The Cyber-Safe Gateway
Unlocking Scotland's Space Cybersecurity Potential

Dr Sharon Lemac-Vincere

University of Strathclyde Glasgow

https://doi.org/10.17868/strath.00090919

Abstract

The Cyber Safe Gateway: Unlocking Scotland's Space-Cyber Potential outlines a bold and transformative strategy for Scotland to seize leadership in the global space economy by focusing on one critical enabler: cybersecurity. With the global space economy projected to reach $1.8 trillion by 2040, and the rapid expansion of space-based infrastructure, securing these assets is not a future challenge but an urgent, present-day necessity. This report addresses head-on the existing skills shortages, underinvestment, and evolving threats that could undermine Scotland's ambitions in the space sector.

The skills gap in both space and cybersecurity is not a looming crisis but a pressing reality. Cybercriminals, state actors, and rogue entities are already targeting satellites, space stations, and communication networks. The vulnerabilities exposed by outdated, unsecured systems are too great to ignore, and the economic risks are immense. What is unique about this report is its integrated approach: *The Cyber Safe Gateway* does not just identify problems—it proposes concrete, actionable steps to align Scotland's strengths in cybersecurity, satellite manufacturing, fintech, and artificial intelligence with the needs of the global space economy.

Scotland has a unique window of opportunity. This report lays out how, by leveraging existing expertise, fostering cutting-edge innovation, and addressing the critical workforce shortfalls, Scotland can become a global leader in space cybersecurity. The stakes are incredibly high. The unchecked exploitation of space assets poses risks not just to Scotland but to global security and economic stability. Space systems underpin critical services, from global finance to communications, and a single cyberattack could have cascading effects that destabilise entire industries. This report argues that the only way forward is proactive, visionary leadership, with Scotland positioned to shape the future of secure space operations. Through immediate investment and long-term planning, *The Cyber Safe Gateway* suggests a path for Scotland to unlock its full potential, ensuring it is not just a participant but a leader in the new space race.

Forward

"Space cyber security is not just a technological challenge; it is the cornerstone of our future in space. By safeguarding our space assets, we secure our innovations, entrepreneurs, economies, and our way of life. As we venture into new frontiers, our resilience and preparedness will define our legacy". (Lemac-Vincere, 2024)

In a world that rarely pauses to consider the silent pulse of satellites and space systems orbiting above, the question of securing our space assets is no longer a matter of if, but how urgently we must act. This report, inspired by discussions from the inaugural Space Cyber Security Conference at the University of Strathclyde (May 2024), and interviews with experts in space and cybersecurity, highlights a topic both complex and deeply consequential.

Unlike the established field of terrestrial cybersecurity, space cybersecurity is still emerging, and therein lies both the challenge and the opportunity. The global space sector has expanded rapidly, fuelled by the relentless pace of technological innovation and the democratization of access to space. But with this progress comes an inevitable vulnerability. As our reliance on space-based assets increases, so does the risk of them becoming targets for those with motives we may not yet understand. In this sense, space cybersecurity is not about defending a single piece of technology—it is about securing an ecosystem that our interconnected lives now depend upon.

Scotland, with its growing satellite industry and spaceports in development, could take a leadership role in this essential new field. But this requires a new kind of thinking. While we can draw lessons from the evolution of cybersecurity on Earth, space presents a unique set of challenges. We are dealing with assets that are light-years beyond our immediate reach, systems that must be resilient enough to withstand not just today's threats but those of the future. In this context, Scotland has an opening to define standards, shape policies, and cultivate a workforce that is not only equipped to tackle known risks but is also adaptable to unforeseen ones.

A critical part of this task will be to break down the barriers that currently exist. Much of the language around cybersecurity and space is inaccessible, filled with jargon and complexities that can alienate potential collaborators, innovators, and investors. This is not a new issue but one that persists in both sectors (and a key concern from the conference at Strathclyde and the Space Cyber conference I held at the University of Lancaster in 2023). By prioritising and fostering a culture of open communication and cross-sector collaboration, Scotland can help bridge this gap. And in doing can create a more inclusive environment for tackling space cybersecurity challenges. It is not just about defending our systems, but about inspiring new ways of thinking and encouraging the diverse perspectives necessary to confront the unknown.

As we explore this new frontier, the path is far from straightforward. But Scotland's history of scientific discovery and its commitment to collaboration give it a solid foundation to build on. By taking bold, informed steps in space cybersecurity, Scotland can not only secure own future but also contribute to a global standard of resilience, one that other nations may look to as they navigate this uncharted terrain.

This report invites us to consider the role of space in our lives with a new sense of responsibility. It challenges us to think not just about innovation but about the security frameworks that must underpin it. This is not about building walls around our technologies, but about fostering a robust ecosystem capable of withstanding the complexities of the future. Scotland can shape this space, and by doing so, set a standard for others to follow. The risks are real, but so is the potential for impact—a legacy that Scotland can contribute to, a world increasingly defined by its reach beyond our atmosphere.

Vincere ad astra – to conquer the stars.

Dr Sharon Lemac-Vincere

PhD (Socio-Legal). MSc HRM, MSc (Crim), LLB (Hons), B.A (Coms)

Acknowledgements: Research, Conference, Global Voices, and Executives

Thank you to everyone who attended and contributed to the first Space Cybersecurity Conference at the University of Strathclyde in May 2024. Your participation was instrumental in making the event a success. A special thank you to those who took part in the follow-up research for this report—your time, insights, and perspectives have been invaluable. I would also like to thank all the presenters for generously sharing their expertise and knowledge, which added real value to the discussions.

- Craig Clark, Founder of AAC Clyde Space and Professor of Practice at the University of Strathclyde
- Wing Commander Jason Vaughan
- Dr Debra Carr, DASA Scotland
- Arthur Van Der Wees, Arthur's Legal Strategies and Systems
- Marc Knepper, DISC Canada
- Eric Alter, Marsh
- Nick Colosimo and Anthony Day: Co-Founder of Moonxcribe
- Allan Cannon: (Founder of Krucial)
- Professor Ivan Andonovic: University of Strathclyde and Lupovis
- Dr Andy Campbell (Scottish Space Network)
- Professor Massimo Vasile (University of Strathclyde)
- Dr Christie Maddock (University of Strathclyde)
- ESA
- Mr Gordon Merrylees (N4 Partners)
- Professor Nicolas Peters. International Space University

I would also like to thank all of those who took the time to make a short video for the 'Global Voices in Space Cybersecurity'. This video can be access by following this link: Cybersecurity in space international voices (youtube.com)

- Reece McAllister, Research on "The potential Space Cybersecurity challenges China poses to the UK, Isle of Man
- Chuck Brooks, Brooks Consulting, USA
- Carrie Hernandez, Rebel Space Tech., USA
- Arthur Van Der Wees, Arthur's Legal Strategies and Systems, Amsterdam
- Professor Vijay Varadharajan, Global Cybersecurity Chair, Newcastle University, Australia

- Stefanie Grundner, BSI Germany
- Dr Bianca Lins, Liechtenstein
- Marc Kneppers, DISC Canada
- Dr PJ Blount, Durham University
- Angoka: Cybersecurity company
- Hanjo Kahabka, Airbus, Germany
- Sascha Fankanel, Germany
- Manuel Hoffman, Germany
- Samuel S Visner, ISAC
- Bart Slowik, Syllab, USA
- NK2 Network, USA

Last but most definitely not least, **Professor Nicolas Peter,** interim President of the International Space University, my conference partner, and colleague. A big thank you to **Dr Heather Anderson** from the University of Strathclyde, my fantastic partner in '*space cyber-crime'*. Your support and collaboration were truly out of this world. I would also like to recognise the two brilliant students, **Susan Wotherspoon**, and **Tweedy**, who volunteered their time and energy for the two-day conference. Your contributions were like shooting stars, brightening up the event and making it a success. I would like to thank **Professor Neeraj Suri** for his continued support for my work in this field.

I would also like to congratulate the first Space Cybersecurity Executive graduates from the University of Strathclyde and the International Space University. They are amongst the first globally to have credentials in this emerging field a video of the course can be accessed here: Space Cyber Security (youtube.com)

Rebecca Meads	**Alan Blackwell**	**Jack Meadows**
Naomi Pryde	**Nick Damien**	**Ross Lang**
	Ross Hamilton	

Contents

Executive Summary

In today’s interconnected world, space and cybersecurity have transcended their origins as separate fields, merging to underpin critical global infrastructure. Scotland, uniquely positioned at this intersection, has an opportunity to redefine how nations approach space-cybersecurity—not as a static exercise, but as a domain that demands innovative thinking, dynamic disruption, and the entrepreneurial spirit, Scotland is well known for (Lemac-Vincere. 2024). Societies reliance on space-based assets to power essential services such as communication, navigation, and surveillance (Gov.UK, 2020; UK Parliament, 2021) means that the security of these systems is paramount. Yet, the rise of commercial off-the-shelf (COTS) technology throughout the space ecosystem has exposed these systems to new vulnerabilities, revealing just how inadequate a simple, compliance-based approach to security truly is (Aerospace, 2024; Varadharajan & Suri,2024, Baylon, 2014). Arguably it is time to move beyond the tick-box mentality and adopt a forward-thinking strategy (Nadi & Brooks, 2023) one which pressure-tests contemporary technology, pushes its capabilities, and ultimately fosters resilience.

As the demand for security innovation intensifies, the integration of advanced cybersecurity measures alongside technological advancements becomes especially relevant to Scotland's expanding space industry. With over 228 organisations contributing £298 million annually to the Scottish economy (Gov.UK, 2024), the sector is anchored by companies such as Alba Orbital, AAC Clyde Space, and Spire (SDI, 2024), positioning Scotland as a leader in small satellite manufacturing and Earth observation. Additionally, launch pioneers like Orbex and Skyrora are redefining space transportation, further solidifying Scotland’s influence in the global space sector. Despite these advancements, concerns have been raised about funding disparities that may leave critical gaps in cybersecurity provisions (Lemac-Vincere, 2024). Between 2017 and 2023, Scotland’s space sector received only 15.8% of UK Space Agency funding and 4.1% from the European Space Agency (Bates, 2024). While these funds support various aspects of space innovation, the limited share allocated to Scotland may not sufficiently address key areas like cybersecurity, which are essential for safeguarding the sector's innovation and progress. Without increased funding and more focused investment, particularly in cybersecurity, Scotland's space industry could face vulnerabilities that may undermine its potential for secure and sustainable growth.

The Evolving Threat Landscape

The global race for space dominance is intensifying, with major powers such as the United States, China, and Russia vying for control over space-based assets critical to global communications, navigation, and military operations. While the United States remains a key player, China is rapidly advancing its capabilities, particularly in quantum communications and satellite technology, positioning itself as a formidable competitor. Russia, meanwhile, has demonstrated its willingness to use cyber warfare, as seen in the 2022 Viasat attack during its invasion of Ukraine, where satellite communications were disrupted (Newman, 2024). Countries such as Japan and South Korea are also expanding their space programmes, driven by regional security concerns, while smaller nations like Luxembourg and Estonia are pioneering

space cybersecurity initiatives. Geopolitical tensions, combined with the increasing use of COTS technologies, have turned space infrastructure into a critical target for state and non-state actors, exposing vulnerabilities across the sector (Varadharajan & Suri, 2024; Baylon, 2014; Kavallieratos & Katsikas, 2023; Mueller et al., 2023). And traditional cybersecurity measures are proving inadequate in the face of growing threats. For example, the war in Ukraine, GPS jamming near Russia and Iranian-backed cyberattacks on satellite systems (BBC, 2024; Newman, 2024) show how hostile actors are already exploiting vulnerabilities. Beyond deliberate attacks, even unintentional failures in critical systems can have devastating effects. A stark illustration of this came in 2024, when a routine software update by cybersecurity firm CrowdStrike inadvertently caused widespread global disruptions (BBC, 2024). While unrelated to space systems, this update failure grounded airports, froze payment systems, and interrupted healthcare services—revealing how deeply interconnected and dependent our global infrastructure has become. This interdependence means that vulnerabilities and failures in space systems, which underpin so many essential services, could have far more severe consequences.

For Scotland, the growing global reliance on space infrastructure offers a clear and timely opportunity. With its strong heritage in satellite manufacturing, Scotland is already in a position of strength. This makes it well-placed to lead the development of "*secure by design*" satellites with advanced cybersecurity capabilities. By incorporating AI into these systems, Scotland can further enhance security through intelligent threat detection and rapid response mechanisms. Leveraging this expertise, Scotland can quickly establish itself as a global leader in this field. This not only protects its own space assets but also positions the country to shape the future of secure space infrastructure on an international scale. However, to sustain this leadership and fully capitalise on these opportunities, Scotland must also focus on preparing a skilled workforce equipped to handle the evolving challenges of space cybersecurity.

Preparing for the Future: Skills Development and Resilience

Scotland’s leadership in space cybersecurity will ultimately be defined by its ability to cultivate a skilled workforce ready to meet the challenges of tomorrow (DIST,2024; ISC2; WEF, 2023; UK Space Agency, 2023). Educational institutions like the University of Strathclyde, Glasgow Caledonian University, University of Edinburgh, and Heriot-Watt University are central to this effort, advancing research and training in critical areas such as AI, cryptography, and adaptive cybersecurity (Cyber Resilience Scotland, 2024). Through investment in education and workforce development, Scotland can build a new generation of cybersecurity experts capable of thinking outside the box and moving beyond static, conventional approaches to security. While cultivating a skilled cybersecurity workforce is crucial, Scotland must also ensure that this talent is supported by robust funding and collaborative efforts to drive innovation in the space sector.

Investment, Collaboration, and a Blueprint for Resilient Growth

Scotland’s space sector is strategically positioned to be a test bed for disruptive innovation, where cybersecurity is not a constraint, but a catalyst for growth.

However, dedicated funding for space-cyber initiatives is critical. The European Space Agency's funding models demonstrate the impact of targeted investment on resilience (ESA, 2024). Scotland must take a similar approach, forging public-private partnerships (Lemac-Vincere, 2024) that align cybersecurity with economic objectives, incentivising investment in technologies like quantum encryption and blockchain for secure space communications. Beyond traditional funding mechanisms, the insurance sector (Atler, 2024) also has a pivotal role to play in driving cybersecurity standards, with insurers increasingly requiring space ventures to demonstrate robust security measures. Scotland's insurance industry is well-positioned to develop products that encourage firms to embed cybersecurity deeply into their operations, fostering a secure and resilient space infrastructure (Kavallieratos & Katsikas, 2023).

Scotland's Opportunity to Lead in the Space-Cyber Frontier

By aligning financial incentives with robust security measures, Scotland can create a strong foundation for innovation in space cybersecurity and seize the opportunity to lead the global space-cyber revolution. By focusing on disruptive and secure technologies, Scotland is poised to set a new benchmark for resilience in the space sector. This ambition aligns with the United Nations Sustainable Development Goals (SDGs), particularly SDG 9 – Industry, Innovation, and Infrastructure, by promoting the development of resilient, cutting-edge infrastructure. Additionally, SDG 8 – Decent Work and Economic Growth, and SDG 17 – Partnerships for the Goals, support Scotland's efforts to foster international collaboration and ensure that its space-cyber initiatives are both technologically advanced and globally relevant.

But Scotland's vision can be even bigger!

As space becomes an increasingly contested and commercialised domain, Scotland has the chance to position itself not just as a protector of space assets, but as a pioneer of the next era of space exploration and innovation. The true opportunity lies in transforming cybersecurity into a driver of growth. By embedding AI, quantum encryption, and blockchain deeply into satellite infrastructure, Scotland can push the boundaries of what is possible—creating systems that are not only secure but also intelligent, adaptive, and self-healing.

This is not just about safeguarding assets—it's about *shaping the future*. Scotland can lead the way in making cybersecurity the cornerstone of space innovation, unlocking new commercial opportunities, fostering global partnerships, and setting the stage for the industries of tomorrow. The decisions made today will define the future of not just Scotland's space sector, but the global space economy. Scotland stands on the brink of a new frontier—where it can move beyond being a player to becoming the architect of the secure space ecosystem that future generations will rely on.

Purpose of the Report

This report delves into Scotland's unique potential at the intersection of space and cybersecurity. It explores the geopolitical, economic, and technological forces driving

these industries and provides strategic recommendations to position Scotland as a leader in the evolving space-cyber landscape. Arguably by building on its strengths—such as its thriving satellite industry, its research expertise, and its growing network of businesses—Scotland can protect its space assets while contributing to global security efforts. This would cement Scotland's status as a resilient, forward-looking space hub.

Key Sections of the Report

Chapter One: The Global Space Cybersecurity Landscape and Scotland's Role

This chapter discusses the global power dynamics in space cybersecurity, with a focus on the United States, Russia, China, and other emerging space players. It positions Scotland as a key player in Europe's space economy, highlighting its potential to lead in secure satellite production and Earth observation technologies while addressing cybersecurity risks.

Chapter Two: Space Cyber Diplomacy

This chapter highlights the urgent need for space cyber diplomacy as global competition in space intensifies. It calls for specialised diplomats to address the intersection of space and cybersecurity, prevent conflict, and foster cooperation, with recommendations for Scotland to lead in space cybersecurity and diplomacy.

Chapter Three: Space Cybersecurity Threat Landscape and its Strategic Importance for Scotland

This chapter explores the growing cybersecurity risks in the space sector as space assets become increasingly integrated with global networks. It highlights key vulnerabilities such as outdated software, supply chain weaknesses, and the risks of cyberattacks on satellites and ground stations. As Scotland's space industry expands, addressing these cybersecurity challenges is essential to safeguarding its infrastructure and ensuring continued global leadership.

Chapter Four: Investments- Securing Scotland's Future:

Details the current lack of dedicated funding for space cybersecurity in Scotland and compares it to proactive models like the European Space Agency's funding initiatives. The chapter recommends introducing targeted funding programs and public-private partnerships to enhance innovation and secure Scotland's place in the global space economy.

Chapter Five: Insurance – The Catalyst to Drive Commercial Behaviour:

Discusses the rising importance of insurance in driving cybersecurity practices in space ventures. Insurers are increasingly requiring space operators to demonstrate robust cybersecurity measures, which presents an opportunity for Scotland's insurance sector to develop tailored products and support the growth of secure space infrastructure.

Chapter Six: Future-Proofing Scotland's Space Sector: Overcoming the Skills Shortage

This chapter focuses on the skills shortage in both the space and cybersecurity sectors, particularly in areas such as AI, cryptography, and incident response. It emphasises the need for Scotland's educational institutions and industry partnerships to address these gaps, ensuring the workforce is equipped for future demands.

Chapter Seven: Future Proofing Space Cybersecurity in Scotland- Predictions

This chapter examines Scotland's unique role at the intersection of space and cybersecurity, exploring how the country can capitalise on emerging opportunities in space tourism, mining, finance, and transport, while addressing the evolving cyber risks that accompany them. The critical message is clear: space cybersecurity is not a passing concern but a fundamental element that will enable Scotland to lead and thrive in this new era.

Research Methodology

The research for this report builds on the findings of '*The Cyber-Safe Gateway: Positioning the UK as a Global Leader in Space Cybersecurity and Innovation'*, report by adapting its broader UK-wide insights specifically to Scotland's space sector. The methodology includes data collected from 40 experts at the Space: Securing our Entrepreneurial Future conference at the University of Strathclyde and interviews with 20 specialists in space technology, cybersecurity, and policy. These findings are further supported by government reports, industry data, and academic research.

While the national report provided a UK-wide perspective on space cybersecurity, this report narrows its focus to Scotland's unique role within this landscape. The report also highlights the reliance of Scotland's space industry on small and medium-sized enterprises (SMEs), which have been pivotal in driving innovation, particularly in satellite manufacturing.

This report identifies key areas where Scotland's space sector can enhance cybersecurity, leverage its strengths, and address vulnerabilities. By aligning its cybersecurity capabilities with its expertise in satellite production and space innovation, Scotland can secure its space assets, attract international collaboration, and establish itself as a global leader in secure space infrastructure.

Limitations of the Report

While this report provides valuable insights into the Scottish space and cybersecurity landscape, several limitations must be acknowledged:

1. Small Sample Size: The findings are based on a relatively small sample of expert opinions, which may not fully represent the broader space and cybersecurity landscape across Scotland or the UK.
2. Geographical Focus: This report focuses on Scotland's space sector and applies UK-wide insights to a regional context. While some conclusions may align with broader UK trends, the focus on Scotland may limit its applicability to other regions.

3. Awareness and Positivity Bias: Many participants in the research were already knowledgeable about space cybersecurity, which may have introduced some degree of positivity bias in their perspectives on the sector's potential and readiness to tackle cybersecurity challenges.

Conclusion

This report provides a recommendation for closing space cybersecurity gaps, fostering disruptive innovation, and ensuring that space and cyber technologies advance hand in hand. Through targeted investments, enhanced collaborations with international partners, and a focus on cyber resilience, Scotland could not only protect its space assets but also to lead the development of secure space infrastructure globally. Scotland's leadership in this dynamic environment will be defined by its ability to stay ahead of emerging threats and to foster innovation at the intersection of space and cyber. By acting decisively, Scotland can solidify its position as a resilient and forward-looking space hub and ensure that it contributes meaningfully to the future of both industries.

Introduction: The UK and Scotland’s Space Cybersecurity Landscape in 2024

The rapid growth of the UK’s space sector presents significant opportunities for economic development, scientific innovation, and national security (UK, Government 2023). However, it also introduces new vulnerabilities, particularly in the realm of cybersecurity. As space systems become increasingly integrated into critical national infrastructure, protecting these assets from cyber threats is becoming a top priority for the UK (MOD 2023, Gov.UK, 2024). This report explores the current state of the UK’s space cybersecurity posture, with a particular focus on Scotland, which plays a key role in the nation's space ambitions.

The UK’s National Space Strategy

The UK’s space sector has rapidly become a cornerstone of both the economy and national infrastructure, contributing £16.5 billion annually and supporting 18% of UK GDP (Gov.UK, 2024). From satellite communications and weather forecasting to national security operations, the sector plays an essential yet often hidden role in the fabric of modern life. Despite its long-standing importance, cybersecurity has only recently been recognised as a fundamental aspect of space sector resilience (MOD, 2022), as its integration with critical infrastructure grows. The UK Space Agency (UKSA), working in collaboration with the National Cyber Security Centre (NCSC), has been developing awareness of the safeguarding needs of both government and private space operations from increasingly sophisticated cyber threats.

