to interrupt a nation's commerce attacking cloud services offered by companies such as Amazon or PayPal or a banking institution. However, nowadays these companies invest heavily in cyber security and are constantly monitoring their systems and networks for malicious activities and vulnerabilities. For an attacker, a simpler and probably a more productive route would be to target space infrastructures that provide connectivity to financial systems and services and attack the space organizations that provide and operate these satellites enabling such services. The ability to impact multiple systems by compromising a central point of failure makes space systems attractive targets. Not only they offer a vast attack surface but also there is a lack of security regulation governing space systems, despite their critical nature. Often space systems are overlooked being part of the underlying infrastructure for critical systems and are not subjected to same level of security standards. Furthermore, the situation is exacerbated due to the ambiguity that often exists when it comes to the responsibility for cybersecurity in space and its ongoing management. Furthermore, commercial transformation of space capabilities also raises some fundamental questions as to how best to regulate the activities of the commercial actors in space.

2. Why space infrastructures are vulnerable?

There are many satellites that are old, but also having some old technologies, which are easily prone to cyberattacks due to weak security functionalities, if any. For instance, they may have their security credentials hardcoded and there can be insecure communication protocols making them vulnerable to attackers. Furthermore, as more and more commercial actors begin to access space and start offering a range of services, it dramatically increases the attack surface.

<u>Vulnerabilities in the Ground Systems</u>

Compromising the ground station infrastructures is the easiest way to attack space systems, as it provides the software and the hardware required to legitimately control and track space objects using existing terrestrial networks and systems. It is important to note that there is also the user segment of the space infrastructure, which can be thought of as an extension of the ground segment for the end-users of a space-based service. This can itself be a distributed infrastructure providing interfaces to various applications and services that can interact with satellite signals directly or with other ground segment systems.

In the same vein as attacks on enterprise infrastructures, the space attack vectors involve techniques such as exploitation of misconfigurations and software vulnerabilities in systems, gaining unauthorized access to critical services, injection of malware and use of phishing to obtain sensitive credentials. For

instance, this could involve exploiting web vulnerabilities or luring the ground station personnel to download malwares and Trojans to their devices to take control of the satellites and sabotage them.

In fact, some of the interesting attacks against space systems have been on the services that enable them. For instance, vulnerabilities in the ground systems or in the satellite data receivers can allow the attacker to infiltrate the ground network and to remain there undetected. Another common threat is the introduction of a malware into the satellite's hardware and software systems (e.g., via the supply chain) can also compromise the ground systems at a later stage. Turla attack [5] on the satellite Internet provider enabled the attacker to steal IP addresses. This attack was not easily detectable because it was dependent on whether the attacker and the legitimate user were using the IP address simultaneously. It allowed an attacker to inject false data to the user systems connected to that IP address, such as an autonomous drone, leading to its crash. Hence such attacks can remain stealthy and unlikely to be detected by intrusion detection systems.

Vulnerabilities in the Space Segment

The space segment comprises groups of satellites in an orbit as well as space stations and launch vehicles designed to release satellites into space. A satellite itself contains a payload and systems designed to carry out the satellite's functions. For instance, these systems are responsible for receiving and processing uplink and downlink signals, validating, decoding, and sending commands to other subsystems, and controlling the stabilization and orientation of the satellite etc.

Such systems can be subjected to at least four types of cyberattacks. Spacecraft could be vulnerable to command intrusions (giving bad instructions to destroy or manipulate basic controls). There can also be malicious control of payload and attacks such as denial of service (sending too much traffic to overload systems). Malware could also be used to infect systems on the ground (like satellite control centres and user systems), as well as the links between them, spoofing the communications from an untrusted source as a trusted one or replaying, interrupting, or delaying communications.