This emphasis on cybersecurity aligns with the UK’s broader National Cyber Strategy 2022, which underscores the need to protect space infrastructure from cyberattacks that could disrupt essential services, compromise sensitive data, or threaten national security. As the UK’s space sector continues to grow at an annual rate of 5.1%, the importance of cybersecurity in safeguarding space-based systems cannot be overstated (UKSA, 2023). This growth also opens up a range of futuristic possibilities, from global broadband connecting remote areas to manufacturing pharmaceuticals and 3D-printing human organs in microgravity, which could revolutionise healthcare and reduce transplant waiting times (Gov, UK, 2024). But these possibilities will all be risk without a secure-by-design cybersecurity posture.

The UK’s ambitions for 2030, outlined in the National Space Strategy (2021), reflects a commitment to integrating space technology into everyday life, enhancing national resilience, and pushing the boundaries of what is possible. However, achieving this vision requires not only innovation but also strong partnerships between government and industry to address the cybersecurity challenges throughout the space ecosystem. Despite the progress made in enhancing space cybersecurity, critical gaps still exist that could undermine the UK’s efforts in this domain. The UK needs to be more ambitious at the intersection of space cybersecurity.

Challenges at the intersection of Space Cybersecurity

As the UK's space sector continues to expand, the cyber threat landscape grows more complex. In 2024, the National Cyber Security Centre (NCSC) reported a 50% increase in significant cyber incidents, with critical sectors like space receiving particular attention (NCSC, 2024). Satellite communications, GPS, and Earth observation systems—vital for both civilian and military operations—are increasingly becoming prime targets for adversaries. This growing threat has necessitated a closer alignment of space and defence cybersecurity, reflected in the UK's Defence Space Strategy, which emphasises the need to secure military space assets from both physical and cyber threats (MOD, 2023). In line with these efforts, UK Space Command successfully launched its first military satellite, *Tyche*, in 2024. This cutting-edge satellite is designed to provide crucial space-based intelligence, surveillance, and reconnaissance (ISR), reinforcing the UK's military space capabilities while highlighting the growing interdependence of space technology and national security (Gov.UK, 2024).

However, while these developments demonstrate significant progress, several critical challenges which could undermine the effectiveness of both the sector and its specific cyber initiatives. One of the most pressing concerns is the lack of a dedicated space-specific cybersecurity strategy. And a key issue which arises from this, is the fragmented approach to space cybersecurity, where different elements such as international cooperation, regulation, and spectrum management are addressed separately. For instance, while the Cyber Essentials Plus programme focuses on protecting SMEs from fundamental cyber threats, it is not designed to tackle the more complex state-sponsored attacks that increasingly target the space sector (UKSA, 2024). Similarly, while the Space Information Sharing and Analysis Centre (Space ISAC) collaboration (Space ISAC, 2024) provides valuable international intelligence sharing, its effectiveness could be compromised by geopolitical tensions. These tensions may hinder the flow of critical information, and there is also a risk that this intelligence may not reach SMEs in the sector quickly enough. Given these challenges, it is crucial to regularly assess how intelligence is being shared and utilised to ensure the entire sector—especially SMEs—is fully supported. A more cohesive approach that accounts for both geopolitical factors and the specific needs of smaller players in the industry will be necessary.

In addition, the regulatory framework provided by the Space Industry Act [2018] and the NIS Regulations (2018), while critical, remain insufficiently comprehensive for the space sector. These regulations tend to apply broader cybersecurity principles without tailoring them to the specific needs of space operations, which are subject to unique risks such as electromagnetic interference and satellite hijacking (UK Government, 2018). Although the Spectrum Statement (2023) emphasises the importance of protecting spectrum for space systems, there is no strong focus on the cybersecurity challenges associated with spectrum use in space in the statement (DIST, 2023). This gap is particularly concerning given that spectrum is a vital component of satellite control and data transmission, and disruptions in this area could have significant repercussions on national security and public services.

Another critical challenge is the skills shortage in the space cybersecurity sector. While the Cyber Security and Resilience Bill mandates increased reporting and

proactive measures to enhance cybersecurity across various sectors, there is a recognised gap in the availability of skilled professionals capable of addressing these emerging threats. The shortage of specialised talent in both space and cybersecurity fields means that the UK may struggle to implement the advanced security measures required to protect its growing space sector (DIST, 2024). Without sufficient investment in education, training, and workforce development, the UK risks falling behind in the race to secure its space infrastructure against increasingly sophisticated cyberattacks (UKSA, 2024).

Furthermore, the evolving nature of cyber threats compounds these challenges. As technologies such as quantum computing and artificial intelligence continue to develop, the space sector will face new types of cyberattacks that current systems are unlikely to be equipped to handle (UKSA, 2024). The growing reliance on space-based systems for critical services, including communications, navigation, and defence, makes it essential for the UK to adopt a proactive approach to addressing these future threats. However, current cybersecurity measures, including those outlined in the Cyber Security and Resilience Bill, may not be sufficient to mitigate the risks posed by these advanced technologies.

As such, while the UK has made strides in enhancing its cybersecurity measures for the space sector, significant gaps remain. The fragmented nature of current strategies, combined with a lack of space-specific regulations, insufficient funding, and a shortage of skilled personnel, leaves the sector vulnerable to increasingly complex cyber threats. A more integrated, robust, and forward-thinking approach is required to ensure the resilience of the UK’s space infrastructure in the face of both current and future challenges.

Scotland’s Strategic Role in UK Space Cybersecurity

As the UK strives to assert itself as a global leader in space innovations, Scotland has emerged as a critical player in this national effort. With the rapid development of strategic spaceport projects, including Space Hub Sutherland and SaxaVord Spaceport, alongside Glasgow’s reputation as Europe’s leading producer of small satellites, Scotland’s contribution to the UK’s space industry has never been more significant. This growth aligns with the UK’s ambition to capture 10% of the global space market by 2030, positioning Scotland as a hub of technological advancement and innovation (SDI, 2023).

However, alongside these advancements comes an evolving cyber threat landscape. The growing reliance on space-based infrastructure, which includes satellite communications, GPS, and Earth observation systems, has made space assets prime targets for cyberattacks. These assets, essential for both civilian and military applications, face unprecedented risks from increasingly sophisticated adversaries. In 2024 alone, the National Cyber Security Centre (NCSC) reported a 50% increase in significant cyber incidents, with the space sector being identified as one of the critical targets (NCSC, 2024).

Given Scotland's pivotal role in the UK’s space ambitions, it is clear that the region will need to enhance its focus on cybersecurity to protect both national and global interests. While efforts like the Cyber Essentials Plus programme have extended to

Scottish space SMEs, further coordinated action is required to address the unique challenges that space operations face in the cyber domain (UKSA, 2024). Moreover, as quantum computing and AI-driven threats loom on the horizon, a comprehensive, space-specific cybersecurity strategy is essential to safeguarding the UK's space infrastructure.

This report aims to provide an in-depth analysis of the current state of cybersecurity in the UK space sector, with a particular focus on Scotland's role and the emerging challenges that must be addressed to ensure resilience against evolving cyber threats. The report will also highlight key recommendations for integrating cybersecurity initiatives more effectively across the UK space sector, with Scotland poised to take a leadership role in this critical area.

Conclusion

The UK's space sector is at a critical juncture, where its future success depends on its ability to safeguard its assets from evolving cyber threats. Scotland's contributions to this effort are substantial, not only in terms of economic growth but also in the realm of national security. By integrating robust cybersecurity measures across all aspects of space operations—from satellite launches to data transmission—the UK, and Scotland in particular, can ensure resilience in the face of emerging threats. Collaborative efforts between government agencies, the private sector, and international partners will be essential to securing the UK's position as a leader in the global space economy.

Chapter One: The Global Space Cybersecurity Landscape –Scotland's Role

This chapter examines the key activities of nation-states and private entities in space cybersecurity. As geopolitical tensions rise, the convergence of space and cyber domains introduces both opportunities and risks. The chapter explores how global powers like the United States, China, Russia, and emerging space nations are navigating these dynamics, alongside the strategic interests of private companies. These developments highlight the need for cohesive international standards to safeguard space assets. By strengthening partnerships and boosting cyber resilience, Scotland can secure its assets and play a pivotal role in future space security.

Geopolitical Challenges in the Convergence of Space and Cybersecurity

The convergence of space and cybersecurity presents a multifaceted geopolitical challenge, with implications extending across national security, economic resilience, and civilian infrastructure. Modern societies rely on space-based systems, but these systems are increasingly vulnerable to sophisticated cyber threats (Salim et al., 2024; Manulis et al., 2021; Thangavel et al., 2022; Racionero-Garcia & Shaikh, 2024; Bailey, 2020). The dual-use nature of many space assets, serving both civilian and defence functions, further complicates the landscape, making it difficult to delineate protections and responsibilities (BAE, 2024; Kavallieratos & Katsikas, 2023; Balleste, 2021; Varadharajan & Suri, 2024; Baylon, 2014).

Historical incidents highlight these vulnerabilities.

In 1998, a cyber intrusion into NASA's Goddard Space Flight Centre led to the loss of Germany's ROSAT satellite, while the Tamil Tigers targeted satellite communications in the early 2000s, revealing the potential of space systems as strategic targets (Li, 2023; Kavallieratos & Katsikas, 2023). More recently, the 2022 cyberattack on Viasat's KA-SAT network, which disrupted communications during Russia's invasion of Ukraine, demonstrated the capacity of cyber tactics to impact both military operations and civilian connectivity on a large scale (Werner, 2024).

This landscape is further complicated by the dual motivations of nation-states. On the one hand, they seek to secure their own space assets, recognising that a stable space environment is critical for both national and global security. On the other hand, many states are actively developing offensive cyber capabilities to exploit vulnerabilities in their adversaries' space infrastructure. This strategic tension creates a paradox: while collective security efforts would bolster resilience against cyber threats, they would also constrain the offensive capabilities that some nations deem essential for military and strategic advantage. The fragmented global response reflects these varied national strategies and a fundamental competition for influence.

There is a clear opportunity for nations to assert power by setting global standards for space cybersecurity. Leading states can shape the rules governing space—a

domain integral to global infrastructure and communication—by establishing and promoting their own norms and protocols. This race to influence standards and policies further fuels rivalry among major powers (Bailey, 2020; Racionero-Garcia & Shaikh, 2024; Fidler, 2018), with significant geopolitical ramifications. As nations seek to balance civil, defence, and economic priorities, they are acutely aware of the power that comes with shaping the frameworks within which all other nations must operate.

As state and non-state actors continue to exploit cyber vulnerabilities in space, the fragmented approach highlights a critical vulnerability in the geopolitical landscape. Achieving resilient defences requires comprehensive international collaboration. However, without globally coordinated policies and enforceable frameworks, the collective response to space cyber threats remains insufficient, leaving a domain central to global stability open to potentially catastrophic disruptions. For Scotland, a burgeoning player in Europe's space economy, understanding the broader geopolitical landscape and regulatory framework is critical to securing its space assets and defining its role on the global stage (see Appendix 1 for more details).

International Standards and Cooperation: Addressing Gaps in Space Cybersecurity

In response to these geopolitical tensions, international standards play a crucial role in harmonising cybersecurity practices across nations. The ISO/IEC 27001 (2013) for Information Security Management, ISO/IEC 27032 (2012) for Cybersecurity guidelines, and ISO/IEC 27017 (2015) for Cloud Security guidelines are widely recognised frameworks that influence national regulations and industry practices. These standards establish a foundation for management systems, yet compliance remains voluntary, leading to inconsistencies in application. The International Telecommunication Union (ITU) regulates satellite communications and ensures the secure use of the radio-frequency spectrum, but it lacks binding enforcement mechanisms. Similarly, the European Cooperation for Space Standardisation (ECSS, 2015) provides key standards like ECSS-Q-ST-80C for software product assurance and ECSS-E-ST-50-14C for space data links security. While crucial for safeguarding space systems, these standards face challenges in achieving widespread adoption.

The Outer Space Treaty (1967) and the Moon Agreement (1984) represent foundational international treaties aimed at promoting peaceful exploration and preventing militarisation. However, these treaties do not address modern cybersecurity challenges. The Outer Space Treaty prohibits the placement of weapons of mass destruction in orbit, but it does not prevent the deployment of conventional or cyber weapons (United Nations, 1967). This loophole leaves space assets vulnerable to exploitation by state actors, particularly in the absence of updated regulations that reflect the digital threats now inherent to space systems.

The strategic tension between major space-faring nations further complicates the development of a cohesive global framework. For instance, while the United States has supported UN General Assembly Resolution A/RES/75/36, which promotes reducing space threats through norms of responsible behaviour, has consistently opposed other resolutions aimed at preventing an arms race in space, such as

A/RES/75/35, A/RES/75/37, and A/RES/75/69 (Parliament UK, 2021; Pobjie & Ortega, 2024). The U.S. prefers voluntary, non-binding approaches to space security, focusing on transparency and confidence-building measures rather than legally binding arms control treaties. In contrast, Russia and China have been strong advocates for treaties aimed at preventing the weaponisation of space, such as the Prevention of an Arms Race in Outer Space (PAROS) and their proposed Prevention of the Placement of Weapons in Outer Space Treaty (PPWT). However, both nations have been criticised for their own counterspace activities, including the development and testing of anti-satellite (ASAT) weapons, which undermine their calls for arms control in space (Pobjie & Ortega, 2024). In this fragmented landscape, international cooperation is essential for developing robust cybersecurity defences. Frameworks like those set by the ITU and ECSS offer technical guidance, but without binding enforcement, they rely on voluntary adoption. The lack of a comprehensive international law specifically addressing cybersecurity in space operations compounds the challenge, leaving space assets exposed to attacks. This vulnerability was exemplified by the 2019 alleged cybercrime involving the International Space Station, highlighting the complexities of addressing cybersecurity within existing legal frameworks (Space.com, 2019).

To bridge these gaps, nations must engage in meaningful collaboration to develop enforceable standards that address the unique risks of space cybersecurity. Regional cooperation, such as within the European Union, offers a model for harmonising standards across borders. However, without global consensus, the security of space assets will remain at the mercy of individual state policies and national interests. For Scotland, embedding itself within these international frameworks is essential not only for securing its own space sector but also for contributing to the broader stability of the global space economy. Below is a summary of various nation states' space cyber approaches; it is not exhaustive and does not cover all nation states.

The United States: Strategic Approach and Critical Gaps in Space Cybersecurity

> As the United States has transitioned from government-driven space exploration to a model that increasingly relies on private sector innovation, it has encountered new cybersecurity challenges. The Commercial Space Launch Act [1984] and the Commercial Space Launch Competitiveness Act [2015] established a regulatory framework that encourages private investment, supporting the U.S. ambition to remain competitive in a rapidly expanding global space market (U.S. Congress, 1984; U.S. Congress, 2015). However, this shift has also introduced complexities, as many commercial entities lack the military-grade cybersecurity standards essential for national security operations (Erwin, 2024; Lemac-Vincere, 2024).
>
> To address these security concerns, the National Institute of Standards and Technology (NIST) created the SP 800-53 framework, outlining voluntary privacy and security controls for federal systems (NIST, 2013). In 2023, NIST released Interagency Report (IR) 8270, extending its Cybersecurity Framework (CSF) specifically to commercial satellite operations, establishing best practices for managing cyber risks in the space domain. However, these

guidelines are non-mandatory, leading to variability in adherence and thus inconsistent cybersecurity measures across private entities responsible for critical infrastructure (NIST, 2023; Werner, 2024).

The Space Policy Directive-5 (SPD-5), issued in 2020, further reflects the reliance on voluntary cybersecurity measures. SPD-5 encourages the integration of cybersecurity-informed engineering and resilience practices but stops short of mandating compliance. This has raised concerns about the adequacy of voluntary standards in defending against state-sponsored cyber threats, as the lack of enforceability could leave essential systems vulnerable (DSD, 2020). The voluntary nature of these policies underscores a fundamental challenge: private sector operators may lack the resources or incentives to prioritise cybersecurity investments, particularly when cost competition and market pressures are in play (Werner, 2024).

In addition to these policy frameworks, the U.S. military has taken steps to enhance space cybersecurity with the establishment of the U.S. Space Force's Space Delta 6, which is responsible for defending military satellites against cyberattacks. Within Space Delta 6, specialised squadrons protect vital satellite communications supporting missile warning systems and launch operations (Werner, 2024). However, the decentralised nature of U.S. space cybersecurity was highlighted during the 2022 cyberattack on Viasat's KA-SAT network. When the incident occurred, Viasat had to engage the National Security Agency (NSA) to coordinate response efforts, revealing a fragmented response framework and an absence of a dedicated central agency to handle cyber incidents comprehensively (Poirier, 2024).

The Commercial Augmentation Space Reserve (CASR), launched in 2024, reflects an attempt to integrate commercial satellite technologies into defence operations, aiming to bolster resilience by diversifying resources. However, CASR's reliance on commercial providers introduces additional risks, as commercial entities may not meet the rigorous cybersecurity requirements expected in military contexts. Responding to these vulnerabilities, Congressmen Maxwell Alejandro Frost and Don Beyer proposed the Spacecraft Cybersecurity Act, which mandates that NASA embed cybersecurity protections from the initial design stages. This legislation is supported by the 2024 Government Accountability Office (GAO) report, which highlighted that NASA's design-phase cybersecurity weaknesses could potentially jeopardise mission success and compromise national security interests (Lemac-Vincere, 2024).

Further illustrating the complexity of integrating commercial and military requirements, the U.S. Army completed a pilot project with Intelsat and SES in 2024, exploring the potential of outsourcing satellite communications as a managed service model. This project demonstrated the flexibility and efficiency of managed services but also underscored the challenges of aligning military needs with commercial capabilities. As Intelsat's David Broadbent observed, the pilot program exposed inefficiencies in the current military satcom procurement model, which is highly fragmented and often lacks agility. Feedback from the Army highlighted a preference for greater

control over budgeting and procurement, reflecting the broader issue of synchronising military requirements with commercial offerings (Broadbent, 2024; Leader, 2024).

Despite these initiatives, the U.S. strategy reflects a persistent tension between promoting private sector innovation and safeguarding national security. The reliance on voluntary standards and the ad hoc nature of current incident response mechanisms reveals critical vulnerabilities in the U.S. space cybersecurity framework. Moreover, the absence of a unified cybersecurity mandate across military and commercial sectors suggests that vital infrastructure could remain exposed to sophisticated state-sponsored threats. As the U.S. seeks to shape international norms for space cybersecurity, the effectiveness of its own policies and practices will play a pivotal role in securing both national security and global stability in the space domain (Werner, 2024; Poirier, 2024).

Canada and the Arctic: A Critical Space Frontier

Canada occupies a critical position in the global space landscape, particularly through its contributions to Arctic surveillance and satellite communications. The formation of the National Space Council in 2024 demonstrates the Canadian government's commitment to advancing its space capabilities while prioritising cybersecurity. Key space assets, such as the RADARSAT Constellation for Arctic monitoring and Canadarm3 for NASA's Lunar Gateway, are essential to national security, making cybersecurity fundamental to protecting these systems from growing threats posed by state and non-state actors.

The RADARSAT Constellation, which provides crucial Earth observation data for environmental and military purposes, underpins Canada's reliance on space infrastructure. As climate change opens new Arctic shipping routes, the region has become a geopolitical hotspot, with countries like Russia and China seeking to expand their influence. This raises the stakes for Canadian space assets, exposing them to risks such as cyber intrusions that could disrupt surveillance capabilities or compromise sensitive data (Babikian & Nesheiwat, 2024). China's ambitions to become a "*polar great power*" by 2030 further heighten these risks (Byres, 2024).

In response, Canada has enacted legislation like Bill C-26, the Critical Cyber Systems Protection Act (CCSPA), which mandates enhanced cybersecurity across vital sectors, including space. This law establishes a framework for cyber resilience applicable to satellites, ground control systems, and other critical space infrastructure, reinforcing Canada's strategic interests in the Arctic and beyond (Public Safety Canada, 2022). Additionally, Canada's $8.6 million investment in the Lunar Exploration Accelerator Program (LEAP) underscores its commitment to space innovation but also brings new cybersecurity challenges, particularly in its participation in international projects like the Lunar Gateway (Mortillaro, 2024). As Canada expands its role in space, robust cybersecurity measures are essential to safeguard its sovereignty, secure its contributions to international space initiatives, and

protect its national interests. By embedding cybersecurity into its space strategy, Canada is positioning itself to address emerging threats in an increasingly contested and geopolitically strategic domain.

Latin America: Space Ambitions and Cybersecurity Challenges

Latin America, led by Brazil, Argentina, and the Dominican Republic, is establishing itself as a notable presence in the global space sector. However, these advancements expose the region to significant cybersecurity vulnerabilities, largely due to fragmented governance and limited investment in robust cyber defences. **Brazil**, with its Alcântara Space Centre, has been a regional leader in space initiatives. However, it faces persistent cybersecurity challenges, with cybercrime costing the nation approximately $8 billion annually. The Brazilian Cyber Defense Command is tasked with federal cybersecurity, but its capacity to protect civilian space assets remains limited, leaving critical infrastructure exposed to both state-sponsored and criminal threats (Lavinder, 2016).

Argentina, meanwhile, has invested in Earth observation satellites for environmental monitoring, exemplified by the SAOCOM satellite programme. While these assets are valuable for disaster response and agricultural planning, they are also prime targets for cyber espionage. Argentina's collaboration with China on projects like the Espacio Lejano ground station raises additional security concerns, as Argentina has limited oversight of this facility, which may compromise data sovereignty and control over critical infrastructure (López & Cerda, 2024). This reliance on foreign partnerships illustrates a broader issue in Latin America's space initiatives: while these collaborations can accelerate technological capabilities, they also risk ceding control over strategic assets to nations with differing security priorities.

The **Dominican Republic** has recently joined the Artemis Accords, a significant step towards international cooperation in space. This development aligns with its ambitions to build a commercial spaceport in the Oviedo region, which would provide near-equatorial launch access, ideal for cost-effective space operations (Foust, 2024) with limited cybersecurity frameworks, the Dominican Republic's expanding space infrastructure could become an attractive target for cyberattacks, especially if the spaceport is used for dual civilian and military purposes (Rainbow, 2024). The rapid pace of these developments could outstrip the country's ability to establish effective cyber defences, exposing its infrastructure to risks from sophisticated cyber adversaries.

Latin America's approach to cybersecurity is further complicated by economic and political constraints. Many nations in the region face competing budget priorities, and political instability often disrupts long-term investments in cybersecurity. The Inter-American Development Bank (IDB) and Organization of American States (OAS) have sought to improve regional cybersecurity capacity, but the impact of these efforts has been limited, with comprehensive strategies yet to be fully adopted across the region (Lavinder, 2016). This lack of unified governance not only hinders individual nations but also weakens

Latin America's collective cyber resilience, making it a focal point for global powers interested in influencing the region's strategic direction.

As geopolitical interest in Latin America's space sector grows, the need for cohesive, region-wide cybersecurity measures becomes increasingly urgent. Both the United States and China are expanding their influence in the region, often through technological partnerships that can introduce vulnerabilities. For example, the U.S.-led Artemis Accords align Latin American signatories with Western space norms, countering Chinese partnerships like those seen in Argentina and Bolivia. However, without a strategic cybersecurity framework, Latin American nations risk becoming collateral in larger geopolitical conflicts, with their space assets potentially leveraged by external powers for surveillance, cyber intrusions, or counterspace operations (López & Cerda, 2024).

Thus, while Latin America's space ambitions are advancing, the region's cybersecurity frameworks must keep pace to protect national interests. Developing a unified, regionally coordinated strategy is essential to secure emerging space infrastructure and to mitigate the risks posed by increasing global interest in the region. Latin American countries would benefit from prioritising cybersecurity within their space agendas, fostering public-private partnerships, and establishing stricter control over technology transfers to ensure that national security is preserved as they expand their role in the global space economy.

South Korea, Japan, and Taiwan: Asia's Rising Space Powers

Asia, South Korea, Japan, and Taiwan are emerging as significant space powers, each facing unique geopolitical pressures that shape their approach to cybersecurity.

Republic of Korea (ROK) has rapidly expanded its space sector (Foust, 2024), with the launch of the KASA space agency (Jone, 2024) developing satellites for both civilian and military purposes but faces constant cyber threats from North Korea. As South Korea moves to enhance its space infrastructure, its collaboration with the United States and Europe on space cybersecurity becomes increasingly important. And its cyber posture, has been updated, with the launch of the National Cybersecurity Strategy (2024) (Wood, 2024). The strategy marks a significant change in direction, moving from a defensive to offensive posture. The strategy also names North Korea as its biggest threat. In 2023 North Korea launched an estimated 1.3 million cyberattacks per day on ROK public institutions (Wood, 2024).

Japan, a leader in space innovation, has integrated cybersecurity into its basic space law, Space Activities Act [2016] and Basic Cybersecurity Act [2014] provide a regulatory framework for national security measures, reflecting its commitment to secure its space infrastructure considering regional tensions with China and North Korea. Japan also aligns with international frameworks including those influenced by NIST. Japan's focus on quantum technologies and advanced encryption places it at the forefront of

global efforts to protect space systems. Japan has also invested in training in cybersecurity in space. However, Japan faces challenges in balancing its regulatory framework with needs to foster innovation and international collaborations.

Taiwan

Taiwan, while not a major space power, plays a critical role in the global supply chain for space technologies, particularly through its production of semiconductors by Taiwan Semiconductor Manufacturing Company (TSMC). These semiconductors are essential for a wide range of space applications, making Taiwan's technology sector vital to the global space ecosystem (TSMC, 2023). However, Taiwan's unique geostrategic position and its technological leadership expose it to significant cybersecurity risks, particularly due to the ongoing geopolitical tensions with China.

China's ambitions to dominate global technology markets, combined with its efforts to exert control over Taiwan, make Taiwan's space and technology sectors frequent targets for cyberattacks. Taiwan faces an alarming volume of cyber threats, with reports estimating that Taiwanese government agencies endure up to five million cyberattacks per day. In the first half of 2023 alone, Taiwan detected an average of 15,000 cyberattacks per second, including various intrusion attempts aimed at critical infrastructure, including its semiconductor production (Atlantic Council, 2024).

Given the integral role that Taiwan's semiconductor industry plays in the global space technology supply chain, these cyberattacks present a significant vulnerability. Any disruption to Taiwan's semiconductor production due to cyber incidents could have far-reaching consequences, impacting not only Taiwan's national security but also the stability of the global technology and space industries (Atlantic Council, 2024).

Taiwan's geopolitical tensions with China further amplify this risk, as China continues to use cyber tactics as part of its broader strategy to undermine Taiwan's security and weaken its competitive position in global markets (Lee, 2023). As space technology increasingly relies on semiconductor innovations, Taiwan remains a critical yet vulnerable link in the global space ecosystem.

To mitigate these risks, Taiwan has adopted several cybersecurity measures, including promoting the U.S. Department of Defense's Cybersecurity Maturity Model Certification (CMMC) framework. This initiative helps local industries, particularly those tied to defense and space technology, enhance their cybersecurity practices and protect themselves from advanced cyber threats, particularly those posed by state-sponsored actors like China (MODA, 2023).

China: Strategic Expansion in Space Cybersecurity

China's approach to space cybersecurity reflects its ambition to become a dominant force in space. This strategy emphasises self-reliance, dual-use capabilities, and a regulatory framework designed to secure its space infrastructure against external threats. Since the 1970s, China has methodically built its space capabilities, now positioning itself as a major player on the global stage with sophisticated cyber capabilities integrated across its space assets (Harrison et al., 2019; Aerospace, 2018). Recent advancements underscore China's commitment to securing its space infrastructure from potential cyber threats, particularly as it competes with western initiatives.

Dual-Use Space Infrastructure and Cybersecurity Implications

China's space program is characterised by dual-use technologies, enabling it to secure both civilian and military objectives. The BeiDou Navigation Satellite System serves as a prominent example, granting China independent global navigation capabilities, thereby reducing its reliance on the U.S.-operated GPS. This self-reliance extends to China's Gaofen and Thousand Sails constellations, which provide high-resolution Earth observation and broadband communications respectively, both of which have substantial cyber defence implications (The People's Republic of China, 2021).

The October 15, 2024, launch of Gaofen-12 (05), for example, integrates high-resolution imaging that supports surveillance and reconnaissance, while the Thousand Sails constellation, aimed at deploying 14,000 satellites, reflects an effort to establish a robust, autonomous communications network. These constellations facilitate secure data transmission, with capabilities designed to resist foreign interference. The Chinese Cybersecurity Law [2017] and Data Security Law [2021] mandate strict controls over these systems, emphasising data localisation and critical infrastructure protection, which underscores China's intention to shield its space assets from cyber intrusions (KPMG, 2024).

Counterspace Capabilities and Offensive Cyber Operations

China's advancements in counterspace technology further illustrate its focus on space cybersecurity. The 2007 anti-satellite (ASAT) test, which destroyed one of its own defunct satellites, was a clear demonstration of China's ability to engage in both physical and cyber-enabled counterspace operations (Weeden, 2019). Moreover, reports of Chinese cyber units targeting U.S. satellites, including incidents of interference from 2007 to 2008, underscore its willingness to engage in cyber offensives targeting critical space infrastructure (BBC, 2011).

China has continued to develop these capabilities with the goal of disrupting or neutralising adversarial satellites. Recent research from Chinese scientists suggests advancements in simulating nuclear blasts against satellites, a capability that could potentially disable Western constellations like Starlink (Chen, 2022a; Chen, 2022b). This development aligns with the People's

Liberation Army (PLA) doctrine on “destruction warfare,” which prioritises the disruption of enemy infrastructure, with space and cyber assets playing pivotal roles in executing this strategy (Demarest, 2023).

Integration of Emerging Technologies in Cybersecurity

In pursuit of enhanced space cybersecurity, China has invested in advanced technologies such as quantum communication and artificial intelligence (AI). The 2016 launch of the Mozi Quantum Communication Satellite, which uses quantum key distribution (QKD) for secure communications, demonstrates China’s commitment to next-generation cybersecurity measures that limit the potential for interception (Pan et al., 2017). Additionally, the integration of AI into China’s space infrastructure facilitates autonomous threat detection and response capabilities, enabling satellites to adjust their operations in real-time when encountering potential cyber threats (Ji et al., 2021).

These technological advancements allow China to strengthen the cybersecurity of its space assets, reinforcing its autonomy in data security and limiting vulnerability to external cyber threats. As China’s space programs continue to incorporate quantum and AI capabilities, it sets a precedent for secure communication and advanced threat mitigation, positioning itself as a leader in space cybersecurity innovation.

Implications for Global Space Governance and Cybersecurity Standards

China’s increasing focus on space cybersecurity also influences global cybersecurity standards. While it has been largely excluded from Western-led standard-setting initiatives, China is actively promoting its own regulatory models through domestic legislation and international forums, such as the IEEE SA P3349—Space System Cybersecurity Working Group (Vecellio Segate, 2024). China’s cybersecurity laws emphasise data localisation and infrastructure control, potentially reshaping global norms as other countries assess China’s model for securing critical infrastructure.

However, China’s lack of transparency and its integration of military objectives into ostensibly civilian projects raise concerns among other spacefaring nations. U.S. military leaders have expressed alarm over the potential for conflict, with U.S. Space Command describing space as a “*potential flashpoin*t” due to China’s rapidly expanding capabilities and lack of international collaboration (Associated Press, 2022). The strategic dual-use nature of China’s space program, along with its growing influence in setting cybersecurity standards, challenges the prevailing norms in space governance, contributing to a more fragmented and competitive landscape.

In summary, China’s space cybersecurity strategy is characterised by a focus on self-reliance, integration of dual-use technologies, and the development of advanced capabilities such as quantum communications and AI-driven threat detection. As China continues to secure its space assets against external cyber threats, it is likely to further influence global space governance, potentially leading to increased polarisation in cybersecurity standards and

practices. This evolving landscape underscores the need for international cooperation and updated regulatory frameworks to address the cybersecurity challenges posed by the increasing militarisation and complexity of space infrastructure.

India

India initially scoped out a draft Space Activities Bill (2017) which aimed to regulate the country's space activities comprehensively. However, this bill has since lapsed and the" country has now developed the Indian Space Policy-2023, which "*inter alia* aims at promoting greater private sector participation in the entire value chain of the space economy, including in the creation of space and ground -based assets" (Mondaq, 2024). Coupled with the Information Technology Act [2000], which includes cybersecurity provisions, India is poised to secure its expanding space sector against cyber threats (Indian Government, 2017; Indian Government, 2000). Critics have highlighted that India's regulatory framework needs to be more agile to keep pace with its rapid advancements in space technology and the increasing involvement of private players. Furthermore, the enforcement of these regulations can be inconsistent, particularly given the diverse range of actors involved in the Indian space sector. As such Indian startups must prepare for comprehensive regulation and potentially inconsistent enforcement, emphasising agility and compliance (Rajagopalan, 2023). And thus, this inconsistency may create gaps in the nations cybersecurity posture and undermine its innovation in space.

Australia

Australia's engagement in space cybersecurity has intensified in response to the growing recognition of the strategic importance of space assets. The 2023–2030 Australian Cyber Security Strategy outlines the necessity for enhanced protections for critical infrastructure, designating the space technology sector as one of the 11 critical infrastructure sectors under the Security of Critical Infrastructure Act 2018 (SOCI Act) (Australian Government, 2023). This classification reflects the integral role that space systems, such as satellite communications and navigation services, play in national security and economic stability. However, the designation also exposes significant vulnerabilities that must be addressed.

A pivotal development in Australia's approach to space cybersecurity is the establishment of the Australian Space Cyber Framework (SCF) and the Space Cyber Architecture (SCA). These frameworks were developed by CyberOps under a $2.5 million contract from the Department of Defence, aimed at uplifting the cybersecurity readiness of Australia's space sector (CyberOps, 2023). While these initiatives are commendable, they also reveal a reactive stance rather than a proactive strategy. The frameworks provide essential security practices and standards, yet they do not fully clarify how cybersecurity reforms will be applied within the space technology sector. This lack of specificity in the SOCI Act raises questions about the enforceability of

cybersecurity measures and the potential for compliance gaps (Cubbage, 2024).

The Australian government’s commitment to international cooperation in cybersecurity, exemplified through the AUKUS partnership and forums such as the Australian Space Cyber Forum, demonstrates an awareness of the global dimensions of space cybersecurity (Satellite Applications Catapult, 2024). The collaboration with UK counterparts is critical, especially in light of the interconnected nature of cyber threats. However, while these international partnerships are beneficial, they also underscore a reliance on external expertise and frameworks, which may not adequately address the unique challenges faced by the Australian space sector. Moreover, as the number of satellites and space-based communication systems continues to grow, so too does the potential for cyber threats. The implications of these threats are particularly concerning given the aging infrastructure of many existing space assets. This raises alarms about the adequacy of current protective measures and the potential consequences of cyber incidents on national security and critical infrastructure.

In summary, while Australia is making notable strides in establishing a comprehensive framework for space cybersecurity, significant challenges persist. The need for clarity in regulatory obligations under the SOCI Act, coupled with the rapid evolution of cyber threats, necessitates ongoing vigilance and proactive measures. A more robust national strategy that integrates cybersecurity into the design and operation of space systems, alongside continuous collaboration with international partners, will be crucial for enhancing the resilience of Australia’s space assets against an increasingly complex cyber landscape.

New Zealand

New Zealand is increasingly positioning itself as a significant player in the realm of space cybersecurity, recognising the strategic importance of safeguarding its national interests in a rapidly evolving global environment. The recent National Security Strategy: Secure Together Tō Tātou Korowai Manaaki outlines the government's commitment to addressing contemporary security challenges, particularly those posed by cyber threats and the militarisation of space (New Zealand Government, 2023). As part of this strategic shift, space cybersecurity has become a critical component of New Zealand's national security framework.

The establishment of the Joint Commercial Operations (JCO) hub marks a significant step in enhancing New Zealand's capabilities in space monitoring and cybersecurity. Collaborating with allies such as Australia, Japan, and the United States, the JCO hub facilitates the sharing of intelligence regarding satellite activities and potential threats, thereby bolstering collective security in the space domain (Pennington, 2024). This partnership highlights New Zealand's commitment to integrating digital technology into defence operations, demonstrating its readiness to tackle the complexities of modern security challenges.

In 2024, the New Zealand Defence Force (NZDF) took proactive steps to enhance international collaboration by assisting in the training of the Japanese military to monitor satellites. This initiative, funded by the United States, exemplifies the strengthening of defence relationships in the region and reflects New Zealand's growing role in the global space domain awareness ecosystem (Pennington, 2024). The training provided to Japanese forces is a testament to New Zealand's dedication to enhancing interoperability among allied nations in the face of emerging cyber threats.

Furthermore, New Zealand's Space and Advanced Aviation Strategy 2024-2030 aims to develop sovereign capabilities in space technology and monitoring, thereby reducing reliance on foreign assets (Ministry of Business, Innovation and Employment, 2024). The strategy underscores the importance of establishing a robust regulatory environment to support innovation while ensuring safety and national security. However, the absence of dedicated indigenous space assets poses a challenge to New Zealand's ambitions in securing its interests in the space domain. Despite these advancements, significant challenges remain. The NZDF's lack of specific guidance on developing indigenous space systems could impede progress in achieving self-sufficiency in space capabilities (Sanmartí, 2024). Additionally, New Zealand's reliance on international partners for critical satellite capabilities raises concerns about sovereignty and operational independence during geopolitical tensions.

In conclusion, New Zealand's proactive engagement in space cybersecurity illustrates its commitment to safeguarding national interests amidst growing global threats. By fostering international partnerships and striving for indigenous capabilities, New Zealand aims to enhance its resilience in the face of emerging challenges. However, addressing the existing gaps in regulatory frameworks and indigenous capabilities will be essential for ensuring the security and sustainability of its space assets in an increasingly contested environment.

Fiji and Tonga

Fiji: Through its partnership with SpaceX's Starlink, Fiji is expanding internet connectivity across its 300+ islands. While this is a game-changer for communication, it also presents new vulnerabilities. Fiji's reliance on satellite-based internet for critical communication during natural disasters highlights the importance of integrating cybersecurity measures into this growing infrastructure. In 2024, Fiji initiated a cyber capacity-building programme with the UK government and the Oceania Cyber Security Centre (OCSC), which focuses on developing a national cybersecurity strategy that includes space assets (Fiji Cyber Capacity, 2024).

Tonga: Similarly, Tonga is in the early stages of developing its cybersecurity framework, particularly as it becomes more reliant on satellite-based communication. As both nations depend on satellite systems for national infrastructure, their emerging cybersecurity frameworks must evolve to protect these assets from external threats**.**

United Arab Emirates: Innovation at the Crossroads of Geopolitics

The United Arab Emirates (UAE) has quickly emerged as a key player in both space exploration and cybersecurity, leveraging its strategic location and substantial financial resources to assert itself on the global stage. The UAE's focus on innovation, combined with a strong emphasis on national security, is positioning the country as a regional leader in the space sector. During the recent Hili Forum, Omran Sharaf, the UAE's Assistant Minister for Advanced Science and Technology, emphasised the nation's commitment to advancing space technology while ensuring robust cybersecurity measures are in place (Sharaf, 2024).

The UAE's investments in artificial intelligence (AI) and space technologies are part of its broader strategy to remain competitive in the global race for technological dominance. The country's proactive approach to integrating cybersecurity across all aspects of its space programme ensures that it is prepared to counter emerging cyber threats, which are crucial to maintaining its influence. Satellite systems used for both military and civilian purposes, particularly in communications and Earth observation, are at the core of the UAE's national security strategy. Ensuring the cybersecurity of these critical assets is essential to safeguarding the nation's geopolitical standing and sustaining its role as a leader in the rapidly evolving space industry.

Saudi Arabia: Aspirations and Vulnerabilities

Saudi Arabia is positioning itself as a major player in the global space sector, with ambitions to generate $2.2 billion from its space initiatives by 2030. However, as the Kingdom ramps up its space activities, it must also address the inherent cybersecurity risks associated with managing large satellite networks and space-based infrastructure. Recent initiatives led by the Saudi Space Agency and the Communications, Space, and Technology Commission (CST) illustrate this growing focus on both space exploration and security. For instance, the launch of programmes such as the Space Challenge Camp Highlights Saudi Arabia's commitment to building national expertise in space sciences and cybersecurity. This is especially critical as the Kingdom's space ambitions extend beyond peaceful exploration, carrying significant national security implications related to satellite communications and Earth observation systems (ENISA Threat Landscape, 2024).

In alignment with its Vision 2030, Saudi Arabia is embedding cybersecurity into its broader space strategy, recognising that the protection of its space infrastructure is essential to national security. With the Kingdom's heavy investment in satellite communications, it has become a prime target for cyberattacks, particularly given the geopolitical tensions in the region. These challenges are further complicated by Saudi Arabia's geographical position, which increases the complexity of satellite launches and the safeguarding of its space assets from potential cyber threats.

Russia

Russia remains a formidable player in space, using its capabilities to advance its geopolitical ambitions. The 2022 cyberattack on Viasat, which disrupted satellite communications during the Ukraine invasion, demonstrated Russia's willingness to employ space-based cyberattacks as a component of conventional warfare. This event reflects a broader strategy in which Russia views space as an essential domain for both influence and disruption. A significant element of Russia's space power lies in its counterspace capabilities, including anti-satellite (ASAT) weapons that can disable or destroy satellites critical to civilian and military infrastructure worldwide. These ASAT capabilities underscore the potential threat Russia poses to global space infrastructure, highlighting its readiness to challenge other nations' space assets if necessary. Moreover, Russia vetoed a UN Security Council vote on all counties to prevent an arms race in outer space in 2024 (Cooney, 2024).

Russia's space activities are regulated under the Federal Law on Space Activity (1993) which includes provisions for addressing "*international issues regarding responsibility, liability and jurisdiction for private entities*" (Lukowski, 2023). However, this law contains notable gaps, as it does not explicitly address cybersecurity, leaving open areas subject to interpretation. While Russian space agencies and companies adopt stringent security protocols, reflecting the centralised control characteristic of Russian governance, the broader Russian cybersecurity landscape is governed by a set of laws that influence space operations:

Federal Law No. 187-ФЗ on the Security of Critical Information Infrastructure (2017) mandates stringent security standards for sectors deemed vital to national security, including space infrastructure. This law requires organisations, particularly in sensitive areas like telecommunications and defence, to transition to Russian-developed software by 2024 and hardware by 2025, restricting the use of foreign technology and align with Russia's ambition of digital sovereignty. By controlling technology sources, Russia aims to mitigate foreign cyber threats in its space operations, but this insularity may hinder access to advanced global cybersecurity solutions.

The **Sovereign Internet Law** (Federal Law No. 90-ФЗ) was enacted in 2019 to establish an independent Russian internet, or "Runet," which could operate autonomously from the global web. This law grants Roskomnadzor, Russia's media oversight agency, sweeping powers to monitor and control internet infrastructure(Hakala, 2021). Extending this principle to space, Russia's space-based communication systems may similarly seek independence from international networks, fostering resilience but risking isolation from beneficial global security frameworks.

Federal Law No. 152-ФЗ on Personal Data (2014) enforces data localisation, requiring that personal data of Russian citizens be stored domestically. This impacts space operations by limiting international data exchanges, which complicates collaboration with foreign entities that rely on data sharing. For Russian space missions, this constraint means restricted data flow, potentially isolating Russian space assets from joint security and scientific initiatives.

The **Yarovaya Law** (Federal Law No. 374-ФЗ on Counterterrorism and Public Safety) grants Russian authorities extensive rights to access encrypted communications, enforcing data storage and decrypt ability for telecommunications providers. This principle may extend to space-based systems, underscoring Russia's focus on maintaining control over critical information networks. In the context of space, this centralised oversight could facilitate offensive cyber capabilities integrated with Russia's space assets, reflecting a readiness to utilise cyber operations in space as part of broader military strategies.

While these laws do not directly target space cybersecurity, they embody Russia's focus on digital sovereignty, self-reliance, control, and restricted foreign influence over critical infrastructure. This approach presents challenges for international collaboration, as Russia's regulatory framework is not aligned with global standards like the NIST guidelines and has limited engagement with international cybersecurity norms. Consequently, Russia's stance on space-based cybersecurity emphasises sovereignty over shared security, which raises concerns about its commitment to collective space governance.

In sum, Russia's space cybersecurity posture—characterised by a preference for domestic technology, counterspace capabilities, and limited transparency—reflects its strategic priorities. This inward focus may reinforce Russia's resilience against external threats but poses risks to global trust and cooperation within the interconnected space domain, potentially fragmenting collaborative efforts on space security today and for the foreseeable future.