Communication Vulnerabilities

The most common threat against the communication channels (uplink and downlink channels) is that of jamming, which compromises the GPS systems [6]. GPS jammers send signals over the same frequency as the GPS device, to override or distort the GPS satellite signals. GPS jammers are widely accessible and cheap to purchase, rendering them available to less sophisticated state and commercial malicious actors. In Nov 2018, Russia was suspected of disrupting GPS signals, when Norway and Finland participated in NATO's Trident Juncture exercise [7]. GPS spoofing involves the manipulation of the GPS signal and is more dangerous than jamming because it appears to the user that the GPS is working as intended. A system that can execute a software-defined spoof attack is easy to develop with low costs (e.g., $1000 or so to build as demonstrated in [8]). For instance, it is believed that, in Sept 2011, Iranians successfully captured an American RQ-170 Sentinel drone by reconfiguring the coordinates of the GPS signal to make the drone land in Iran instead of its base in Afghanistan [9].

All it takes is the production of a relatively inexpensive spoofer, and an attacker can command and control the uplink signal to a satellite. If the downlink from a satellite is spoofed, false data can be injected into a target's communications systems, fooling the receiver into calculating an incorrect position. Intentional alteration of data communicated to the spacecraft can have a catastrophic effect, if either no action occurred (e.g., command is discarded) or a wrong action taken by the onboard

systems in the spacecraft. Furthermore, if the traffic is unencrypted, the attacker could also intercept and eavesdrop on the satellite traffic. In the near-term, these kinds of attacks will likely remain, coming not only from nation state actors, but also from well-resourced non-state actors (e.g., criminal groups seeking financial gain), as more communications capabilities come online via space.

Supply Chain Vulnerabilities

Another major issue in space system security arises due to the complexity of supply chain and vendor ecosystem of government funded systems. Usually, the specialized components needed for space assets are not all developed by a single manufacturer. In fact, to keep the costs down, space organizations often purchase components from catalogues of approved vendors around the world. The approval process for these vendors does not necessarily specifically include cyber security vetting standards. When a space organization purchases a component from a vendor, for instance, it has little control over the code written by a software developer of that component. This lack of insight introduces considerable cyber security risk.

In addition to vendors being vulnerable across the system supply chain, often space organizations tend to work with several research institutions, who may have their own vulnerabilities. Naturally collaborations across multiple partners exacerbate potential supply chain security issues, which make it difficult to ascertain who should be operationally (and financially) responsible for the cyber security of a system at various point of the space asset's lifecycle. Hence the security challenge in the space asset supply chain life cycle is caused by the complexity of development, management, use and the ownership of space assets.

Furthermore, nowadays cloud infrastructures form an integral part of service provision, and hence are often used for data storage and processing by ground station systems. These cloud systems are owned by other commercial providers, and vulnerabilities and failures in in these infrastructures can have adverse impact including hindering operations of satellite real time systems and denial of service attacks on the satellite receivers.

Unlike critical infrastructures, space assets are often not owned by the same organization that manages the infrastructure, which results in uncertainties related to liability if they are attacked. Further, the longer lifespan of the space asset itself complicates it even more. Space missions can last decades and because of this, security concerns are exacerbated from unpatched legacy systems. Not dissimilar to industrial control systems, space assets are built to last and because they are functional in the field for long periods and are mission critical, system downtime is not usually an option. This makes space assets difficult, if not impossible, to patch for security flaws, when they are discovered. Furthermore, with the increasing use and connectivity to Internet of Things (IoT devices), attacks on space satellites can cause wide disruptions to communication channels endangering national as well as international security [10].

3. Security Challenges

Given the rapid growth of the space sector and the increasing ability to manipulate and exploit the vulnerabilities in space systems by an increasing number of diverse space actors, cyber security for space poses several unique challenges. Not only space is becoming increasingly congested, contested, and competitive, it is also becoming more commercial. The danger with growing space activities and

the proliferation of space-capable actors is that it can lead to mistrust among the parties, which can potentially lead to miscalculations and misunderstandings especially with new technologies. Let us now examine some new and unique security challenges in space infrastructures.