Europe's Collaborative Model:

The European Union (EU) has adopted a collaborative approach to space cybersecurity, integrating cybersecurity principles across its space programs. The launch of the IRIS satellite program, which aims to enhance Europe's technological sovereignty, is an example of how Europe is positioning itself to secure space-based communications through a secure-by-design approach. The EU coordinates its space activities under the European Space Policy (2007) and is finalising a comprehensive EU Space Law, expected by 2025, which is likely to include stringent cybersecurity requirements. This new legislation will build on the security framework established by the General Data Protection Regulation (GDPR, 2018) and the Network and Information Security (NIS) Directive (2016), both of which set robust data protection and cybersecurity standards across the EU (European Union, 2007; European Union, 2016).

Despite these efforts, the EU faces challenges in harmonising cybersecurity regulations across its member states, which vary in technological capabilities and cybersecurity maturity. Enforcement is further complicated by the need for coordination among multiple national regulatory bodies. Below are some examples of how some European nations have made a strategic decision to focus on space cybersecurity:

France's Law on Space Operations (2008, amended 2023) is a pioneering regulation that includes specific cybersecurity provisions. Article 27 mandates cybersecurity measures to prevent unauthorised commands to spacecraft. Article 39-3 requires space operators to implement a comprehensive cybersecurity plan (French Government, 2023). These amendments underscore France's commitment to securing its space activities against emerging cyber threats. However, some commentators have argued that the broad and somewhat vague requirements of these articles could lead to inconsistent implementation and compliance issues among operators. Enforcement of these provisions can be challenging due to the complexity and rapid evolution of cybersecurity threats. French startups must develop detailed cybersecurity plans to comply with national regulations, ensuring robust protection against cyber threats.

Luxembourg, a smaller nation but an outsized player in space law and technical standardisation, has developed a space strategy that prioritises cybersecurity. Through its 2020-2030 Standardization Strategy, Luxembourg has embedded cybersecurity into its space sector from the ground up, offering a model for smaller nations like Scotland to follow. By advocating for strong international regulations on space cybersecurity, Luxembourg ensures that its space assets are resilient to cyberattacks, positioning itself as a key partner in Europe's space future. Liechtenstein: Regulatory Pioneering in Space Law and Cybersecurity

Liechtenstein, though a small country, is playing an increasingly proactive role in space policy. In 2023, it introduced new space laws that integrate cybersecurity provisions to protect its emerging space sector. By incorporating cybersecurity from the outset, Liechtenstein's legislation underscores the importance of building security into the development of space infrastructure (Liechtenstein Space Law, 2023). As a small but growing player in the global space landscape, Liechtenstein demonstrates that even countries with modest space programs can contribute to the security and stability of the global space ecosystem through forward-thinking regulation.

Estonia is emerging as a key player in space cybersecurity, driven by geopolitical tensions and the increasing reliance on space-based systems. Paul Liias, head of Estonia's space policy, highlights the strategic importance of protecting satellite communications and data services, especially considering the Ukraine conflict. Estonia is focusing on making space cybersecurity more accessible and affordable for both large and small players in the space sector. Estonia in collaboration with the European Space Agency

(ESA), Estonia is developing a space cyber range—a virtual environment where space companies can simulate cyberattacks and test their software to improve their defence capabilities (Hankewitz, 2023). Estonia's innovation in this area highlights the growing need for cyber resilience as the global space economy becomes increasingly vulnerable to cyber threats. Estonia's space cyber range offers an example of how smaller nations can play a critical role in securing global space systems.

UK Space Cyber

The UK has taken steps to address cybersecurity in space with the Space Industry Act [2018] regulates space activities, including commercial spaceflight and satellite operations. The Space Industry Act [2018] emphasise security and safety, implicitly covering cybersecurity measures necessary for licensing (UK Government 2018). Complementary to these are the Data Protection Act (2018) and the NIS Regulations (2018), which implement GDPR and the NIS Directive, respectively, ensuring comprehensive cybersecurity across critical infrastructure, including space systems (UK Government, 2018).

In recent developments, the UK's space industry has been supported by significant legislative and policy efforts. The UK Space Agency and the National Space Strategy aim to bolster the UK's position in the global space sector through innovation and international collaboration (Clyde & Co, 2024; House of Commons Library, 2024). The "Space Regulatory Review 2024" provides updated insights into the UK's regulatory landscape, addressing challenges and opportunities in ensuring the safety and security of space operations (UK Government, 2024). This review highlights the UK's commitment to maintaining high standards of cybersecurity and regulatory compliance, reflecting the evolving nature of space technology and the need for adaptive legal frameworks.

However, post-Brexit, the UK faces the challenge of maintaining alignment with rapidly evolving EU regulations while developing its independent framework. Furthermore, while the regulations set high standards, actual enforcement and compliance will vary (and are largely untested), potentially undermining their effectiveness. UK-based startups will also have to align with both national and international cybersecurity standards (as they develop) and will require skilled leaders to navigate these emerging challenges.

Big Tech's Diplomatic Power in Space and Cybersecurity

The diplomatic influence of Big Tech companies is reshaping global power dynamics, particularly in the intersection of space and cybersecurity. Companies such as SpaceX, Microsoft, and Meta (Facebook) now operate as geopolitical actors with technological capabilities and financial resources that rival those of nation-states (Bremmer, 2021; Fox & Probasco, 2022). Their growing influence requires new diplomatic frameworks as they increasingly play pivotal roles in shaping international relations and security outcomes (Farrell, 2018).

Elon Musk’s Starlink satellites, for example, were instrumental in maintaining Ukraine's internet connectivity during the Russia-Ukraine conflict, underscoring the critical role private actors can play in geopolitics (Fox & Probasco, 2022). However, Musk’s suggestion that the U.S. military should contribute funding for Starlink services highlighted how financial incentives can influence these actors’ commitments in conflicts, raising concerns about the dependency of state actors on private interests (CNN, 2022). This case illustrates a broader issue: private companies are not neutral actors in international affairs, and their decisions often have significant diplomatic and security implications (Fox & Probasco, 2022; Bremmer, 2021).

As these companies expand their influence, they increasingly shape space governance and cybersecurity protocols, areas traditionally dominated by state actors. For instance, SpaceX’s dominance in satellite launches raises concerns about the monopolization of space resources, potentially limiting access for other nations and restricting international cooperation (Fox & Probasco, 2022; House of Commons, 2022). Similarly, the acquisition of shares in OneWeb by entities with connections to China highlights the diplomatic complexities introduced by private ownership in critical space infrastructure (House of Commons, 2022). These developments blur the lines between state sovereignty and private influence, complicating traditional diplomatic frameworks (LaFrance, 2021).

Big Tech's growing involvement in cybersecurity also demonstrates their significant diplomatic role. Microsoft’s defense against Russian cyberattacks on Ukraine, coupled with Google’s removal of certain data flows during the conflict, demonstrates how these companies now act as key players in cyber diplomacy (Fox & Probasco, 2022; Wadhwa & Salkever, 2022). The reliance on private actors to manage critical cyber defenses illustrates a shift in power, where their actions directly impact national security and international relations (Bremmer, 2021; LaFrance, 2021). These companies' interests may not always align with those of nation-states, creating potential risks where diplomatic responses are influenced by commercial considerations rather than solely by national or global security needs (Fox & Probasco, 2022).

The diplomatic challenges posed by Big Tech extend to the governance of space. Much like the transnational commercial actors of the colonial era, such as the Dutch East India Company, today’s tech giants have the potential to shape the future of space exploration and security (Phillips & Sharman, 2015). However, their dominance risks creating monopolies that could stifle innovation and limit alternative approaches to space governance (Fox & Probasco, 2022; Bremmer, 2021). This concentration of power among a few private actors narrows the scope for diverse approaches to space exploration and cybersecurity, posing a challenge for international diplomacy (Farrell, 2018).

In conclusion, Big Tech’s expanding role in space and cybersecurity calls for the development of new diplomatic strategies. As these companies continue to shape global security and governance structures, states must navigate complex relationships with powerful private actors whose decisions have far-reaching

implications. The future of diplomacy in these areas will depend on how effectively governments can engage with these companies, balancing their commercial interests with the broader needs of international security and cooperation (Fox & Probasco, 2022; LaFrance, 2021; House of Commons, 2022).

Scotland's Strategic Role in a Global Context

As this chapter has discussed, nation-states like the United States, China, and Russia are prioritising their space assets by implementing specific cybersecurity frameworks that align with their broader national security agendas. Scotland, with its emerging spaceports in the Highlands and a thriving satellite manufacturing industry in Glasgow, has the potential to adopt a distinctive approach that leverages European principles of secure-by-design infrastructure, like the EU's IRIS² satellite program.

However, Scotland must also navigate the complexities brought by private space companies acting as "unofficial nation-states" with expansive, cross-border reach. While countries like the United States have embraced private sector involvement with significant military partnerships, Scotland has an opportunity to establish a balanced framework that not only attracts commercial actors but also enforces stringent cybersecurity standards. This approach would help secure its space assets from both state-sponsored threats and non-state cyber actors, especially as private companies play increasingly influential roles in global space security.

Scotland's strategic interest is further highlighted by its geographical proximity to the Arctic, where climate change is accelerating geopolitical tensions. Like Canada's Arctic surveillance goals, Scotland could play a pivotal role in monitoring and securing new shipping routes and regional resources. By prioritising a resilient space cybersecurity posture and aligning with European regulatory frameworks, Scotland can not only enhance its own space infrastructure but also contribute to Europe's broader strategic goals. In doing so, Scotland is well-positioned to assert itself as a key player in a rapidly evolving global space economy, securing both its assets and its influence in this critical domain.

Recommendations for Scotland's Space Cybersecurity Strategy

- **Expand Strategic Partnerships**: Scotland should foster partnerships with emerging space powers and innovative smaller nations. These collaborations can enhance Scotland's cybersecurity resilience and contribute to global efforts in securing space infrastructure against cyber threats.
- **Prioritise Investment in Disruptive Technologies**: To maintain a competitive edge, Scotland should invest in cutting-edge technologies such as quantum encryption, AI-driven threat detection, and blockchain for secure space communications. These technologies will be critical in building a robust cybersecurity posture that aligns with global advancements.
- **Advocate for Robust International Cybersecurity Standards**: Scotland can position itself as a thought leader in space cybersecurity by advocating for international cybersecurity regulations that protect space assets. By contributing to global regulatory frameworks, Scotland can play a pivotal role in shaping secure and sustainable space governance.

- **Implement a Scotland-Specific Space Cybersecurity Framework**: While UK-wide cybersecurity initiatives are beneficial, Scotland's growing space sector would benefit from a dedicated, Scotland-specific cybersecurity framework. This framework could address the unique needs of Scotland's space infrastructure, particularly given its emphasis on satellite manufacturing and regional spaceports.

Conclusion

As space and cybersecurity continue to converge, Scotland has a significant opportunity to lead in developing secure space infrastructure. By drawing on the experiences of larger powers and smaller innovative nations, Scotland can navigate complex geopolitical dynamics and strengthen its position in the global space economy. With strategic investments and international partnerships, Scotland is well-equipped to secure its space assets and assert its role in shaping the future of space security.

This chapter aligns with the United Nations Sustainable Development Goals

SDG 9: Industry, Innovation, and Infrastructure.
SDG 16: Peace, Justice, and Strong Institutions
SDG 17: Partnerships for the Goals
SDG 13: Climate Action
SDG 8: Decent Work and Economic Growth

Chapter Two: The Critical Role of Specialised Diplomats in Space-Cyber Diplomacy

As outlined in the previous chapter, the evolving geopolitical landscape is marked by increased competition among both established and emerging space powers. These tensions now extend into space and cyber domains, where the intersection of cyberattacks and space technologies presents significant challenges for international diplomacy. Space infrastructure—integral to national security, communications, navigation, and global economic systems—is increasingly vulnerable to cyberattacks by nation-states such as China, Russia, Iran, and North Korea (CSIS, 2024; Radanliev, 2024). These attacks, often part of broader strategic campaigns, add complexity to diplomatic efforts by blurring the line between civilian and military space systems (Roberts, 2024; Meyer, 2021).

Historical Context: The Evolution of Space-Cyber Diplomacy

The current challenges in space-cyber diplomacy are the culmination of decades of technological advancements and geopolitical shifts. Space diplomacy during the Cold War was primarily shaped by the need to avoid direct conflict between the U.S. and the Soviet Union, resulting in agreements like the Outer Space Treaty (1967), which emphasized the peaceful use of space. As cyberspace emerged in the 1990s, global governance focused on cybercrime and internet governance, reflected in the Budapest Convention (2001). However, the increasing convergence of space and cyber technologies in the 21st century has exposed the inadequacies of these earlier frameworks, which were designed for a world without AI, quantum computing, or the commercialisation of space.

Furthermore, the development of cyber diplomacy (Potter, 2002; Pahlavi, 2003; Attatfa et al; 2022; Maulana, et al, 2023;) gained momentum as cyber operations became more integrated into geopolitical strategies. The Tallinn Manual (2013), which provided a comprehensive interpretation of how international law applies to cyber conflicts, including cyberattacks on critical infrastructure, remains a cornerstone for understanding how existing laws could govern cyberattacks on space-based assets. The manual's focus on the rules of engagement under international humanitarian law has significant implications for space diplomacy, especially given the dual-use nature of satellites and other space infrastructure. Applying cyber rules of engagement to space remains a complex issue requiring further diplomatic dialogue (Wess, 2021).

Emerging Threats and Diplomatic Complexity

The convergence of space and cyber commercialisation and warfare has revealed significant disparities in how nations navigate these dual domains. States like the US, China, and Russia have developed advanced capabilities in both space and cyber operations, positioning themselves as dominant players in the emerging space-cyber arena (CSIS, 2024; Radanliev, 2024). While some nations engage in

persistent, state-sponsored cyberattacks targeting both civilian and military space systems,other nations face daily cyber assaults on their space assets but lack the technological resources to defend or retaliate effectively, leaving them increasingly vulnerable (Liebermann & Peter, 2024).

The geopolitical landscape has become more complex, as traditional state-to-state diplomacy struggles to adapt to the realities of cyber-enabled space conflicts (Roberts, 2024). Cyberattacks on space systems—difficult to attribute and counter through conventional military means—have transformed space into a contested domain where both state and non-state actors vie for dominance (Radanliev, 2024). The attribution challenge creates a new form of warfare, one that operates in the grey zone of non-attribution, allowing actors to engage covertly with minimal risk of retaliation.

This environment is further complicated by the increasing use of proxy actors. States like Russia and China often rely on third-party groups to conduct cyberattacks on space infrastructure, adding a layer of deniability and making it difficult to hold aggressors accountable (CSIS, 2024; Liebermann & Peter, 2024). These proxy conflicts blur the line between peace and conflict, creating enduring diplomatic challenges for nations attempting to maintain stability while facing persistent cyber threats.

At the heart of these emerging threats is the dual-use nature of space assets, which complicates diplomatic responses. Civilian satellites are often interconnected with military operations, meaning that a cyberattack on a commercial satellite network can have far-reaching consequences for national security. This dual-use reality demands new diplomatic frameworks that can address the overlapping civilian and military dimensions of space systems, as well as the growing role of private actors (Schmidt, 2024).

Developing Nations and the Imbalance of Power

While major spacefaring nations are well-positioned to leverage space and cyber technologies, developing nations and smaller actors remain vulnerable. Many of these nations rely heavily on foreign satellite infrastructure for communication, navigation, and economic activities, making them highly susceptible to cyberattacks. For example, nations in Africa and Southeast Asia face significant security risks but lack the technological sovereignty to protect their space assets (Ford, 2024). The digital divide (Ishaq, 2001; UN 2023) in space-cybersecurity reflects broader global inequalities, where less technologically advanced nations are unable to influence global governance frameworks, leaving them exposed to the interests of more powerful states.

This power imbalance complicates efforts to build inclusive international agreements on space-cybersecurity. Nations with fewer resources face a diplomatic landscape dominated by larger powers, which often shape governance frameworks to suit their strategic interests. Addressing this disparity requires diplomatic approaches that empower smaller nations and ensure that their vulnerabilities are considered in the formation of global governance structures.

New Challenges in Diplomacy

1. Norm Fragmentation and Diplomatic Disunity

The fragmented nature of existing governance frameworks—such as the Outer Space Treaty (1967) and the Budapest Convention (2001)—makes it difficult to establish cohesive international norms for space-cybersecurity. These frameworks were developed at different times and for different purposes, leading to norm fragmentation that hinders diplomatic unity (Radanliev, 2024; Polkowska, 2019). Diplomats must navigate these disparate legal systems, adding complexity to international negotiations.

2. Sovereignty and Jurisdictional Ambiguities

The question of sovereignty in space and cyber domains remains ambiguous. Space assets, for instance, traverse multiple jurisdictions, while cyberattacks often cross borders in seconds, raising difficult questions about jurisdiction and sovereignty in response to attacks (Smith, 2020). This lack of clarity complicates diplomatic efforts to establish rules for self-defence, jurisdiction, and international cooperation.

3. Cultural and Strategic Differences in Cyber Norms

Different nations view cyber governance through their own strategic and cultural lenses, leading to diplomatic deadlocks. While some countries advocate for open, secure space and cyber technologies, others like China and Russia push for cyber sovereignty, asserting more control over their national cyberspace (Meyer, 2021; Schmidt, 2024). These differences make consensus-building in international diplomatic settings highly challenging.

4. The Role of Private Actors

The growing influence of private actors, such as SpaceX and OneWeb, adds another layer of complexity. These companies operate across borders and are driven by commercial interests, which do not always align with national security concerns (Grillot & Méndez, 2024; Polkowska, 2019). Their involvement introduces new challenges in establishing unified international cybersecurity norms and regulatory frameworks, further complicating diplomatic efforts to manage global space governance.

5. Speed of Technological Change

Technological advancements—particularly in AI and quantum computing—are progressing faster than diplomacy. Diplomatic frameworks, which often take years to negotiate, risk becoming obsolete by the time they are enacted (Walker, 2023; Wang & Dubbins, 2024). This gap between technology and governance creates vulnerabilities that can be exploited by state and non-state actors.

6. Escalation Risks and Unintended Consequences

The interconnected nature of space and cyber technologies increases the risk of unintended escalations. A cyberattack on a satellite could be misinterpreted as an act of war, potentially triggering retaliatory actions that escalate into broader conflict (Radanliev, 2024). Diplomats must develop de-escalation protocols to manage these risks, but this is complicated by the lack of transparency and the difficulty in attributing attacks.

7. Lack of Transparency and Trust in Diplomatic Negotiations

Cyber and space capabilities are often shrouded in secrecy, making it difficult to build trust-based diplomatic agreements (Liebermann & Peter, 2024). Unlike traditional arms control agreements, space-cyber diplomacy lacks clear mechanisms for transparency and verification, further complicating negotiations. Diplomats must focus on building **trust** through new forms of transparency, such as international inspections or third-party oversight.

8. Diplomatic Skill Gaps in Emerging Technologies

Diplomatic efforts are hindered by a lack of expertise in highly technical fields like Space, Cybersecurity, AI and quantum encryption (Polkowska, 2019). The gap between technological advances and diplomatic understanding creates challenges in negotiating robust, relevant international agreements. Specialised space-cyber diplomats, equipped with both technical knowledge and diplomatic skills, will be essential in bridging this gap (Walker, 2023).

Public-Private Partnerships and Corporate Accountability

A crucial component of future governance is the role of public-private partnerships in shaping space-cybersecurity. Companies like SpaceX, Amazon, and OneWeb are developing vast satellite constellations and influencing space infrastructure on a global scale, often without the same regulatory constraints that bind state actors. This raises questions about corporate accountability—how should private actors be integrated into diplomatic discussions to ensure that their operations do not compromise global security?

Collaborating with private entities will be essential for establishing comprehensive regulatory frameworks that protect both national security and commercial interests. This includes establishing norms that ensure private companies adhere to international security standards while still allowing for innovation. The role of public-private partnerships will be crucial in ensuring that the commercialisation of space does not exacerbate existing security vulnerabilities or undermine diplomatic efforts.

The U.S. Strategic Framework for Space Diplomacy

The U.S. Strategic Framework for Space Diplomacy, developed by the U.S. State Department in 2023, provides a potential blueprint for global cooperation in managing space-cyber threats. The framework emphasizes U.S. leadership in establishing global norms and governance structures that include both state and non-state actors to manage space-cybersecurity (U.S. State Department, 2023).

However, as Drummond (2024) highlights, an overly U.S.-centric approach risks alienating emerging space powers such as China and India, who are rapidly advancing their own space capabilities. These nations are shaping their own strategies, often in ways that challenge the existing Western-led governance structures (Smith, 2020).

Science Diplomacy in Space Cybersecurity

In addition to traditional diplomatic strategies, science diplomacy offers a potential solution for fostering international cooperation in the face of emerging space-cyber challenges. Science diplomacy—the use of scientific collaboration to build trust between nations—can facilitate dialogue even amidst geopolitical tensions (Royal Society, 2010). By advancing scientific research in critical areas like space cybersecurity, quantum encryption, and AI regulation, nations can create the groundwork for future diplomatic agreements (Schmidt, 2024).

Science diplomacy can take several forms, as outlined by the Royal Society (2010):

> **Diplomacy for Science**: Governments collaborate to support scientific research. For example, international cooperation on quantum encryption could enhance satellite communication security (Schmidt, 2024).
>
> **Science in Diplomacy**: Scientific expertise informs foreign policy decisions. Cybersecurity experts can guide diplomats on the technical aspects of space-related international agreements, leading to more informed and effective policies (Smith, 2020).
>
> **Science for Diplomacy**: Collaborative scientific projects can help build relationships between states. Joint initiatives in space-cybersecurity research, such as efforts to manage space debris, can foster cooperation and build trust (Van der Meer, 2011).

The Need for Integrated Solutions

Technological advancements such as AI and quantum computing introduce further complexities, and current governance frameworks are often unable to keep pace with these changes. As highlighted earlier, the technological asymmetry between developed and developing nations adds further complexity to diplomacy, as nations with superior technology have a disproportionate influence on global governance (Goldman Sachs, 2023). This imbalance demands that global governance structures evolve to ensure equitable access and security for all nations, regardless of their technological capabilities.

Conclusion: A New Diplomatic Paradigm

All of these emerging threats—state-sponsored cyberattacks, proxy conflicts, dual-use infrastructure, the rise of private actors, and the rapid pace of technological advancement—demand new diplomatic solutions. Traditional treaty-based diplomacy, which focuses on state-to-state agreements, is no longer adequate for managing the continuous, covert nature of cyber-enabled threats in space. Instead,

there is an urgent need for integrated, real-time governance models that are capable of responding to these threats as they arise.