- The current state of the art in security in space systems is often based upon strong boundary protection in the ground segment together with encryption to secure communications between the ground station and the space objects. Onboard the space object such as a satellite, often the assumptions made are that its components are trusted based on the assurances in the supply chain. This in turn means that the spacecrafts themselves are designed with few if any security defence mechanisms. For instance, if an adversary were able to gain access to the ground segment or insert malware into a spacecraft component, then there are often few or no protections to prevent them from directly controlling the space segment.
- A consequence of lack of built-in security measures in space systems is that it provides a new opportunity for the attackers to discover and exploit vulnerabilities, and maliciously manipulate remote space objects. Scarce documentation and lack of source code availability create the "security through obscurity" mentality with which vendors often develop these space products.
- In terrestrial network systems, we regularly employ intrusion detection and prevention systems (IDS/IPS) to monitor and respond to threats in infrastructures. Similar technology will be required for space systems to observe and tackle potential attacks on-board satellites such as data protocol and RF-based attacks. Intrusion detection and prevention technologies leveraging machine learning to detect and block cyber intrusions onboard space objects would be the natural approach to consider in future space systems. However, this can introduce additional issues related to competing power and memory requirements and scalability, as well as some additional trusted hardware and software, which themselves need to be secured. Furthermore, having an IDS/IPS technology should not act as a replacement for secure design and development of space systems.
- Moreover, the remoteness and lack of physical access to space assets create some unique challenges. One such challenge arises from the need to perform software updates on space system components, e.g., satellite firmware updates. Unpatched software exposes space systems to attack vectors that are openly documented and available for exploitation. However, these updates can only be performed when the satellites are visible to ground stations and may require more than a single fly-by. Furthermore, a firmware update that may need to be delivered to multiple satellites, by beaming them to a single satellite across multiple passes over a ground station, and then that satellite transmitting them to other satellites requiring the same update. Software updates can introduce vulnerabilities, either inadvertently through a legitimate transmission of the update, or through an attacker using this circumstance to purposefully inject flaws into the space object [11]. For instance, in the case of the space probe Phobos 2 [12], a software update inadvertently caused the spacecraft to lose its lock on the Sun, which drained power and ceased communications. Techniques such as software attestation can enable the software to prove its identity thereby increasing its trustworthiness.
- Despite the challenges in dealing with remoteness, the software problems afflicting space objects are somewhat similar to those afflicting systems on the earth. These problems can be particularly pronounced in space systems, as security has not been incorporated into the design of space computing systems in the first place. Furthermore, there can be many components in space systems with legacy software, pre-dating the time security was considered important.

- When it comes to detecting malicious behaviour, an important issue is that of intent of an entity's actions. Often, when monitoring manoeuvres of foreign space objects, there is little information beyond what is being perceived with telescopes and radars. These observations might reveal the trajectory of the space object and some physical characteristics, but it can be difficult to determine the nature of a space object's mission without further information. This makes the assessment of intent even more challenging when it comes to the movement of space objects. In the absence of further additional information, there is only the official state policies of others on their space activities to provide the necessary context for what certain actions might mean. Such policy declarations are often general in nature and do not necessarily cover specific classes of activities, which adds uncertainty to the decision making.
- As many strategic military systems (such as missile systems) rely on space infrastructures for navigation and command and control, cyberattacks on space systems would undermine the integrity of strategic weapons systems and have the potential to obfuscate the originator of the attack. As cyber technologies are increasingly within the grasp of non-state actors, they create hitherto unparalleled opportunities for even small malicious groups to instigate high impact attacks. In fact, the asymmetricity in cyber is exasperated in the space domain, where offence is easier than defence, both technologically as well as geopolitically.

3.1 Specific Security Problems

We will now briefly outline some specific security aspects that present significant problems in the design and deployment of secure space systems.