Specialised space-cyber diplomats will play a critical role in this new landscape. Equipped with both technical expertise and an understanding of the geopolitical dynamics at play, they will be essential for bridging the gaps between state actors, private companies, and international governance frameworks. Their role will be pivotal in creating diplomatic solutions that reflect the interconnected nature of space and cyber technologies, while fostering transparency and cooperation in an increasingly contested domain (Polkowska, 2019).

In conclusion, the intersection of space and cyber domains has exposed the limitations of traditional diplomatic frameworks. As cyberattacks blur the lines between peace and conflict, and as power imbalances between technologically advanced and less advanced nations become more pronounced, the need for a new diplomatic paradigm is evident. This paradigm must be agile, inclusive, and capable of managing both state and non-state actors in a rapidly evolving space-cyber environment. Without this shift, critical vulnerabilities in space infrastructure will continue to be exploited, with significant consequences for global security and stability.

This chapter aligns with the United Nations Sustainable Development Goals

SDG 9: Industry, Innovation, and Infrastructure

SDG 16: Peace, Justice, and Strong Institutions

SDG 17: Partnerships for the Goals

Chapter Three: Space Cybersecurity Threat Landscape and its Strategic Importance for Scotland

Building on the previous chapter's analysis of global space cyber dynamics and the growing need for specialised diplomacy, this chapter narrows its focus to the evolving threat landscape at the intersection of space and cybersecurity. By examining real-world cyberattacks, it identifies key vulnerabilities—such as outdated legacy systems, reliance on commercial off-the-shelf (COTS) technologies, and insecure communication protocols—that leave critical space infrastructure exposed to exploitation. As Scotland solidifies its role in the global space sector, addressing these cybersecurity challenges will be essential for protecting national security, driving economic growth, and maintaining technological leadership in an increasingly competitive and contested arena.

Space Cyber-security

As space and cyberspace increasingly intersect, vulnerabilities once limited to terrestrial networks now extend into orbit, broadening the threat landscape. Satellite systems, ground control stations, and their supporting software are now prime targets for adversaries, including nation-state actors and cybercriminals (Varadharajan & Suri, 2024). However, the risk is not confined to advanced technologies. Simple and often overlooked vulnerabilities—such as weak passwords, phishing attacks, or unsecured office networks—can provide attackers with entry points. A breach in everyday business systems, including emails, cloud applications, or employee devices, can lead to unauthorised access to sensitive space infrastructure, endangering national security (Mukhar, 2024; Kavallieratos & Katsikas, 2023).

Many space systems also depend on outdated software and commercial off-the-shelf (COTS) technologies, further increasing the attack surface (Varadharajan & Suri, 2024To effectively safeguard space assets, companies must adopt a comprehensive cybersecurity approach. This involves securing not only advanced space technologies but also addressing everyday operational risks, such as keeping software up to date and ensuring the security of business communications. By doing so, organizations can protect both their critical assets and the broader national security landscape.

Historical Examples of Space-Cyber

The need for this comprehensive cybersecurity approach is underscored by numerous historical cyberattacks targeting space assets. These incidents highlight the vulnerabilities in space infrastructure and the critical consequences of such attacks. One of the earliest publicly documented cyberattacks occurred in 1998 when Russian hackers infiltrated NASA's Goddard Space Flight Centre, resulting in the failure of the joint U.S.-German-British RoSat satellite (Wess, 2021, Aerospace, 2024). This highlighted the ability of cyber adversaries to disrupt satellite operations, which has become a persistent threat in the years since. Another pivotal event

occurred in 2007, when the Tamil Tigers hacked into IntelSat's satellite communications, exposing the vulnerability of satellite systems to non-state actors. This incident demonstrated the potential for critical communication links to be compromised by cybercriminals and insurgent groups (Space News, 2007, Aerospace, 2024). In addition to awareness of weaknesses in space systems, subsequent incidents continued to expose vulnerabilities in satellite control systems. Between 2007 and 2008, Chinese hackers successfully compromised two U.S. satellites – NASA's Terra and Landsat-7. These attacks allowed unauthorised access to the satellites without causing immediate damage, but they exposed severe vulnerabilities in satellite control systems, underscoring the risks posed by state-sponsored cyber threats (Aerospace, 2024).

More recently, Russia employed cyberattacks to target space assets, most notably during its 2022 invasion of Ukraine. A cyberattack on Viasat's satellite network disrupted Ukrainian military communications and affected over 45,000 modems across Europe, illustrating the scale and impact of such attacks (Manson, 2023). This incident highlighted the potential for cyber warfare to disrupt both military and civilian operations reliant on satellite infrastructure. SpaceX's Starlink network, which played a crucial role in maintaining Ukraine's internet connectivity during the conflict, was also targeted by cyberattacks and jamming efforts. These attacks on commercial actors underscore the growing involvement of private space companies in geopolitical conflicts and the subsequent risks they face (Manson, 2023).

Even beyond geopolitical conflicts, commercial actors have found themselves in the crosshairs of cyberattacks. For instance, between 2014 and 2015, Russian hackers used malware to compromise commercial satellite data links, further demonstrating the evolving tactics employed by cyber adversaries to target the space sector (Aerospace, 2024). In 2012, NASA faced a serious cyberattack where hackers gained full functional control over their key systems, allowing them to modify, copy, or delete sensitive data. This attack, which affected over 5,000 systems, exposed the critical vulnerabilities within NASA's cybersecurity infrastructure (BBC, 2012). And more recently in 2023, the Japan Aerospace Exploration Agency (JAXA) experienced a cyberattack, which led to a mass data leak of over 10,000 files, including classified material. This attack not only impacted JAXA but also affected other major entities such as NASA, Toyota, and Mitsubishi, showcasing the far-reaching consequences of cyberattacks on space agencies (Shimbun, 2024).

These reported incidents collectively highlight the increasing frequency and sophistication of cyberattacks targeting space assets. With the growing reliance on space-based systems for communication, navigation, and military operations, the need for robust cybersecurity measures is more critical than ever. The combination of state-sponsored threats, non-state actors, and the involvement of commercial entities demonstrates that space cybersecurity is now a global security priority.

Key Cybersecurity Threats in the Space Sector

To further understand the impact of these threats, it is essential to examine specific examples of cyberattacks on space systems. While not exhaustive, these cases highlight the significant vulnerabilities within the space sector. Many incidents remain undisclosed due to national security concerns or are only shared within intelligence

and industry circles. Therefore, while the examples provided demonstrate the range and evolution of cyber threats, it is likely that many more incidents remain outside the public domain. This partial view underscores the urgent need for robust cybersecurity strategies to protect space assets against both known and emerging threats.

1. Software Vulnerabilities in Space Systems

Outdated software is a common weakness in space systems. Many satellites rely on legacy software not originally designed to counter modern cyber threats. Once deployed, these systems become hard to update, leaving vulnerabilities that persist for years. A significant incident occurred in 1998 when the U.S.-German ROSAT X-ray satellite was compromised by hackers who accessed it via insecure ground station software, ultimately causing the satellite's destruction (NASA, 2018).

Jonathan James, alias "c0mrade," gained unauthorized access to NASA's computer systems in 1999, stealing sensitive data and exposing software vulnerabilities within the U.S. Department of Defense and NASA. His actions underscore the importance of securing software against breaches, no matter the source (Petkauskas, 2023).

In 2018, NASA's Jet Propulsion Laboratory faced a data breach due to outdated systems, underscoring ongoing issues with legacy software in space. The Galileo satellite system in 2019 also encountered disruptions due to software vulnerabilities, which further highlights the risks in satellite operations (European GNSS Agency, 2019).

Why it matters for Scotland: Scotland's space industry, a leader in small satellite production, must prioritise secure software development and robust patch management to mitigate such risks. A compromised satellite could disrupt critical services like weather forecasting, impacting both the UK and international stakeholders.

2. Supply Chain Attacks on Space Infrastructure

Supply chain attacks remain a significant threat to space systems. For instance, the SolarWinds attack in 2020 allowed hackers to embed malware into a widely used software product, leading to a global compromise of systems including those managed by U.S. government agencies. This incident demonstrated how attackers could exploit software updates to spread malware across various systems (SolarWinds, 2021).

Why it matters for Scotland: As Scotland contributes significantly to satellite manufacturing, securing the supply chain is essential. An infected software update or compromised component could expose satellites to unauthorised access or operational failures.

3. Phishing and Social Engineering Attacks

NASA's 2014 phishing attack is a prime example of the risks posed by social engineering. In this case, compromised employee credentials allowed attackers to access sensitive systems, potentially impacting mission-critical data (CISA, 2019).

A more recent example from 2024 involved Iranian attacks targeting space contractors, further underscoring the global reach and persistence of phishing threats in the space industry.

Why it matters for Scotland: Scotland's space sector heavily relies on skilled personnel. A successful phishing attack could lead to unauthorized access, disrupt missions, or compromise data integrity. Continuous training and robust cybersecurity protocols are essential to prevent such attacks.

4. Ransomware and Satellite Hijacking

Ransomware attacks are also targeting space infrastructure. In 2020, a ransomware attack on the European Space Agency forced the temporary shutdown of some services. Similarly, the NASA satellites Terra and Landsat-7 were reportedly hijacked by hackers who gained unauthorized access in 2018. These incidents illustrate how attackers can disrupt satellite operations, either through ransomware or hijacking control systems (ESA, 2020).

Why it matters for Scotland: Scotland's expanding satellite capabilities make it an attractive target for ransomware. A compromised ground station or satellite could lead to operational delays, financial loss, and reputational damage.

5. Jamming, GPS Spoofing, and Denial-of-Service (DoS) Attacks

During the 2018 NATO Trident Juncture exercises, suspected Russian forces jammed GPS signals, leading to widespread navigation disruptions. More recently, in 2024, the RAF plane carrying UK Defence Secretary Grant Shapps experienced GPS jamming near Kaliningrad. This kind of interference, which also affected over 46,000 flights across Europe, demonstrates how vulnerable navigation systems can be to electromagnetic attacks (Waterman, 2024).

Why it matters for Scotland: Scotland's reliance on satellite navigation for critical sectors makes it essential to strengthen resilience against GPS spoofing and jamming. Disrupted navigation could compromise emergency responses, defines operations, and essential services, highlighting the need for robust cybersecurity defences.

6. Insider Threats

Insider threats can be both accidental and intentional. In 2018, an IT contractor leaked sensitive data about Australian defence systems, revealing potential vulnerabilities in space infrastructure (ZDNet, 2018). In 2012, NASA experienced a significant breach due to insider threats, allowing attackers to gain full access to sensitive systems.

Why it matters for Scotland: As the Scottish space industry grows, the risk of insider threats becomes more prominent. Implementing stringent access controls, thorough background checks, and ongoing monitoring of personnel can help mitigate such risks.

7. Physical Security of Ground Stations

Physical breaches also pose risks to satellite operations. For example, a Brazilian satellite dish was physically sabotaged in 2019, leading to communications disruptions. This incident highlights the need for robust security at ground stations, as physical access can allow attackers to compromise satellite operations (Security Magazine, 2019).

Why it matters for Scotland: With plans for the Sutherland Spaceport, Scotland must secure its ground stations against physical sabotage to protect the integrity of satellite communications.

8. Satellite Hardware Vulnerabilities

Hardware vulnerabilities, including those related to satellite sensors and antennas, pose another challenge. In 2019, a hardware fault in the Galileo system rendered it temporarily non-operational. This illustrates the need for secure and resilient satellite hardware (European GNSS Agency, 2019).

Why it matters for Scotland: Scotland's small satellite manufacturing must include rigorous testing and secure hardware standards to ensure operational reliability and security.

9. Data Transmission Security

Securing data in transit is critical for satellite operations. In 2008, a breach at a NASA satellite control centre allowed attackers to intercept communications, illustrating the risks associated with unprotected data transmission (NASA OIG, 2008).

Why it matters for Scotland: Protecting data transmission between satellites and ground stations is vital for sectors like defence and research. Implementing strong encryption and secure communication protocols will help mitigate the risk of interception.

10: Internet of Things (IoT) Devices in Space Systems

The integration of IoT devices into space systems presents additional risks. In 2016, the Mirai botnet exploited IoT vulnerabilities, causing widespread internet disruptions. Similar IoT-based attacks could target space systems, compromising the functionality of networked devices (Trend Micro, 2017).

Why it matters for Scotland: With the increased use of IoT devices in satellite production and ground operations, Scotland's space sector must prioritize secure IoT deployments, including robust encryption and regular updates, to prevent exploitation.

11. The Unknown and Emerging Threats

One of the most significant yet often overlooked cybersecurity challenges is the unknown: the constant innovation and disruption driven by criminal gangs, hacker collectives, and nation-state actors. These adversaries push the limits of technology, often using tactics and exploiting vulnerabilities that have yet to be fully understood or anticipated by defenders. From deploying novel forms of malware to experimenting with advanced AI and quantum techniques, these actors are continuously evolving their attack strategies.

While cybersecurity professionals are frequently constrained by compliance-driven approaches, such as ticking off annual audits or meeting regulatory requirements, adversaries face no such limitations. Instead, they exploit gaps in security strategies that are reactive, outdated, or overly reliant on static solutions. This rapid pace of innovation in the criminal world leaves many organisations, particularly SMEs in the space sector, struggling to keep up with the sophistication of these evolving threats. Emerging technologies, like AI, machine learning, and quantum computing, are not only tools for space exploration and business but also provide cyber adversaries with unprecedented capabilities. These unknown risks represent a critical challenge for organisations that are often playing catch-up with the latest security trends.

***Why it matters for Scotland*:** As a leader in satellite production and space technology, Scotland's space industry faces not just current, known threats, but also a wave of emerging and unknown cyber risks. Criminals and nation-state actors are continuously innovating, targeting high-value sectors like space to test the limits of what can be compromised. Without a proactive and forward-thinking approach to cybersecurity, the Scottish space sector could face risks that traditional security frameworks are not prepared to handle.

12: Cyber Hygiene

Poor cyber hygiene—relying solely on periodic cybersecurity checks rather than continuous monitoring—can leave critical systems vulnerable to new and evolving threats. As cyberattacks grow more sophisticated, gaps between annual or bi-annual assessments can be exploited by adversaries, potentially leading to breaches in satellite systems, communications networks, and other space infrastructure.

***Why This Matters to Scotland*:** For Scotland's growing space sector, maintaining strong cyber hygiene is crucial. A lack of continuous cybersecurity practices could leave critical assets like satellites and ground control systems vulnerable to attack, threatening both economic stability and national security. By fostering a culture of good cyber hygiene through real-time monitoring and constant system updates, Scotland can protect its space industry, ensuring its assets remain secure and

resilient in the face of emerging threats. This is vital for maintaining the country's competitive edge in the global space economy.

Generating Novel Scenarios to Avoid Surprise

A critical factor in enhancing cybersecurity for space assets is the development of innovative scenarios that anticipate and prepare for potential cyberattacks. As Nadi and Brooks (2023, p.2) suggest, *"Generating novel scenarios involves envisioning possible future cyber threats that have not yet been encountered, allowing for the development of proactive measures and the avoidance of strategic surprise.*" This proactive approach is especially relevant for Scotland, given its growing role in the global space industry and the increasing cyber threats targeting critical infrastructure.

Dr Lemac-Vincere at the University of Strathclyde is currently working on a platform designed to support this kind of scenario development, further advancing Scotland's capabilities in the space-cybersecurity sector. By embracing this forward-looking methodology, Scotland could position itself as a leader in disrupting the space cybersecurity field through innovation. By prioritising scenario planning and simulation exercises, Scotland can identify emerging vulnerabilities and test the resilience of its space systems against future threats. This would not only strengthen the nation's space infrastructure but also create opportunities for Scottish companies to develop cutting-edge solutions that address these challenges.

Furthermore, such an approach fosters innovation by encouraging creative problem-solving and challenging existing defence strategies. With its strong research institutions and thriving space sector, Scotland is well-positioned to lead this effort. By investing in advanced scenario development and cybersecurity simulations, Scotland could carve out a distinctive role in the global space cybersecurity landscape, driving both economic growth and security in this rapidly evolving field.

Recommendations for Scotland

1. **Develop a National Space Cybersecurity Framework**
   Scotland's growing role in the UK space sector demands a framework tailored to satellite and spaceport security. This should align with the UK strategy, focusing on satellite hijacking, jamming, and supply chain vulnerabilities.
2. **Strengthen Supply Chain Cybersecurity**
   Given the risks associated with Commercial Off-the-Shelf (COTS) components, Scotland should enforce cybersecurity certifications for suppliers, conduct regular audits, and perform risk assessments to protect satellite manufacturing processes.
3. **Invest in Cybersecurity Training and Workforce Development**
   To build a talent pool skilled in both cybersecurity and space systems, Scotland should collaborate with universities and industry partners on training programs and establish a research hub focused on satellite security innovation.
1. **Establish a National Space Cyber Incident Response Centre**
   A dedicated response centre would enable Scotland to quickly address cyber incidents impacting its space assets, working in coordination with the UK's cybersecurity infrastructure.

2. **Foster International Partnerships and Knowledge Sharing**
   Form alliances with global space and cybersecurity leaders to share threat intelligence and best practices. Joint research initiatives with countries like the United States and EU members can accelerate Scotland's cybersecurity capabilities.
3. **Promote Cyber Hygiene Practices in Space Operations**
   Cyber hygiene is essential for resilience. Scotland should mandate routine security assessments, patch management, and cybersecurity training within its space sector to prevent breaches.
4. **Invest in Quantum-Resistant Encryption**
   Scotland must stay ahead of emerging threats like quantum computing by funding R&D for quantum-resistant encryption and advanced technologies like AI-driven threat detection.
5. **Mandate Scenario-Based Cybersecurity Training**
   Scenario-based training will help Scottish space sector stakeholders prepare for real-world cyber incidents, improving their response strategies and resilience to complex cyber threats.
6. **Advocate for Global Cybersecurity Standards in Space**
   Scotland should work with international bodies to establish global cybersecurity standards for space, ensuring it contributes to shaping policies that secure critical space assets.
7. **Create a Space Cybersecurity Innovation Fund**
   A dedicated fund for cybersecurity innovation would support SMEs and research institutions in developing advanced solutions like AI-driven threat detection and blockchain technology for secure space communications.

Conclusion

Scotland’s growing role in the space sector places it at the forefront of the UK’s efforts to build a robust and secure space infrastructure. However, this also makes Scotland a prime target for sophisticated cyberattacks. Addressing these cybersecurity challenges is critical for safeguarding both economic interests and national security. Investment in secure software development, supply chain security, phishing prevention measures, and incident response planning is essential to protect Scotland’s space assets from compromise. Moreover, the collaborative efforts of universities, SMEs, and industry partners will be crucial in developing innovative cybersecurity solutions to tackle these emerging threats. By prioritising these measures, Scotland can ensure its space infrastructure remains resilient and continues to contribute to the UK’s strategic goals in space.

This chapter aligns with the United Nations Sustainable Development Goals:

SDG 9: Promotes resilient infrastructure and innovation.
SDG 11: Sustainable Cities and Communities
SDG 13: Climate Action
SDG 16: Peace, Justice, and Strong Institutions
SDG 17: Partnerships for the Goals

Chapter Four: Investing in Scotland's Space-Cyber Ecosystem - A Strategic Approach

Expanding on the previous analysis of global space cyber challenges, this chapter transitions to Scotland's strategic priorities in particular investment and growth. Scotland's space sector has grown significantly in recent years, driven by a blend of government support, private investment, and strong research institutions. With a strategic goal to capture £4 billion of the global space market by 2030, Scotland is positioning itself as a leader in space technology and innovation (Scottish Government, 2024). However, a critical area requiring greater attention is the integration of cybersecurity into space technologies. As the space economy continues its transformative growth, the convergence of space and cybersecurity presents a strategic investment opportunity—one that holds potential for Scotland to become a market leader in secure space solutions.

The Market Opportunity for Space Cybersecurity Investment

As the global space economy accelerates toward a projected valuation of $1.0 trillion to $1.8 trillion by 2040 (Morgan Stanley, 2023), the demand for securing space-based assets and infrastructure is growing at an unprecedented rate. Cybersecurity in the space sector is emerging as a high-growth market, driven by increasing reliance on satellites, space exploration, and space-based services. For investors, this convergence represents a significant opportunity: cybersecurity is not just about defence but is becoming a core enabler of sustainable growth in the space industry. Currently, the global cybersecurity market is valued at $173.5 billion and is projected to grow to $266.2 billion by 2027 (Statista, 2023). The more interconnected and complex space systems become, the more attractive they are to cyber adversaries. This creates a strong market for cybersecurity firms that can offer innovative, space-specific solutions in threat detection, encryption, secure communications, and incident response.

The UK cybersecurity sector, currently valued at £11.9 billion, is expanding rapidly, driven by public and private investments (UK Government, 2024, p.1). With over 60,680 professionals employed across 2,091 active companies, the UK is already a major hub for cybersecurity. Scotland's space industry, which is composed of more than 95% small and medium-sized enterprises (SMEs), is ideally positioned to capitalise on this growing need for cybersecurity solutions tailored to space technologies (Gov.UK, 2024). Building on this potential, investors have significant opportunities to target key areas within space cybersecurity, where growth is expected to accelerate in the coming years.

Market Breakdown: Space Cybersecurity Investment Potential

The space cybersecurity market is poised for growth in several key areas, driven by the strategic importance of space assets. Although there are no widely available market estimates specific to space cybersecurity, trends from the broader cybersecurity and space sectors indicate substantial potential:

1. **Satellite Communications Security**: As of 2024, there were approximately 9,900 active satellites are orbiting Earth, with a significant portion operated by commercial entities. SpaceX, through its Starlink megaconstellation, commands the largest share, with over 6,100 satellites currently in orbit (NanoAvionics, 2024; CEOWORLD Magazine, 2024). This dramatic increase in the number of satellites reflects a broader trend in the space industry. The number of satellites is expected to continue its rapid growth, potentially reaching nearly 60,000 by 2030 as more constellations are launched to support services such as global broadband (NanoAvionics, 2024)
2. **Space-Based Data Security**: The demand for space-based data, including Earth observation and satellite imagery, continues to grow. According to **Euroconsult**, the Earth observation satellite data market is expected to grow to **$6.6 billion by 2029**. Protecting this data from cyber threats will be vital for governments and businesses alike.
3. **Space Exploration and Defence**: Government investments in space exploration and defence are increasing worldwide. For example, NASA's budget for 2023 was approximately **$25.4 billion** (NASA, 2023). The rise in space missions and defence initiatives creates new opportunities for cybersecurity firms to protect mission-critical data and infrastructure.

These areas not only highlight the growing need for space cybersecurity but also underscore the potential for high returns**,** particularly in regions like Scotland that are emerging as key players in this sector**.** The entrepreneurial capacity of Scottish SMEs can drive innovations in these areas**,** ensuring that Scotland remains at the forefront of the global space-cyber landscape.

Scotland's Opportunity in Space Cybersecurity

Scotland's space sector, known for its strength in satellite manufacturing, data analytics, and space communications (SDI, 2024), is poised to become a key player in this emerging market. However, the underinvestment in cybersecurity across its SMEs presents a unique market opportunity for investors to fund innovative security solutions that can safeguard space infrastructure and enable long-term growth.

For this market to fully develop, it requires the integration of three critical elements: entrepreneurship, space, and cybersecurity. Scotland's entrepreneurial ecosystem, which has historically been at the forefront of innovation, plays a vital role in advancing these solutions. By bringing together space technologies and cybersecurity expertise, Scottish SMEs can lead the charge in building secure space infrastructures.

Given the projected growth of the global space economy and the increasing threats to space assets, the demand for space-specific cybersecurity services is likely to expand rapidly. Investors who focus on the intersection of space and cybersecurity can gain early access to a market that is still developing but has enormous potential. The agility and innovation of Scotland's SMEs—combined with the strategic importance of cybersecurity—offer a rare opportunity to shape the future of space security.

Projected Returns and Growth Areas

Investment in space cybersecurity is driven by several high-growth areas, which include:

- **Current SME UK and Global Market**
- **Satellite Cybersecurity**: The global satellite market is forecasted to reach **$308 billion by 2025** (Satellite Industry Association, 2022). With increasing satellite deployments, the need for securing satellite communications and operations offers substantial investment opportunities.
- **Space Infrastructure Security**: As mega-constellations and space stations become integral to the space economy, the need for cybersecurity solutions that protect these assets is expected to grow, potentially unlocking **multi-billion-dollar markets** in the coming decade.
- **Commercial Space Ventures**: The rise of private space companies like SpaceX and Blue Origin, combined with the growing interest in space tourism and exploration, creates opportunities for cybersecurity firms to secure these next generation ventures.

For investors, the space cybersecurity market represents a high-growth opportunity to capitalise on the next wave of innovation in the space industry. By addressing vulnerabilities and empowering entrepreneurial ventures in the space-cyber domain, investors can position themselves at the forefront of a sector that is both strategically essential and highly profitable.

Investment Challenges and Opportunities in the Space-Cyber Domain

Despite the compelling need for secure space solutions, space-cybersecurity remains underfunded. Investors frequently focus on either the space or cybersecurity sectors independently, leading to a gap in funding for projects that integrate the two (Garrett, 2023). High upfront costs, long development cycles, and regulatory complexities make the space-cyber domain less attractive to institutional investors, who often prefer ventures with predictable revenue streams and shorter return timelines (Davis, 2023, Brown, 2023).

However, for Scotland, this funding gap represents a strategic opportunity. As demonstrated by the UK Cyber Security Breaches Survey, approximately 50% of UK businesses experienced a cybersecurity incident in 2023, underscoring the need for enhanced security measures (Gov.UK, 2024). Moreover, the global cybersecurity market for SMEs is underdeveloped. Given that 43% of cyberattacks target small businesses, the demand for advanced, space-specific cybersecurity solutions is rising (Gov.UK, 2023). Scotland’s space sector could leverage this demand to become a leader in secure space technologies across the ecosystem, attracting investment and supporting national security.

Example: Creative Destruction Lab Space Programme

> The Creative Destruction Lab (CDL) Space Programme with Canadian astronaut Chris Hadfield exemplifies how targeted support can help emerging space-cyber companies. Operating from four global locations, CDL provides early-stage space startups with mentorship from astronauts, scientists, and investors to help them raise capital, build networks, and refine their business models. CDL's focus on technologies like satellite communications, Earth observation, and space logistics aligns with Scotland's strengths and could serve as a model for local initiatives (CDL, 2024). By developing a similar programme that supports space-cyber innovation, Scotland can foster a competitive advantage in secure space technology.

The Creative Destruction Lab (CDL) Space Programme illustrates how targeted support can help emerging space-cyber companies develop and scale vital technologies. However, as these companies grow and attract investment, the need for effective governance structures becomes ever more important. Whilst programmes like CDL provide the tools for early-stage development, the long-term success of these ventures also relies on strong oversight and governance.

For space-cyber companies, this means that beyond technical innovation, there must be a focus on embedding cybersecurity into wider strategic frameworks. As institutional investors increasingly scrutinise cybersecurity risk, boards must take a leading role in ensuring these risks are managed effectively. Governance structures that prioritise cybersecurity will not only safeguard companies from operational disruptions but also help build investor confidence and long-term resilience. The role of boards in embedding security into strategic planning is crucial as these companies transition from startups to key players in the global space economy.

The Role of Boards and Governance in Cybersecurity

Internationally, institutional investors are increasingly scrutinising board oversight of cybersecurity risks in the space sector. This scrutiny stems from the growing recognition that cybersecurity is not just a technical issue but a key business risk that can significantly impact a company's financial health, reputation, and long-term viability (NCSC, 2023). Boards are uniquely positioned to oversee this risk at the highest level, ensuring that cybersecurity is integrated into broader business strategies.

The National Cyber Security Centre (NCSC) toolkit highlights that effective governance structures that prioritise cybersecurity as part of risk management are essential for operational resilience and investor confidence (NCSC, 2023). Without robust board oversight, companies may leave themselves vulnerable to cyberattacks that can lead to operational disruptions, data breaches, and loss of intellectual property—all of which can undermine investor trust and market position. Board oversight ensures that cybersecurity moves beyond technical teams and becomes a core component of business strategy, shaping the company's long-term vision and risk management.

In the investment process, due diligence (Jones, 2023) must now extend beyond traditional financial analyses to include comprehensive cybersecurity evaluations. Companies that demonstrate strong board involvement in cybersecurity governance—through regular security audits, employee training, and incident response planning—are more likely to attract capital from informed investors (Williams, 2023). Boards must go beyond a superficial, "tick-box" approach, ensuring that cybersecurity policies are continuously evaluated and aligned with evolving global standards, such as NIST or other frameworks as they emerge.

The board's role is vital because it sets the tone at the top. By embedding cybersecurity into strategic planning and fostering a culture of accountability, boards can protect the company's long-term assets, ensure regulatory compliance, and maintain operational integrity. Ultimately, strong board oversight on cybersecurity ensures not only the protection of the company's digital infrastructure but also the preservation of its competitive edge and attractiveness to investors.

Public-Private Partnerships and Tax Incentives

While Public-private partnerships (PPPs) represent a critical mechanism for stimulating investment in space-cyber technologies, as they allow for a blend of public sector support and private capital. By absorbing some of the financial risk associated with early-stage technology development, PPPs can help Scottish space-cyber companies scale effectively, particularly in high-stakes areas where the cost and complexity of innovation can be barriers to entry. For instance, the Scottish Government could emulate successful PPP models seen in the United States and Europe, working closely with private entities to establish dedicated funding pools for space-cyber projects. Such initiatives can bolster confidence among venture capitalists, making the sector more attractive for substantial investment (Brown, 2023).

Tax incentives also present a practical avenue for encouraging investment in Scotland's space-cyber sector. Enhanced R&D tax credits targeting space-cybersecurity projects could reduce the perceived risk for investors and establish Scotland as a competitive player on the global stage. Following the example set by the European Space Agency (ESA), which has developed a zero-equity funding model to support cybersecurity innovations specific to space, Scotland could stimulate growth in technologies like quantum encryption and AI-driven threat detection by offering similar financial incentives. The ESA's model provides up to €200,000 in grants for companies working on advanced space-cybersecurity solutions, thus reducing the barriers to entry for emerging enterprises focused on cutting-edge technologies (ESA, 2024).

Additionally, the Scottish National Investment Bank (SNIB) has previously supported space-related ventures, including companies like Orbex and Skyrora. However, there is an opportunity for more targeted support in space-cybersecurity. Expanding R&D tax credits to include disruptive technologies such as autonomous cyber-physical systems would position Scotland as a leader in space-cyber innovation and draw international interest from both investors and collaborative partners. By reducing upfront costs through tax incentives, the government can lower the perceived risk of

investment in the sector, attracting private capital to this high-growth area and helping to drive further technological advancements (Garrett, 2023).

Beyond financial incentives, such support frameworks contribute to building a secure foundation for the space-cyber market, enabling Scottish companies to invest confidently in the security of their systems. With sustained investment in both technology and cybersecurity, Scotland has the potential to lead in space-cyber innovation, not only benefiting its economy but also contributing to the UK's broader national security and technological resilience.

Supporting Scotland’s Space SMEs: Closing the Cybersecurity Gap

Scotland currently has a modest share of the UK’s cybersecurity sector—only 7% of cyber firms are located in Scotland (Gov.UK, 2023)—which presents a significant opportunity for growth, particularly considering the urgent need for enhanced cybersecurity within high-stakes industries like space. There is also substantial growth potential within Scotland's space sector. If adequately supported, Scotland’s space SMEs are well-positioned to disrupt the global market with their agility and innovative capacity. However, to achieve this potential, they must prioritise cybersecurity as a strategic asset. Currently, there is a clear gap in the market for space-cyber technologies, and Scottish SMEs could close this gap by adopting advanced security measures and embedding cybersecurity into their business models. While the UK’s Cyber Essentials programme offers a good starting point, the high-stakes nature of space operations demands a more robust approach (NCSC, 2024).

Furthermore, for Scottish SMEs, demonstrating strong cybersecurity practices is no longer just a compliance issue; it is likely to become a key competitive differentiator. For example, the US military’s Commercial Augmentation Space Reserve (CASR) initiative highlights the importance of secure, resilient space assets when competing for government contracts (Lemac-Vincere, 2024). SMEs that commit to advanced cybersecurity frameworks will be better positioned to win national and international contracts, including high-value defence contracts from global markets like the US and EU. The long-term economic benefits for Scotland are clear: ensuring that its SMEs adopt secure-by-design principles will not only protect national infrastructure but also drive international investment and collaboration. Scotland’s ability to attract partnerships with leading global space agencies and defence contractors will largely depend on how well its space ecosystem addresses cybersecurity concerns across every level of the ecosystem.

Collectively, Scotland’s market opportunity, its growing national reputation as a leader in cybersecurity, and its focus on secure-by-design practices and resilience across the space ecosystem will set it apart in the global space sector. By promoting these strengths and attracting investment from both public and private sectors, Scotland is poised to become a key differentiator in the space industry, leading in secure space technologies.

Recommendations for Strengthening Investment in Scotland's Space-Cybersecurity Sector

1. Establish Dedicated Space-Cyber Investment Funds

Rationale: The intersection of space and cybersecurity is an emerging and high-risk sector that often requires substantial upfront capital. Investors may be hesitant to commit to space-cyber ventures due to the perceived technical risks, long development cycles, and limited awareness of potential returns. A dedicated investment fund would de-risk initial investments and attract venture capital by providing a clear pathway for funding innovative and strategically important projects.

Action: Scotland could introduce a space-cyber investment fund, potentially through the Scottish National Investment Bank (SNIB) or in collaboration with private investment partners. This fund could provide grants, equity investments, and loan guarantees to support early-stage and scale-up ventures in the space-cyber sector. By focusing on disruptive technologies, such as quantum encryption for satellite communications and AI-driven threat detection, this fund could help bridge the current investment gap and build a robust pipeline of innovative projects.

2. Implement Tax Incentives for Space-Cyber Investments

Rationale: Tax incentives are proven mechanisms for driving investment into high-growth sectors. Like biotechnology and renewable energy, the space-cyber sector faces high risks but offers significant strategic value. By introducing tax relief specifically for space-cyber investments, Scotland can create a favourable investment environment that attracts both domestic and international investors.

Action: The Scottish Government could introduce R&D tax credits and capital gains tax relief specifically targeting space-cyber technologies. For instance, offering enhanced tax relief for investments in satellite encryption technologies, secure communication protocols, and autonomous threat detection systems could incentivise more investors to engage with the sector. These tax incentives should be widely promoted through industry events and government publications to increase awareness and attract investors from a range of backgrounds.

3. Establish a Public-Private Partnership (PPP) Model for Space-Cyber Projects

Rationale: Public-private partnerships (PPPs) allow the government to share financial risk with private entities, making it easier for investors to engage in high-stakes sectors like space-cybersecurity. PPPs can attract venture capital by providing a stable source of co-investment, thereby reducing financial barriers for private investors.

Action: Scotland could create a PPP initiative that combines government-backed grants with private capital for strategic space-cyber projects. This model could follow successful examples from countries like the United States, where government contracts and funding are used to support dual-use technologies. The Scottish Government could also act as a customer for space-cyber services, such as secure

satellite communications, thereby creating a steady revenue stream that further reduces risk for private investors.

4. Create a Space-Cyber Investment Tracking System

Rationale: Tracking investment flows into the space-cyber sector allows for better resource allocation and provides transparent data that can attract additional investors. Currently, the lack of specific data on space-cyber investments makes it challenging to assess progress and identify gaps in funding, thereby limiting Scotland's ability to strategically grow the sector.

Action: The Scottish Government, in collaboration with industry bodies, could develop an investment tracking system to monitor capital flows into the space-cyber sector. This system would track funding trends, sector growth, and investment returns, providing key metrics for policymakers and investors alike. By publishing an annual report on space-cyber investments, Scotland could highlight areas of high potential and create a transparent environment that encourages further investment.

5. Promote International Engagement to Attract Foreign Capital

Rationale: Scotland's space-cyber sector has unique strengths, such as its focus on small satellite production and advanced research institutions. To fully capitalise on these assets, Scotland needs to attract foreign investment. Engaging with the global investment community can bring in not only capital but also valuable expertise and partnerships that can help accelerate sector growth.

Action: Scotland could host annual space-cyber investment forums that bring together investors, industry leaders, and policymakers from around the world. These events could showcase Scotland's space-cyber capabilities, highlight successful case studies, and offer networking opportunities to attract foreign venture capital. Additionally, Scotland's trade and investment agencies could work with international partners to promote Scottish space-cyber projects in key markets such as the United States, Europe, and Asia.

6. Develop an Accelerator Programme for Space-Cyber Startups

Rationale: Space-cyber startups face unique challenges, including long development timelines, complex regulatory requirements, and significant technical risks. An accelerator programme tailored to space-cyber startups would provide these companies with the resources, mentorship, and funding needed to overcome these challenges, helping to scale innovative technologies.

Action: Scotland could create a space-cyber accelerator programme that offers intensive support to early-stage companies working at the intersection of space and cybersecurity. This programme could provide access to government funding, office space, and a network of industry mentors. Additionally, the accelerator could partner with research institutions like the University of Strathclyde and private companies such as Orbex and Skyrora to offer technical expertise and guidance. By nurturing startups through an accelerator model, Scotland can help ensure a steady pipeline of innovative companies in the space-cyber sector.

Conclusion

Scotland's space-cyber ecosystem offers significant investment potential, with far-reaching implications for both national security and economic growth. However, the success of this sector depends on the integration of entrepreneurship, space technologies, and cybersecurity. Investors who recognise the synergy between these three elements will be positioned to lead the next wave of innovation and secure the future of space infrastructures.

For investors, the time to act is now. Scotland's combination of enterprising spirit, burgeoning space industry, and emerging cybersecurity needs offers a rare opportunity to support a market that is still in its early stages. By aligning with Scotland's growth strategy and investing in space-cyber solutions, stakeholders can secure not only significant financial returns but also help shape the future of global space security.

This chapter aligns with the United Nations Sustainable Development Goals:

SDG 8 – Decent Work and Economic Growth:
SDG 9 – Industry, Innovation, and Infrastructure:
SDG 17 – Partnerships for the Goals
.

Chapter Five: Insurance – The Catalyst to Drive Commercial Behaviour

Following the exploration of Scotland's investment and growth in the space-cyber ecosystem, this chapter shifts focus to the pivotal role insurance plays in managing the risks associated with the expanding space sector. As space industry evolves and become more technologically complex, the associated risks—particularly from cyberattacks—have surged. Consequently, cybersecurity has become a core requirement for both space operators and insurers. This chapter examines how the global insurance market is responding to these changes, with insurers now often mandating cybersecurity measures as a prerequisite for coverage. For Scotland, aligning space operations with these global standards (as they arise) is essential for ensuring resilience, attracting investment, and maintaining long-term success.

Insurance as a Driver of Cybersecurity Innovation

Historically, insurance has served as a financial safety net for space missions, but its role is now shifting towards actively driving cybersecurity improvements throughout the ecosystem. Data from Marsh's Cyber Self-Assessment (CSA) highlights concerning gaps in current cybersecurity practices, with 70% of organisations relying on end-of-life (EOL) systems and many failing to implement essential measures such as multi-factor authentication (MFA) and privileged access management (PAM) (Marsh, 2023). These outdated systems pose significant risks, particularly in space missions where security breaches can have catastrophic consequences. Addressing these cybersecurity gaps is not only critical for safeguarding the space ecosystem but also for securing insurance coverage.

The Growing Importance of Cybersecurity for Insurance

In today's insurance landscape, cybersecurity is no longer optional—it is a mandatory component of insurable space missions. In leading markets like the UK, United States, and Germany, insurers now require space operators to adopt advanced cybersecurity protocols. For example, the European Union's Galileo satellite programme mandates comprehensive security measures as part of its insurance requirements, while US operators implement AI-driven monitoring systems to meet insurer expectations (European Space Security Report, 2023; Tech Insurance Review, 2023). These protocols help mitigate risks such as hacking, sabotage, and malicious acts, which traditional satellite insurance policies often exclude (Atler, 2024; Gallagher, 2024). The case of Inmarsat's I-5 F3 satellite in 2016 highlights the importance of clarity in insurance policies and close collaboration between operators and insurers. Despite being insured, prolonged claims negotiations followed due to ambiguities in policy terms, underscoring the need for space operators to ensure comprehensive coverage against cyberattacks and state-sponsored threats (Space Generation Advisory Council, 2022; Gallagher, 2024).

Addressing Cybersecurity Gaps and Aligning with Global Standards

The insights from Marsh's CSA and other reports reveal a pressing need for space operators to address cybersecurity weaknesses. With 60% of organisations lacking

mandatory MFA for accessing critical systems and only 32% implementing adequate PAM protocols, these vulnerabilities could jeopardise not only the missions but also the ability to secure insurance coverage (Marsh, 2023). Proactively addressing these gaps will be crucial for Scotland's space sector to meet both insurance requirements and international cybersecurity standards, such as the EU's NIS 2 Directive, which mandates MFA and PAM protocols (European Space Security Report, 2023).

By adopting cutting-edge technologies like blockchain for secure data transmission and quantum encryption for robust communications, Scotland's space sector can strengthen its cybersecurity defences and align with global best practices. These advancements not only mitigate risks but also position the sector as a leader in secure space innovation, ensuring long-term viability in an increasingly competitive and risky environment.

Opportunities for Scotland's Insurance Industry

This evolving landscape represents a new market opportunity for Scotland's insurance industry. As the intersection of space and cybersecurity grows more complex, there is significant potential for Scottish insurance businesses to develop specialised products that cater to the unique needs of space ventures. By leveraging Scotland's expanding space capabilities, insurers can position themselves as key players in this emerging market, offering tailored coverage that addresses both the technological and security challenges faced by space operators.

For example, Scottish insurers could develop performance-based policies that reward space operators for adopting cutting-edge cybersecurity technologies, such as real-time satellite monitoring and automated encryption updates. This model would not only reduce the risk of cyberattacks but also incentivise companies to continuously improve their cybersecurity posture.

Recommendations for Space Cybersecurity Insurance

1. Establish Space-Cyber Insurance Standards

> **Rationale:** Insurance companies in countries like the US and Germany increasingly require robust cybersecurity measures as a prerequisite for coverage. Scotland can create its own space-cyber insurance standards to ensure space operators adhere to high levels of cybersecurity resilience, helping to attract international investors and insurers.
>
> **Action:** Collaborate with insurers, cybersecurity experts, and space industry stakeholders to develop a Scotland-specific insurance standard for space-cyber risk. This standard would outline required cybersecurity practices (e.g., multi-factor authentication, AI-driven threat detection) that space ventures must adopt to be eligible for coverage.

2. Incentivise Cybersecurity through Insurance Premium Reductions

Rationale: By incentivising advanced cybersecurity measures through reduced insurance premiums, insurers can drive the adoption of cutting-edge security technologies in Scotland's space sector. This aligns with the broader goal of strengthening Scotland's position in secure space technology.

Action: Work with Scottish insurers to design performance-based insurance models that offer reduced premiums for space operators who demonstrate high cybersecurity standards, such as continuous monitoring or automated encryption updates. This would encourage companies to adopt advanced security practices to qualify for these savings.

3. Develop Blockchain-Based Insurance Solutions for Space Data Integrity

Rationale: Blockchain technology provides a tamper-proof record of operations, allowing insurers to verify the integrity of satellite data. Leveraging this technology aligns with Scotland's goal of fostering innovation within the space-cyber domain.

Action: Partner with blockchain technology providers to pilot blockchain-based solutions for space insurance policies. These solutions could be used to verify satellite data integrity, ensuring that any tampering or anomalies are automatically recorded and reported, reducing risks associated with cyberattacks on space assets.

4. Establish a Space-Cyber Insurance Innovation Hub

Rationale: Creating a dedicated hub would promote research and development in space-cyber insurance products, building upon Scotland's expanding capabilities in both sectors. This aligns with prior recommendations to position Scotland as a leader in space-cybersecurity.

Action: Set up a Space-Cyber Insurance Innovation Hub in collaboration with Scottish universities, insurers, and space industry partners. This hub would focus on creating innovative insurance products for the space-cyber market, such as policies that cover quantum-encrypted satellite communications or blockchain-secured satellite monitoring.

5. Promote Awareness of Cyber Insurance as a Strategic Necessity

Rationale: Raising awareness of space-cyber insurance benefits would drive investment in cybersecurity, addressing one of the main challenges faced by Scotland's space industry. As insurance increasingly becomes a prerequisite for operational success, aligning with global trends will be essential.