- Lightweight Security Protocols
    - Most satellite communication protocols are designed to be lightweight to reduce power and memory requirements and to increase the speed of transmissions. Securing these protocols introduces an overhead into the communication stack, increasing power consumption and memory usage. Depending on the mission, this overhead may not be tolerable, so security and mission's needs must be weighed in the design and decision-making process to create an acceptable risk level for the mission.
    - Whilst there has been attempts to document and recommend certain communication protocols, there is no consensus in the space industry in how best to implement secure communications and authentication, or which missions warrant the need for higher or lower security requirements. Security is often added as an afterthought in the protocols used in space, and some current options utilizing existing terrestrial techniques may not be suitable for satellites. Even in satellite systems which use encryption, maintaining unencrypted connection for emergency situations such as satellite tumbling could be important. However, these communications would be in cleartext, able to be retrieved by eavesdropping on the connection.
    - Quantum technologies are likely to play an important role in secure communications in the future, for instance, when it comes to the distribution of keys used to encrypt terrestrial and satellite data. For instance, quantum entanglement technology can enable distribution of keys to ground stations at the same time. This is more secure than traditional RF or optical communications, where eavesdropping and spoofing can occur without the knowledge of the two parties trying to communicate. However,

challenges associated with the distance and system complexity still need to be overcome.

- Security Management
    - Scalability — Whilst it may be a straightforward task to manage security parameters such as keys of a single or small cluster of satellites, large satellite constellations require a large number of keys, making scalable key management an open issue. Constellations aiming to provide high data rates, such as broadband services, will also encompass a large network of ground stations, each of which having their own keys.
    - Group dynamics — Another design aspect relates to the dynamics of satellites entering and leaving a constellation. For the satellites entering and leaving the constellations, keys must be issued and revoked respectively for payload management and user interactions. The situation could become further complicated with the satellite neighbours needing to update their keys due to changes in the constellations. Issuing and revocation of keys need to be achieved in a secure and efficient manner to allow for changes in constellation group dynamics.
- Routing between Space Objects
    - The use of inter-satellite links (ISLs) provides communication routes which do not rely solely on ground infrastructure, but also give rise to questions over when, where, and how routes are calculated. A constellation operator must decide whether routes are static or dynamic, should be calculated on-demand or pre-computed, and implemented on a centralized, decentralized or distributed platform [13]. Each of these options has security implications. Centralized static routes offer fixed communication paths administered by a single authority, which may provide more control over the routes but is a single point of failure with fault tolerance and network congestion issues. Distributed on-demand routing splits computations among different nodes when required which increases fault tolerance. However, it also increases the attack surface of the routing procedure as more nodes are required and an attack may be easier to propagate through a network. Though there are several protocols for ISL routing offering both single and multi-layer constellations, more work is required to address aspects such as network resilience after satellite destruction, flexible space networking mechanisms and optimal ground segment coverage.
- Distributed control
    - As mentioned earlier, when it comes to large constellations, scalability is an ongoing challenge, not only for the space segment but also for the ground. The management of large constellations are likely to be distributed over several sites, requiring coordination between sites and handover from one to the next. This in turn also necessitates the need for establishing standardized ground station security practices.
- Fault tolerance
    - The space environment is a harsh one with severe thermal, radiation and vibration extremes which can affect satellite components. For instance, radiation can cause a change of state in components, leading to bits being flipped, and potentially damaging data stored on the satellites. This can lead to, for instance, keys stored on the satellite getting altered due to flipped bits and impacting secure communications (using encryption) between the satellites and the ground station. Hence new fault-tolerant based security mechanisms will be required to account for these types of challenges in the space environment.

- Security and positioning
    - With satellite constellations, it is important to ensure that the satellite one is communicating with is the one you think it is. A rogue satellite attempting to appear legitimate, whilst communicating with the ground or other satellites correctly, cannot occupy the same physical space of another legitimate satellite. Hence in addition to security mechanisms, satellite ranging, and positioning can be securely incorporated as part of verifying a satellite's identity.
- Open-source space components
    - The use of commercial-off-the-shelf (COTS) components in space systems provide increasing opportunities for malicious actors to alter components in the supply chain. Information on open-source components being publicly available gives an added advantage to an attacker in discovering security vulnerabilities. It is therefore paramount to establish the confidence in the supply chain and trust to ensure that satellites, ground stations and user devices are designed, built, and managed by parties who are held to high security standards.
- User applications
    - User applications provide new ways for users to interact with space systems and their services. Whether interacting directly with a receiver or accessing a service through software or web portals, several challenges arise on how to deliver these services in a secure manner. Authentication and authorization play a large part in securing such interactions. For instance, it is necessary to authenticate and authorize dedicated receivers accessing space services or data, rather than just relying on the access to the device itself. Similarly secure authentication and authorization need to be designed for software or web-based solutions accessing on-demand services to reconfigure payloads or direct satellites. There is a need for robust verification of user and device identities as well as the level of access based on their privileges, whilst minimally impacting usability.