Action: Launch a Scotland-wide initiative aimed at educating space sector stakeholders on the strategic importance of cyber insurance. This could include workshops, seminars, and publications detailing the role of insurance

in mitigating cyber risks and ensuring operational continuity for space missions.

6. Pilot Quantum Encryption Solutions as an Insurance Mandate

Rationale: Quantum encryption offers a high level of security for space communications and is becoming an attractive option for insurers. This aligns with Scotland's focus on promoting disruptive technologies within its space-cyber sector.

Action: Partner with quantum technology firms to pilot quantum encryption on satellite systems as part of an insurance mandate. This could involve offering insurance premium reductions for space operators who implement quantum encryption, fostering adoption of this technology in the Scottish space sector.

7. Facilitate Access to Global Insurance Markets for Scottish Space Ventures

Rationale: By helping Scottish space companies access international insurance markets, Scotland can align its space sector with global standards, making it more attractive to foreign investors and insurers. This links with previous recommendations to enhance Scotland's international collaborations and global market positioning.

Action: Work with international insurance brokers and Scotland's trade agencies to provide space ventures with access to global insurance markets. This could involve connecting Scottish companies with insurers offering policies that cover advanced cybersecurity and space-cyber risks, thus enhancing Scotland's international competitiveness.

Conclusion: Insurance as a Catalyst for Scotland's Space-Cyber Growth

Insurance is no longer just a financial safety net in the space sector—it is a catalyst for driving cybersecurity innovation and commercial success. As insurers increasingly require robust cybersecurity measures, space operators must rise to the challenge, embedding advanced security technologies into their mission planning from the outset.

For Scotland, this presents a unique opportunity. By aligning its space ventures with international insurance standards and developing specialised products tailored to the needs of the space-cybersecurity sector, Scotland's insurance industry can play a pivotal role in securing the nation's space future. This, in turn, will enhance Scotland's reputation as a leader in both the space and cybersecurity sectors, attracting investment, fostering innovation, and ensuring long-term resilience in an increasingly competitive global market.

This chapter aligns with the United Nations Sustainable Development Goals

SDG 9 – Industry, Innovation, and Infrastructure

SDG 8 – Decent Work and Economic Growth.

SDG 17 – Partnerships for the Goals

Chapter Six: Future-Proofing Scotland's Space Sector: Overcoming the Skills Shortage

So far, this report has explored the global space-cyber posture, diplomacy, threats, investment, and insurance, but fundamentally, people are at the core of space-cyber innovation. This chapter confronts the urgent and growing skills shortage within the cybersecurity and space sectors, focusing on the unique challenges facing Scotland's rapidly expanding space industry. With a scarcity of skilled professionals in critical areas such as cyber security, artificial intelligence, machine learning, and secure communications, Scotland's ambitions to lead in space technology are at risk. These shortages represent a formidable barrier to future growth, innovation, and competitiveness on a global scale. Through a rigorous analysis of the current skills landscape, this chapter proposes actionable and transformative solutions—including targeted education programs, specialised apprenticeships, and strategic industry-academia partnerships—designed to close this gap. By proactively addressing these issues, Scotland can cultivate a resilient, high-calibre workforce capable of meeting the complex demands of the global space-cybersecurity sector, thereby securing its position as a leader in space technology and digital security.

Skills Gap

The skills shortages in both the cybersecurity and space sectors are critical issues that demand immediate attention, particularly in regions like Scotland, where the space industry is rapidly expanding. Globally, the cybersecurity industry faces a predicted shortfall of around four million professionals (ISC2, 2023; WEF, 2023), and these skills shortages are reflected in the UK.

Approximately 44% of UK businesses report basic cybersecurity skills gaps, such as a lack of confidence in setting up firewalls or managing secure data (DIST, 2024). Further, 27% of businesses report gaps in advanced skills like penetration testing, which are crucial for protecting complex systems, including those used in space operations (DIST, 2024). In addition, cloud security (35%), AI and machine learning (32%), and penetration testing (27%) are key areas where companies struggle to find talent (WEF, 2023). Despite some reductions in skills gaps in recent years, significant gaps remain in cryptography and communication security, where shortages have increased from 12% to 24%, a critical issue as secure communication is vital for space infrastructure (DIST, 2024). These gaps put both space assets and cybersecurity infrastructure at risk.

In the space sector, skills gaps are similarly pervasive. Around 72% of space organisations report shortages in software and data skills, particularly in AI and machine learning, which are becoming increasingly important for space operations (UK Space Agency, 2023). Hiring and retaining skilled staff is a growing challenge, with 48% of organisations struggling to hire, and 45% reporting that new hires lack essential skills (UK Space Agency, 2023). These challenges are having a major impact on business productivity, with 97% of organisations acknowledging the adverse effects of skills shortages (UK Space Agency, 2023).

Global Efforts to Address the Skills Gap

Countries like Germany, France, Japan, New Zealand, and the United States have recognised the urgency of this issue and are implementing national cybersecurity education and training programmes for Space. For example, the US National Initiative for Cybersecurity Education (NICE) is focused on expanding the cybersecurity workforce through public-private partnerships and tailored educational programmes. In Europe, the EU's Digital Europe Programme is investing in closing the skills gap through training and reskilling initiatives, especially in advanced technologies like AI and cybersecurity.

While these global efforts are essential for addressing the general cybersecurity skills gap, specific and more specialised skills are still lacking, particularly at the intersection of space and cybersecurity. Outlying Skills Gaps at the Intersection of Cybersecurity and Space remain a significant challenge, especially in areas that are crucial for ensuring the security of space operations.

Outlying Skills Gaps at the Intersection of Cybersecurity and Space

Several outlying skills are particularly critical at the intersection of the space and cybersecurity sectors:

- **Cryptography and Communication Security:** A shortage of cryptography expertise exists in 24% of cybersecurity firms, posing risks for space operations that rely on secure data transmission (DIST, 2024).
- **AI and Machine Learning:** Gaps in AI and machine learning are problematic for both sectors, with 32% of cybersecurity firms and 41% of space organisations reporting shortages. These skills are essential for threat detection and managing automated space systems (UK Space Agency, 2023).
- **Incident Response and Forensic Analysis**: In cybersecurity, 48% of businesses lack confidence in incident response capabilities, a gap that could lead to catastrophic consequences for space infrastructure in the event of a breach (DIST, 2024).
- **Cyber-Physical Systems Security**: Cyber-physical systems (CPS) security is vital for the control of space missions and integrated systems, yet the cybersecurity industry reports shortages in skills related to securing CPS, which impacts spacecraft and ground station operations (UK Space Agency,2023)

Below the table highlights the specific skills gaps within the cybersecurity and space sectors, while also identifying critical overlaps between the two industries, helping to pinpoint areas where targeted workforce development is needed to address these challenges.

Skill Category	Cybersecurity Sector (Skills Gaps)	Space Sector (Skills Gaps)	Intersection of Both Sectors
Software & Data	44% of UK businesses lack basic cyber security skills, including software	72% of organisations report gaps in software & data skills, including	Critical in both sectors for handling and processing data, securing operations, and

	management, secure data storage, and data handling [1].	AI, machine learning, and data analysis [2].	interpreting system vulnerabilities.
AI & Machine Learning	32% of businesses report shortages in AI and machine learning, key for automation, data analysis, and threat detection [1].	41% report gaps in AI & machine learning, crucial for automating space operations [2].	Automation and data-driven decision-making through AI are essential for cybersecurity and space exploration tasks.
Systems Engineering	Gaps in secure system architecture and advanced system design (55% of firms) [1].	39% of organisations report gaps in systems engineering [2].	Both sectors need secure system design to ensure operational integrity and protection against cyber threats.
Penetration Testing & Vulnerability Management	27% of businesses report gaps in penetration testing skills, vital for vulnerability assessment [1].	No direct equivalent but testing and diagnostics gaps exist in electronics design (43%) [2].	Both sectors need testing capabilities—penetration testing in cybersecurity and hardware/software testing in space.
Data Analysis & Modelling	18% of firms face gaps in advanced data analysis for monitoring and responding to cyber threats [1]	36% of space organisations report gaps in data analysis and modelling [2].	Data analysis is essential for both threat detection in cybersecurity and operational optimisation in space.
Electronics Design & RF Engineering	Gaps in secure electronics systems, including cryptography and communication security (24%) [1].	43% report gaps in electronics design, particularly RF engineering and electronics manufacturing for space operations [2].	Securing communication channels is critical for both satellites in space and cybersecurity defences.
Commercial Operations	Skills in business continuity, project management, and leadership (41%) [1].	51% of space organisations report gaps in commercial operations, including business development and project management [2].	Effective management of cybersecurity and space projects requires strong operations and planning.
Transferable Skills	34% report a lack of complementary (soft) skills such as communication, problem-solving, and teamwork in cyber teams [1].	38% report gaps in transferable skills like communication and teamwork [2].	Both sectors benefit from problem-solving, communication, and teamwork skills to align technical solutions with business goals.

[1] DIST, 2024 [2] UK Space Agency 2023

Without robust cybersecurity, Scotland's rapidly expanding space infrastructure is vulnerable to cyberattacks, which could compromise national security and economic growth. Investing in closing these skills gaps, particularly in cryptography, AI, and CPS security, will be critical for safeguarding Scotland's space infrastructure. Furthermore, developing a diverse and skilled workforce that bridges both space and cybersecurity will be essential for Scotland to remain competitive and innovative in this high-growth industry (UK Space Agency, 2023; DIST, 2024).

Opportunities for Scotland's Educational Institutions

Scottish universities, such as the University of Strathclyde, have a unique opportunity to become world leaders in space-cybersecurity education. By partnering with international universities such as the International Space University (ISU) industry and government agencies, universities can develop tailored programmes that address the critical skills shortages in both sectors.

Moreover, the education sector also has a real opportunity to expand its commercial offering to industry by creating tailored micro-credential modules in this emerging field. Micro-credentials can be developed and delivered in a short timeframe, thus contributing to the ambition of developing a highly skilled workforce and responding timely to industry challenges. Arguably if Scotland seeks to seize the opportunity, it could represent an exciting time for Scotland to position itself at the forefront of space-cyber education, providing the workforce needed to secure its expanding space infrastructure and create an in demand skilled workforce.

Management and Leadership Gaps

While Scotland's space and cyber sectors are uniquely positioned for growth, their potential is constrained by critical leadership and management gaps. These challenges arise from the complex demands of both the space and cybersecurity industries, which, when combined, require a unique blend of technical and strategic expertise. Effective leadership in this sector demands individuals capable of bridging these domains, essential for scaling Scotland's space-cyber capabilities and ensuring resilience. Leaders need informed, expert advice to navigate cyber threats effectively, underscoring the importance of cybersecurity expertise alongside other critical advisory roles (Smith, 2024, p. 4). This highlights the necessity of embedding cybersecurity knowledge at the highest levels of decision-making. Without such expertise, there is a heightened risk of underestimating cyber threats or failing to implement effective countermeasures, potentially leading to catastrophic security breaches. Below are some of the key challenges impacting both Space and Cyber:

1. High Turnover and Retention Challenges

The *UK Space Sector Skills Survey* (2023) underscores a persistent "brain drain" in the space industry, particularly at the middle-management level. This exodus of talent is driven largely by a lack of competitive career progression and compensation, with many professionals leaving for higher-paying roles in sectors like consulting. This trend weakens the sector's talent pipeline and disrupts continuity in leadership—a crucial concern for a sector that relies heavily on in-depth, domain-specific knowledge.

In parallel, the cybersecurity sector also faces high turnover rates among Chief Information Security Officers (CISOs), largely due to the immense pressure and liability concerns associated with the role. According to the Team8 report (2024), 54% of CISOs report significant well-being impacts due to liability concerns, and many are seeking additional legal protections as a result. The pressure and stress associated with cybersecurity leadership roles contribute to burnout and frequent turnover, leaving critical positions unfilled or filled by less-experienced individuals.

In the context of space-cybersecurity, these challenges are compounded. Leaders in this field need not only experience in managing complex space operations but also a strong grasp of the cybersecurity threats unique to space assets. Scotland's space sector, which is primarily made up of SMEs, often lacks the resources to retain such high-calibre leaders, further exacerbating the leadership gap. The reliance on external recruitment, which is both costly and time-consuming, means that the sector is struggling to build a consistent leadership pipeline that meets its unique demands.

2. Project Management and Strategic Oversight Deficits

Effective project management is fundamental to the success of long-term, high-stakes projects in the space sector, such as satellite development and spaceport operations. However, 67% of companies in the space sector report a lack of project management expertise (UK Space Sector Skills Survey, 2023). This shortfall is especially concerning given that space projects often require multi-year timelines, substantial budgets, and the ability to adapt to regulatory requirements that vary internationally. Without strong project management capabilities, space projects risk costly delays, misaligned priorities, and operational inefficiencies.

The cybersecurity sector faces similar challenges. Leaders in cybersecurity are responsible not only for technical security measures but also for providing strategic oversight in the face of rapidly evolving threats. However, many cybersecurity leaders lack the necessary training and experience to anticipate and mitigate the broad array of risks that space-cyber projects entail, which include both physical and digital security considerations.

In the context of space-cybersecurity, the need for project management and strategic oversight is even more acute. Leaders must oversee initiatives that involve satellite security, secure communications, and regulatory compliance, all of which require extensive coordination across technical and operational teams. The leadership gap in these areas means that Scotland's space-cyber projects may struggle to maintain alignment with broader strategic objectives, potentially limiting the sector's ability to compete internationally.

3. Cross-Sector Collaboration and Dual-Use Leadership

The intersection of space and cybersecurity necessitates a dual-use leadership approach, as technologies in this space often serve both commercial and defence applications. In the space sector, leaders must navigate the challenges of satellite operations, international regulations, and national security implications. In cybersecurity, leaders are responsible for safeguarding critical infrastructure from sophisticated threats, including AI-driven attacks, which have become more prevalent.

At their intersection, space-cyber leaders are expected to bridge these demands, operating across traditionally siloed domains. They need to collaborate with commercial partners, defence agencies, and regulatory bodies to ensure the security of space assets, all while driving innovation and maintaining operational efficiency. Currently, Scotland's leadership pool lacks the dual-use expertise needed for effective cross-sector collaboration. Leaders must be able to translate complex

technical challenges into strategic decisions that align with both commercial objectives and national security priorities.

4. Limited Internal Training and Succession Planning

Another factor exacerbating the leadership gap in Scotland's space-cyber sector is the limited availability of internal training and succession planning, particularly within SMEs. Without structured leadership development programs, many SMEs are forced to rely on external hires for senior roles, which can be both time-intensive and costly. This reliance on external recruitment disrupts organisational continuity and means that there is often a loss of institutional knowledge—a critical factor in a domain as complex as space-cyber.

The *UK Space Sector Skills Survey* (2023) highlights that 43% of space sector companies report insufficient training resources, which limits their ability to foster internal leadership pipelines. Additionally, the cybersecurity sector has seen similar trends, with limited opportunities for mid-level professionals to gain the necessary skills and exposure for senior leadership roles. The absence of structured progression pathways leaves emerging leaders without the support needed to transition into roles that require both technical and strategic expertise.

Practical Example: Executive Space Cybersecurity Training

An example of how these gaps is being addressed is the *Executive Space Cybersecurity Training* program, offered by the International Space University in partnership with the University of Strathclyde. This three-day course aims to provide senior executives with foundational knowledge in space-cybersecurity, covering:

- A comprehensive overview of space and cybersecurity integration.
- Satellite programming and vulnerability assessment.
- Threat detection, response strategies, and compliance.
- Insights into legal and strategic challenges in space-cyber operations.
- Simulation exercises that foster cross-sector collaboration.

The course provides leaders with a multidisciplinary perspective, equipping them with the skills needed to navigate the complexities of space-cyber projects. However, while this program is valuable, it highlights the broader challenge: Scotland needs systemic, consistent leadership development initiatives that go beyond isolated training sessions to build a sustainable leadership pipeline in space-cybersecurity. And the data from both the space and cybersecurity sectors reveal significant leadership and management gaps at their intersection, underscoring the need for Scotland to cultivate leaders with integrated, dual-use expertise. Addressing these gaps will be essential for Scotland to establish a competitive edge in space cybersecurity. By prioritising structured leadership development programs, cross-sector training, and retention strategies, Scotland can build a leadership pipeline that is resilient, adaptive, and prepared to meet the unique demands of the space-cyber domain.

Table of Leadership Gaps in Space and Cybersecurity

Category	Space Leadership Issues	Cyber Leadership Issues	Intersection of Space & Cyber (Leadership & Management)	Opportunities for Scotland
Liability and Scrutiny	Leadership in space is under pressure to manage liability for satellite failures, space debris, and risks of international conflict (Bates, 2024).	Cybersecurity executives are increasingly liable for breaches, AI-driven attacks, and regulatory non-compliance. CISOs face heightened scrutiny and legal concerns (Vainilavičius, 2024).	Both sectors face increasing regulatory and legal scrutiny, with leadership under pressure to ensure compliance and manage liability.	Scotland can create a unique space-cyber regulatory hub, providing specialised legal and risk consultancy services for space and cybersecurity leaders managing international treaties, satellite operations, and AI-driven cyber risks.
Well-being and Pressure	Space leaders face high psychological stress due to the stakes involved in launching missions, securing space assets, and international tensions (UK Space Agency, 2023).	Cybersecurity leaders experience rising stress and concern for personal well-being due to liability, the growing sophistication of cyberattacks, and board-level pressure (Vainilavičius, 2024).	Both sectors report a negative impact on personal well-being, driven by high-risk, high-pressure environments where mistakes can have serious consequences.	Scotland could provide leadership wellness and resilience training, focusing on managing stress and risk in high-pressure environments like space cyber. This would position the country as a destination for high-quality executive training.
Legal Safeguards	Space sector leaders may seek legal counsel and additional safeguards related to satellite collisions, mission failures, or breaches of international treaties (Vainilavičius, 2024).	Cybersecurity executives, particularly CISOs, are increasingly turning to legal counsel and adjusting contracts to protect against personal liability due to breaches.	Leaders in both sectors are turning to legal protections and adjusting contracts to mitigate risks from the rising complexity of liability.	Scotland has an opportunity to develop a legal framework and advisory services for mitigating leadership liability in space-cyber sectors, offering specialist insurance products and legal consulting for emerging risks in both industries.
Technological Complexity	The integration of AI in satellite systems, automation in space missions, and emerging technologies like quantum computing adds to the complexity space leaders must navigate (UK Space Agency, 2023).	CISOs must address new AI-driven cyber threats like deepfakes and advanced phishing techniques, along with securing AI development and deployment pipelines (Vainilavičius, 2024).	Both sectors deal with the challenges of rapidly evolving technologies, including AI, which requires new skillsets and leadership strategies to manage effectively.	Scotland can invest in research and development focused on AI and cybersecurity within the space sector, positioning itself as a centre of excellence for space-cyber technology integration and leadership in

				handling emerging risks.
Budget Increases	Space ventures are seeing increased budgets for enhancing satellite security, ensuring robust ground control systems, and managing space assets (Growth Markets, 2024).	Cybersecurity teams report larger budgets, particularly to tackle AI-related threats and ensure robust data protection.	Budget increases in both sectors are driven by the need to safeguard critical infrastructure from emerging threats and ensure operational resilience.	Scotland could capitalise on these budget increases by offering specialised consulting services to help organisations manage these expanding resources and deploy them effectively in space-cyber operations.
Skills Shortages	Leadership gaps in space stem from a shortage of experienced professionals in satellite management, AI, and data analysis for secure space operations (UK Space Agency, 2023).	Cybersecurity faces significant leadership challenges due to skills shortages in areas like AI, machine learning, cryptography, and incident response (DSIT, 2024).	Both sectors experience critical skills shortages in AI, data management, and secure system design, affecting the ability of leaders to manage space-cyber risks effectively.	Scotland can establish training centres or partnerships with universities to develop the next generation of leaders equipped with both space and cybersecurity skills, particularly in AI and data management.
AI and Emerging Risks	Space sector leadership must prepare for AI-driven satellite automation, risk management, and decision-making systems that are integral to future space missions.	CISOs are increasingly focused on addressing AI-driven threats such as phishing, deepfakes, and unregulated AI systems (shadow AI), which present new cyber risks (Vainilavičius, 2024).	Both sectors are heavily impacted by AI, and leadership must focus on mitigating risks while leveraging AI to enhance operational efficiency and resilience.	Scotland has the opportunity to lead in AI governance and risk management, particularly in industries where space and cybersecurity overlap. AI leadership programmes and initiatives could be a competitive advantage.
Data Protection	Space leaders must secure sensitive satellite communication and mission-critical data, ensuring systems are protected against espionage and breaches (UK Space Agency, 2023).	CISOs are prioritising AI-related data privacy, securing third-party systems, and addressing insider threats.	Data protection is a shared priority, with both sectors focused on securing critical data from cyber threats, especially as AI becomes more integral.	Scotland could become a leader in space and cybersecurity data protection standards, offering expertise in compliance, governance, and protecting sensitive data in space missions and AI-integrated cybersecurity systems.

Neurodiversity at the Intersection of Space and Cybersecurity in Scotland

As Scotland aspires to be a leader in space cybersecurity, incorporating neurodiverse talent presents an opportunity to address critical skill gaps and foster innovation within this emerging field. Neurodiversity encompasses individuals with a range of neurological differences, including autism, ADHD, and dyslexia, who often exhibit unique abilities in areas such as pattern recognition, logical reasoning, and sustained focus—traits particularly relevant for complex cybersecurity roles (Wiederhold, 2024). In an industry marked by rapid technological advancement and a persistent skills shortage, the recruitment and retention of neurodiverse professionals could become a strategic advantage for Scotland.

The integration of neurodiverse individuals into cybersecurity roles, however, requires the adaptation of traditional hiring and management practices, which often pose barriers. Traditional interview processes typically emphasise soft skills, eye contact, and other social competencies that may disadvantage neurodiverse candidates, despite their technical capabilities (UK Cyber Security Council, 2023). Scotland's space cybersecurity sector can differentiate itself by adopting more inclusive practices, such as skills-based assessments and providing job previews or structured tasks that focus on technical aptitude over social interaction. This approach not only opens doors to neurodiverse talent but also supports cognitive diversity, which has been shown to reduce groupthink and improve problem-solving capabilities within teams (RAND Corporation, 2023).