4. Emerging Technology and Space Trends

New space services are emerging such as the AWS Ground Station, which is a fully managed service that allows users to control satellite communications, process data, and carry out operations from their desktops and laptops, without requiring the traditional ground station infrastructure (such as from a space agency). This implies that such services can be accessed by users from their desktops or laptops, from anywhere from the world. For instance, using the AWS ground station, the user can download data from satellites and store them in the AWS cloud, and then use applications in the AWS to do processing on the downloaded satellite data. As this gives access to space systems for distributed users from their own devices, there is a critical need to ensure secure access to such emerging space services and the associated operations. For instance, not only users and devices must be authenticated before accessing these services but also there is a need for secure authorization services that control the operations of the users on the space infrastructure and data. Furthermore, security mechanisms are needed to ensure that malicious payload is not uploaded infecting space systems as well as denial of service attacks.

Another major area of emerging interest is the softwarization and virtualization of space systems and ground station infrastructures. The use of software defined platforms will make space systems more

flexible by allowing programming of software to configure dynamically satellite functions to meet changes in demand, thereby helping to improve the efficiency of operations [14]. For instance, a software-defined payload can reconfigure the antenna beam on-demand by sending a new program in uplink communication. This can be used to vary the mission of satellite during its lifetime depending on demand dynamics. Software enabled satellite systems would make satellite systems more adaptable for counteracting jamming attacks by dynamically varying frequencies in jamming areas as well as making them more easily amenable for mobile applications providing coverage to moving targets such as aircraft or vessels or even to cover short temporary events (e.g., natural disasters and exceptional high demand for communication).

Softwarization of space systems is enabled using emerging technologies such as software defined networks (SDN) and network functions virtualization (NFV), providing programmability, flexibility, and modularity that are required to create multiple logical networks, each tailored for a given use case, on top of a common network. SDN and NFV technologies can be applied to both the ground and the space segments of the network infrastructure. Cyber security has a key role to play in these new technologies. For instance, secure smart software enabled satellites can better detect and defend against cyber threats autonomously and update on-board cyber defences to address new threats. They can also diagnose issues with greater precision and back each other up when needed, significantly enhancing resiliency. The virtualization technology with the hypervisor securely containerizing virtual machines helps to optimize memory, on-board processing, and network bandwidth. For instance, it enables the smart satellites to process more data in orbit thereby only transmitting the most critical and relevant information and saving bandwidth costs and reducing the burden on ground station. This will ultimately help to host future data centres and infrastructures in space. The novelty of software enabled space architectures is that it can provide end-to-end logically isolated network services supporting diverse use cases from multiple tenants, with independent control and management, and which can be created on demand over a common infrastructure. It can also support new network services on-board space platforms, with the capability to provide arbitrary per-flow logic and accommodate rapid topology changes in constellations. However, such softwarization of space will introduce a whole set of new security challenges, as security and trust are critical for the dynamic provision and management of space services and counteracting sophisticated security attacks against space systems [15,16].

Another important technology relevant for space is that of trustworthy autonomous space agents, collaborating with each other to realize overall system goals, carrying out a multitude of tasks, in a dynamic, adversarial, and contested setting. These agents should have the ability to dynamically learn from the environment. As they will be operating under contested environment, they should have mechanisms to protect themselves from attacks from other malicious space objects. They should be capable of making trustworthy decisions under uncertainty and adversarial threats as well as able to adapt to changes in the environment and behave in a goal directed manner involving different levels of forward planning to fulfill their mission [17,18].

Such trustworthy autonomous agents are needed in the establishment of future space facilities such as hosting and managing infrastructures in space stations (e.g., the moon) for further space exploration. They also form part of new generation smart satellites. For instance, such trustworthy autonomous satellites can be used to police routes in space and counteract attacks against space facilities from rogue space entities. The dedicated trustworthy autonomous space entities could even

help to constitute new space force for protecting space facilities. This can be seen as a natural extension to the current use of satellites in military conflicts. For instance, several countries (e.g., USA, Russia, and China) have launched numerous small satellites to support military functions over the last decade [19].

5. Response and Mitigation: Technological and Policy Solutions

It is clear that mitigating cyber threats in space require both technological as well as policy solutions. Though many of the technology solutions for terrestrial systems can be applicable for space infrastructures, as previously identified in Section 3, space creates certain unique cyber security challenges. Furthermore, as the threat environment is dynamic, the technological solutions also need to be dynamic and adapt to new threat situations. In addition to traditional security mechanisms counteracting attacks such as GPS spoofing and lightweight security protocols, new security architecture and solutions are required to cater for softwarization of space systems, advanced autonomous space agents and managed services enabling user access to space objects, and quantum-based security technologies, as outlined in Section 4. However, a comprehensive approach to effective response and mitigation requires a systematic and unified policy solution that can guide the technology efforts to protect space assets and services. There must be mechanisms for the enforcement of policies, which enable legitimate users and actions while increasing the costs for illegitimate users and their behaviours.

The policy solution needs to address several dimensions as new actors (state, non-state and commercial) and new technologies are expanding and transforming space activities. However, at the present, neither space policy nor cyber security policy is prepared for the challenges created by the meshing of space and cyberspace dramatically increasing the security risks. The commercialization of space with the market incentives to lower costs and entrepreneurial activities such as space tourism and asteroid mining, heighten cyber security concerns. There is also a growing development in the networks of small satellites and new satellite services for use in a range of applications such as agriculture, transportation, and environmental monitoring, producing valuable data, which can be targets for cybercrime and espionage.

The central premise of the policy solution is that it should reflect an end-to-end framework for cyber security, incorporating measures into all stages of space system development and operations. With the increasing reliance of the space sector on commercial technologies and the use of commercial off the shelf components, it is critical that polices should be established to enforce strict cybersecurity requirements for all components of space systems and their supply chains, spanning both civilian and military space assets and activities, for instance, considering the Cybersecurity Maturity Model Certification (CMMC), which has been introduced as a requirement for all defence contractors and providers, including small vendors [20] by the US Dept of Defence. There should also be a supply chain risk management program and software assurance methods within the software supply chain to reduce the likelihood of malware being inserted in components and modules. Enforcing strict cyber security standards in government contracts will help to promote the security of commercial products potentially leading to changes across the whole industry.

Another key concern for the policy framework is the need for appropriate regulations for the commercial space sector. With the growth in the range of space activities the private sector is

planning, the regulatory framework would provide commercial space enterprises with regulatory certainty while at the same time allow the states to comply with any of the existing space treaty obligations (such as the Outer Space Treaty [21]). It is critical that private parties are included in the discussions establishing the regulatory framework prioritizing industry led efforts strengthening cyber security and collaboration across different sectors in assessing what is non-negotiable versus acceptable risk. Furthermore, international cooperation and agreement with both traditional and non-traditional allies, including international space supply chain stakeholders, is vital for creating sustainable frameworks for mitigating risk in space in the long-term.

Cyber security skills are an important piece in the overall policy framework. A major challenge in securing space systems is the "systems of systems" aspects, requiring a deep understanding of how such systems work and the various threats and opportunities for the attackers to disrupt them. With space systems, expertise in both systems infrastructures such as servers, networks, and systems as well as knowledge of specialised space infrastructures such as ground control systems and satellites are needed. The policy framework should identify specific steps in developing professionals who have capabilities and expertise in both these areas.

Furthermore, the policy framework should have mechanisms and metrics to identify and assess whether the intended policy impacts are occurring. For instance, these include having mechanisms to measure whether the components being used to develop space systems have the required security capabilities, whether providers of space components follow the security guidelines in developing their products and services, whether there is an increase in the capacity of people with cyber and space skills, as well as whether the policy framework is recognized by the different commercial and state actors, and the policies themselves are explainable and auditable thereby enhancing accountability.

References

1. T.Harrison, K.Johnson, M.Young, "Defence against the Dark Arts in Space", Centre for Strategic and International Studies Report, Feb 2021.
2. G. Falco, Job One for Space Force: Space Asset Cybersecurity, Belfer Center for Science and International Affairs Harvard Kennedy School, 2018.
3. Australian Space Agency, Advancing Space: Australian Civil Space Strategy 2019-2028, Commonwealth of Australia, 2019; available at: https://www.space.gov.au
4. G. Baram and O.Wechsler, Cyber Threats to Space Systems, Joint Air & Space Power Conference 2020.
5. Kaspersky, Satellite Turla: APT Command and Control in the Sky, https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/
6. Ali Jafarnia-Jahromi et al., "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques, International Journal of Navigation and Observation", 2012 https://doi.org/10.1155/2012/127072
7. Andrew Dalton, "Russia Hopes to Block Cruise Missile Attacks with Cell Towers,'' Engadget, online paper, 17 Oct. 2016, https://www.engadget.com/2016/I0/17/russia-jamming-cruise-rnissile-attacks-with-cell-towers/, DW News, "Finland to probe reports of Russia disrupting GPS during NATO drill", https://www.dw.com/en/finland-to-probe-reports-of-russia-disrupting-gps-during-nato-drill/a-46253512

8. T. E Humphreys et al., “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In Proceedings of the Institute of Navigation GNSS (ION GNSS 2008), 2008.
9. S. Peterson, "Iran Hijacked US Drone, Says Iranian Engineer,'' The Christian Science Monitor, 15 Dec. 2011, https://www.csmonitor.com/World/ Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer
10. M.Manulis et al., “Cyber Security in New Space”, International Journal of Information Security, https://doi.org/10.1007/s10207-020-00503-w
11. B. Min, V. Varadharajan, et al., "Anti-Virus Security: Naked during Updates", Journal of Software: Practice and Experience, 2013.
12. E.V.Bell, “Phobos project information”, https://nssdc.gsfc.nasa.gov/planetary/phobos.html
13. L. Franck, G. Maral, “Routing in Networks of Intersatellite Links”, IEEE Trans. Aerospace Electronics Systems, Vol 38 (3), 902–917 (2002)
14. Lockheed, “Lockheed Unveils Software-Defined Satellite Tech”, https://blog.executivebiz.com/2019/03/lockheed-unveils-software-defined-satellite-tech-for-changing-missions-rick-ambrose-quoted/
15. V. Varadharajan, K. Karmakar, U. Tupakula, & M. Hitchens, “A Policy based Security Architecture for Software-Defined Networks”. IEEE Transactions on Information Forensics and Security. 14, 4, p. 897-912 16 p., Apr 2019
16. V Varadharajan, U Tupakula, "On the design and implementation of an integrated security architecture for cloud with improved resilience", IEEE Transactions on Cloud Computing 5 (3), 375-389, July 2017.
17. P.Theron, A.Kott, et al., “Towards an Active, Autonomous and Intelligent Cyber Defence of Military Systems: the NATO AICA Reference Architecture”, Proc of the International Conference on Military Communications and Information Systems, May 2018.
18. V.Varadharajan, “Challenges in the Design of Secure and Resilient Autonomous Systems”, Keynote Speech at the Self-Protecting Systems Workshop, IEEE International Conference on Autonomic Computing and Self-Organizing Systems, ACSOS 2021, Sept-Oct 2021.
19. Bryce Space and Technology: Smallsats by the Numbers 2022 Report, https://brycetech.com/reports
20. Office of the Under Secretary of Defence for Acquisition & Sustainment, “Cybersecurity Maturity Model Certification”, https://www.acq.osd.mil/cmmc/
21. United Nations office for Outer Space Affairs, “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies”, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

Vijay Varadharajan
Global Innovation Chair Professor and Chief Cyber Strategist
The University of Newcastle, Australia
vijay.varadharajan@newcastle.edu.au

26 March 2022
Version 1.0