In practice, a neurodiverse workforce offers specific strengths that could enhance Scotland's resilience in space cybersecurity. Studies indicate that individuals with autism, for example, can process visual information more rapidly and with greater accuracy, making them adept at identifying patterns and anomalies within vast datasets (MITRE, 2019; SAP, 2022, Kang, 2023). Similarly, people with ADHD often excel in dynamic environments requiring rapid response and adaptability, as they can maintain focus on critical tasks under pressure (Deloitte, 2024). These strengths align with the needs of space cybersecurity, where the ability to detect and counteract cyber threats in real-time is essential.

Moreover, building a neuroinclusive workplace is not only beneficial for the productivity and effectiveness of teams but also aligns with Scotland's broader social and ethical goals. The potential for neurodiverse individuals to contribute meaningfully to cybersecurity has already been demonstrated by initiatives such as MITRE's programme, which provides customised training to help neurodiverse hires thrive in cybersecurity roles. These efforts show how tailored support structures, such as clear communication guidelines, flexible work environments, and accommodations for sensory needs, can make the workplace more accessible and empowering for neurodiverse employees (Wiederhold, 2024). By prioritising these adaptations, Scotland can set a benchmark for diversity and inclusion within the field, positioning itself as a leader in both space cybersecurity and neuro-inclusion.

Embracing neurodiversity also offers a practical response to the cybersecurity skills gap. With the sector facing a shortage of over 14,000 skilled professionals, tapping

into underrepresented groups, including neurodiverse individuals, is essential to closing this gap. The UK Cyber Security Council emphasises that neurodiversity brings a fresh perspective to cybersecurity challenges, particularly as cognitive diversity can lead to faster problem-solving and more innovative solutions (UK Cyber Security Council, 2023). By fostering a neuroinclusive culture, Scotland can attract a broader talent pool and enhance its cybersecurity infrastructure, strengthening its position within the global space sector.

Women's Leadership at the Intersection of Space and Cybersecurity: Challenges and Strategic Imperatives for Scotland

The intersection of space and cybersecurity presents a powerful opportunity for Scotland. However, as with many high-tech fields, this sector remains dominated by men. Women make up only 29% of the UK space workforce and 17% in cybersecurity, highlighting not just a gender imbalance but also a range of systemic challenges that limit diversity and inclusion (UK Space Skills Alliance, 2020; Muncaster, 2024, Brown, 2020; Brown, 2021). This underrepresentation is not only a matter of numbers but reflects broader issues such as discrimination, harassment, and persistent pay gaps, which create a complex landscape for women leaders in the space-cyber domain.

Discrimination remains a pervasive issue in both sectors, with 41% of women in the space workforce reporting experiences of prejudice, compared to only 10% of men (Space Skills Alliance, 2020). Furthermore, women in cybersecurity often face exclusion and harassment, with many expressing concerns about not being taken seriously or being subjected to a lack of inclusivity and respect (Deloitte, 2024). Such challenges can discourage women from advancing into leadership roles, where they are critically needed to drive innovation and foster a more inclusive, resilient space-cybersecurity field. In Scotland, where the space sector is expanding rapidly, addressing these barriers is essential not just for equity but for the sector's strategic growth.

The pay gap is another significant barrier, with women consistently earning less than men—a disparity that widens with age and seniority, from £1,000 in junior roles to £9,000 in senior positions (Space Skills Alliance, 2020). These financial inequities contribute to what is often called the "leaky pipeline," as talented women leave the sector or avoid it altogether due to lack of career advancement and recognition. In addition, nearly half of the women in the space sector report feeling unwelcome, an issue compounded by the lack of clear paths to promotion: women are less likely to hold senior roles compared to their male counterparts, even when they have comparable experience (Space Skills Alliance, 2020). This data indicates that the sector's culture and structures are not yet conducive to retaining and empowering women, which could limit Scotland's ability to compete globally if left unaddressed.

At the leadership level, women's perspectives are crucial for the development of adaptive strategies to secure space assets against sophisticated cyber threats. Diverse leadership teams have been shown to perform better in high-stakes environments and are more adept at spotting risks and developing innovative solutions (Reis & Menezes, 2019). However, female leaders in cybersecurity often

face unique biases: research indicates that employees may show less compliance with security measures advocated by women leaders, due to entrenched stereotypes about gender and leadership style (Bansal & Axelton, 2024). Such biases not only undermine women's leadership but can also detract from overall organizational effectiveness, especially in sectors like space-cybersecurity where the stakes are exceptionally high.

For Scotland, the path forward involves recognising these challenges and implementing targeted initiatives to support women at all career stages. Establishing mentorship programs, promoting transparent pay practices, and creating inclusive workplaces are essential steps toward attracting and retaining female talent in the space-cybersecurity field. This proactive approach will not only help bridge existing skill gaps but will also position Scotland as a leader in developing an inclusive, forward-looking workforce capable of navigating the complexities of an interconnected, high-risk global environment. Addressing these gender disparities is not merely an ethical imperative; it is a strategic one that will allow Scotland's space-cybersecurity sector to thrive on the international stage.

Thinking Outside the Box: The Need for Innovative Space Cyber Education

In responding to multifaceted challenges and recognising the need for a more inclusive and representative workforce also requires out-of-the-box thinking when it comes to training and preparing professionals for the demands of space cybersecurity. One effective model for this is the Hack-a-Sat initiative, which brings together hackers and cybersecurity experts in a competitive environment to find and exploit vulnerabilities in satellite systems. These types of simulation-based challenges provide participants with invaluable experience in detecting and mitigating potential cyber threats in real time. As space ventures increasingly rely on satellite communication and mission-critical systems, it is essential for cybersecurity professionals to experience the complexities of defending space assets firsthand.

Introducing similar simulation exercises in UK education programmes—focused specifically on space infrastructure—would ensure that future leaders can think on their feet, develop cyber resilience, and respond to evolving threats with confidence. Initiatives like Hack-a-Sat could also be expanded into annual competitions hosted in the UK, fostering international collaboration, and drawing global talent to the country's space sector. Expanding these types of training programmes and integrating more hands-on experience will be essential for ensuring that the UK can meet future demand.

The Need for a Targeted Space Cybersecurity Pathway

While there are already funding initiatives and training programmes in place for both space technologies and cybersecurity, there remains a critical gap at the intersection of these fields. It is no longer sufficient to hope that cybersecurity skills will naturally spill over into the space sector—space cybersecurity requires a dedicated pathway to ensure that the unique challenges of securing space infrastructure are met with focused expertise. Cybersecurity for space involves distinct vulnerabilities and

risks—from defending satellite communications to protecting mission-critical systems—and these demand specialised training. The UK cannot afford to rely on existing, generalised programmes to fill this gap. It is essential to develop a bespoke pathway for space cybersecurity that integrates both fields from the outset.

This pathway should be designed to equip professionals with cross-disciplinary knowledge, combining cybersecurity principles with a deep understanding of space systems. Hack-a-Sat-style competitions, simulation exercises, and hands-on training with real-world scenarios should be central to this approach. The absence of a tailored pathway leaves the UK exposed to significant cybersecurity risks, which could derail its ambitions to lead in the global space sector.

The Consequences of Inaction

Failing to address the skills gap will have serious implications for the Scotland's economic growth and national security. With space-based technologies underpinning everything from financial transactions to national defence systems, a shortage of skilled professionals could leave the UK vulnerable to cyberattacks. As has already been seen from incidents like the Viasat cyberattack, which targeted satellite communications, the consequences of insufficient cybersecurity expertise can be devastating. Without a skilled workforce, the UK's space sector could struggle to respond effectively to similar incidents, leaving critical infrastructure exposed to disruption. Closing the skills gap offers the UK an opportunity to create a new generation of experts who can secure space ventures against evolving cyber threats. By investing in education pathways and training programmes, the UK can ensure that the talent pipeline is robust enough to meet the challenges of the future.

Recommendations for Addressing Skills Shortages in Scotland's Space and Cybersecurity Sectors

1. **Develop Specialised Space-Cybersecurity Education Pathways**

   Rationale*:* As the space and cybersecurity sectors continue to converge, there is a critical need for a workforce with skills specific to the unique vulnerabilities of space systems. Currently, most educational programs either focus on space technology or cybersecurity but rarely address the intersection of the two, creating gaps in expertise for defending Scotland's growing space infrastructure.

   Action: Scotland should establish dedicated educational pathways that integrate space and cybersecurity studies. Universities could offer specialised degrees, micro-credentials, or joint certifications that address both fields. This approach would provide students with hands-on experience in areas such as secure satellite communication, threat detection for space systems, and cryptography for space operations.

2. **Launch an Industry-Academia Partnership Initiative**

   Rationale: Closing the skills gap in Scotland's space sector requires a collaborative approach between academia and industry to ensure that training and education programs align with real-world needs. Industry partnerships can help inform curriculum development, provide internship opportunities, and facilitate research in space cybersecurity.

   Action: Scotland should establish a structured partnership program between universities, space companies, and cybersecurity firms. This initiative could involve developing curricula informed by industry leaders, offering internship placements for students, and creating joint research projects that focus on space cybersecurity challenges. Funding support from the government for these partnerships would further strengthen Scotland's innovation ecosystem.

3. **Expand Leadership Development Programs in Space Cybersecurity**

   Rationale*:* The rapid evolution of space-cyber threats requires leaders who not only understand advanced technologies but also possess the management skills to navigate high-stakes situations. Currently, Scotland faces a shortage of such leaders, which could limit its ability to scale and maintain its competitive edge in the global space market.

   Action: Establish a leadership development program focused on space-cybersecurity, targeting mid-career professionals in the space and cybersecurity sectors. This program could include mentorship, strategic project management training, and practical scenarios related to space-cyber threats. Scotland could also partner with institutions like the International Space University to offer advanced executive training tailored to dual-use leadership.

4: Promote Diversity and Inclusion in the Space-Cyber Workforce

Rationale*:* A more inclusive workforce that incorporates diverse perspectives—such as those from neurodiverse individuals and women—can enhance innovation and resilience within the space-cyber sector. Currently, underrepresented groups face barriers that limit Scotland's ability to leverage a broader talent pool.

Action*:* Scotland should implement targeted recruitment initiatives, including partnerships with advocacy groups, tailored hiring practices for neurodiverse individuals, and mentorship programs for women in STEM. Establishing inclusive hiring practices and providing workplace accommodations will help attract and retain talent from diverse backgrounds, fostering a culture of innovation.

5: Prioritise Research and Development in Emerging Technologies

Rationale: Emerging technologies like AI, machine learning, and quantum computing are essential for building a resilient space-cybersecurity infrastructure. However, Scotland's space sector currently faces a shortage of professionals skilled in these areas, which could limit its ability to deploy secure space systems.

Action*:* Scotland should prioritise funding and support for R&D projects in emerging space technologies, particularly in AI-driven threat detection and quantum-resistant encryption. This could involve grant programs for SMEs, research funding for university labs, and partnerships with international organisations. By focusing on these areas, Scotland can strengthen its technological capabilities and safeguard its space assets against advanced cyber threats.

Conclusion

The convergence of the space and cybersecurity sectors presents a complex landscape for Scotland, offering both significant opportunities and critical challenges. As Scotland continues to position itself at the forefront of the global space economy, leadership and management gaps in these sectors must be urgently addressed to fully capitalise on emerging opportunities. The growing reliance on advanced technologies, such as AI, machine learning, and cryptography, highlights the need for robust leadership that can navigate the risks posed by cyber threats, while simultaneously steering innovation and operational integrity within the space industry.

Strategic investment in leadership development, alongside targeted education and training initiatives, is essential to bridging the skills gaps in both technical and managerial roles. Collaborations between academia, industry, and government will be vital to build a resilient workforce capable of safeguarding Scotland's expanding space infrastructure. With focused efforts in leadership and skills enhancement, Scotland has the potential to not only secure its space assets but also play a pivotal role in shaping the future of the global space-cybersecurity nexus. The time to act is now, as the ability to lead and innovate will determine the country's competitive edge in the rapidly evolving space sector.

This chapter aligns with the United Nations Sustainable Development Goals:

SDG 4 – Quality Education:

SDG 5 – Gender Equality:

SDG 8 – Decent Work and Economic Growth.
SDG 9 – Industry, Innovation, and Infrastructure:
SDG 10 – Reduced Inequalities:
SDG 17 – Partnerships for the Goals:

Chapter Seven: Space Cybersecurity in Scotland- Predictions

Having explored the multifaceted aspects of Scotland's growing space sector—from its global space cyber posture, diplomacy, and emerging threats to the critical roles of investment, insurance, and skills—the focus now turns to the future. The final chapter shifts from examining the current landscape to envisioning Scotland's future leadership in space cybersecurity. This chapter will explore how Scotland can leverage its strengths and expertise to anticipate and address the evolving challenges and opportunities that will define the space industry by 2050, positioning itself as a global leader in the secure and sustainable growth of space-based technologies and infrastructure.

Securing Scotland's Space Economy in 2050 – The Age of Celestial Innovation

By 2050, space will be an integral part of global economic infrastructure, and Scotland will be at the forefront of its cybersecurity. The Digital Space Shields protecting space assets will leverage quantum encryption (Krelina, 2023, Snatiago, 2023, Inglesant,et al 2018) AI-driven adaptive cybersecurity systems, and nanotechnology-based self-healing defences. As space operations grow more sophisticated, so too will the cyber threats.

Scotland could play a key role in leading a Quantum Cybersecurity Alliance, providing interplanetary secure communication networks. These networks could protect spacecraft, satellites, and space stations from quantum-powered cyberattacks, which could breach traditional encryption systems. Through predictive AI, Scotland's cybersecurity systems could anticipate and neutralise cyber threats before they manifest, ensuring the continuity of space-based operations and protecting critical infrastructure such as asteroid mining fleets and space habitats.

New Horizons in Space Cybersecurity: The "Shareable Brain"

One of the most groundbreaking advancements by 2050 could be the development of intergenerational knowledge databases—or the "shareable brain" (Lemac-Vincere. 2024). These vast digital repositories of human experience, knowledge, and skills would be stored in secure, quantum-proof in orbital data centres (Allan, 2023). Individuals could upload their cognitive data, contributing to a collective pool of knowledge that could be passed on through generations.

Securing these databases will be of the utmost importance. A breach could compromise sensitive personal memories, scientific discoveries, or even strategic military data. Scotland, as a leader in space cybersecurity, could develop systems to safeguard these cognitive archives using quantum-secured off world storage systems combined with AI-driven access control to prevent misuse, theft, or tampering.

Space Mining and Resource Extraction: Scotland's Role in the New Space Economy

By 2050, space mining (Glen and Gordon, 1998; Pace, 2023) could be one of the largest industries, with robotic mining drones extracting trillions of pounds worth of resources from asteroids. These operations would generate vast amounts of data, making them prime targets for cyberattacks. Threat actors could manipulate mining data, hijack fleets, or disrupt entire mining operations, leading to devastating economic losses.

Scotland's spaceport hubs and AI-based cybersecurity frameworks could be at the forefront of defending these operations. Self-repairing nanotechnology could secure mining fleets from both physical damage and cyber vulnerabilities. Scotland's innovations in AI-driven mining management systems will ensure that all operational data and logistics are encrypted, preventing any unauthorised access or tampering.

Autonomous Resource Chains and Cybersecurity

By 2050, Scotland could also lead in the development of autonomous space resource chains, overseeing the secure transport of mined materials from asteroids back to lunar or Earth-based spaceports. However, these supply chains, reliant on AI, will be vulnerable to cyber threats like AI system manipulation and supply chain data hijacking.

To protect these operations, Scotland could pioneer space resource cybersecurity protocols that secure every step of the supply chain—from the moment the resources are extracted to their arrival on Earth. These protocols will ensure that Scotland's space mining industry remains resilient against cyberattacks aimed at disrupting supply or stealing critical resources.

Celestial Currency: The Emergence of Space-Based Financial Systems

By 2050, celestial currencies such as "astro-dollars" or "space pounds" could be used for interplanetary transactions. Scotland's established fintech sector could play a leading role in securing these transactions with quantum-resistant encryption and AI-driven financial security systems. These systems could autonomously detect fraud, validate transactions, and protect against complex cyberattacks designed to exploit the time delays and vulnerabilities associated with interplanetary commerce.

Interplanetary Financial Networks and Cybersecurity

Interplanetary financial networks could handle more than simple transactions; they will support value exchanges between planets, moons, and space stations, making them a primary target for cybercriminals. Scotland could develop AI-enhanced blockchain networks (Bikos, A.N. & Kumar, S.A.P, 2022) that could allow for secure,

real-time celestial currency exchanges, ensuring that space commerce operates smoothly and without disruption.

Scotland's fintech expertise could also extend to designing space-specific trade and taxation systems, working with international regulatory bodies to ensure that space commerce is both secure and compliant with Earth-based governance. This will make Scotland a hub for secure interplanetary financial transactions and trade management.

Flying Cars, Autonomous Systems, and Space Transport: Securing the Future of Space Mobility

By 2050, fleets of autonomous flying cars (Van Der Wees, 2024) could be transporting goods and passengers between Earth and space. These vehicles will rely on satellite-based navigation and communication, making them vulnerable to cyberattacks such as satellite signal manipulation, GPS spoofing, and cyber hijacking.

Scotland could lead in the development of AI-driven transport security systems that defend these vehicles against cyber threats in real time. Neural-linked control systems—where operators use brain-computer interfaces (BCIs) to control fleets remotely—will provide fast and efficient responses to cyberattacks, helping to neutralise threats before they can cause significant damage.

Spaceports as Cyber Defence Hubs

Scottish spaceports could act as cyber defence hubs (Lemac-Vincere, 2024), overseeing the cybersecurity of autonomous transport fleets. These hubs could deploy AI-enhanced threat detection systems capable of identifying and stopping cyberattacks on space transport networks. Scotland could become a leader in creating and maintaining secure spaceport operations, ensuring safe travel across Earth and space.

Space Cyber Executive Training: A Global Leadership Initiative

By 2050, space cybersecurity will be a core competency required across all sectors involved in space entrepreneurship. Scotland could be home to the Space Cyber Executive Training Course, a programme designed by the University of Strathclyde in 2024 (Lemac-Vincere) to equip leaders from across the globe with the skills to protect space infrastructure from cyberattacks.

This course in 2050 could feature immersive holographic simulations that allow participants to experience cyberattacks on space assets in real time. Executives on the course learn how to secure satellites, spaceports, and autonomous vehicles using only neural commands. The programme will include real-time scenarios where participants must defend against space ransomware attacks, AI-driven cyber warfare, and satellite hijacking—offering a hands-on approach to mastering the complexities of space cybersecurity. Scotland's expertise in space cyber education

will place it at the forefront of training a new generation of leaders equipped to protect space-based operations in a rapidly evolving cyber landscape.

Education and Workforce Development: Preparing Scotland for the Space Economy

Scotland's universities, such as the University of Strathclyde, will be world leaders in space cybersecurity research and education by 2050. Scottish institutions will not only produce graduates with advanced technical skills but also offer specialised programmes in space-related cybersecurity. Scotland will continue to work in partnership with international organisations such as NASA, ESA (European Space Agency), and leading private space companies to develop cutting-edge research and development programmes that keep Scotland at the forefront of innovation. Programmes like space cyber apprenticeships will provide hands-on experience, ensuring that the next generation of space cybersecurity professionals are equipped to defend against evolving threats.

Ethics in Space Cybersecurity: Safeguarding the Future

By 2050, space cybersecurity will involve more than just technological solutions—it will require robust ethical frameworks. Scotland could lead in developing ethical guidelines that ensure space cybersecurity respects privacy, transparency, and fairness. As space-based data collection expands, Scotland could champion the development of systems that protect individual privacy and prevent the abuse of power by governments or corporations operating in space.

Scotland could also play a crucial role in ensuring that space mining, trade, and financial systems operate ethically. By working closely with global frameworks which may replace or enhance the Artemis Accords and the Outer Space Treaty, Scotland could contribute to the development of fair governance structures that promote sustainability and equitable resource distribution in space.

The potential developments suggested above over the next 25-year horizon seek to map out the technological advancements expected by 2050, the following table outlines the status of key technologies, their mid-term developments, long-term projections, and potential leadership opportunities for Scotland.

Table of Key Technologies and Scotland's Leadership Opportunities

Technology	Current Status (2020s)	Mid-Term (2030s)	Long-Term (2050)	What This Means for Scotland
Quantum-Resistant Cryptography	NIST has selected the first algorithms (e.g., CRYSTALS-Kyber) for quantum-resistant encryption. Standardisation expected by the mid-2020s.	Quantum-resistant encryption is widely adopted across critical industries like finance, government, and space.	Fully adopted as the global standard. AI-enhanced cryptography evolves dynamically to respond to new threats.	Scotland could lead in implementing quantum-resistant cryptography for space communications and secure interplanetary transactions, ensuring leadership in space finance and spaceport security.

Quantum Computing	Early quantum computers exist but are experimental, with limited practical use cases.	Capable of solving more complex problems, but not yet able to break classical encryption.	Fully developed, capable of breaking classical encryption systems. Quantum computers will be widely used in research and industry.	Scotland could establish itself as a hub for quantum computing research, advancing quantum-secure space communications, and collaborating with global research centres to further AI-enhanced quantum encryption systems.
AI-Driven Cybersecurity	AI is currently used for real-time threat detection and response in cybersecurity systems.	AI systems become integrated into cryptography, adapting protocols dynamically to counter emerging threats.	AI-enhanced cryptography evolves autonomously, continuously updating defences in response to new global threats.	A potential area for leadership for Scotland is in AI-driven cybersecurity for space operations, where adaptive AI systems defend spaceports, satellites, and space-based financial systems in real time.
Neural Interfaces (BCIs)	BCIs are in the research phase, allowing limited control of prosthetics and basic devices.	BCIs allow specialised users to control digital systems in real-time, with applications in healthcare and defence.	Fully integrated into decision-making environments, allowing space operators to control space systems with neural signals.	Scotland could become a leader in BCI research for space systems, developing neural-linked interfaces for controlling space habitats, fleets, and security systems in high-risk space environments.
Self-Healing Materials & Nanotech	Nanotechnology and self-healing materials are in early research and development stages.	Early applications of self-healing materials emerge in aerospace and defence industries.	Self-healing nanotech and materials are widely used in space infrastructure, autonomously repairing physical damage and cyber vulnerabilities.	Scotland could lead in the development of self-healing nanotechnology for spaceports and satellites, positioning itself as a leader in space sustainability and reducing space infrastructure maintenance costs.
Holography & Immersive Simulations	Basic holographic technologies exist but are primarily used for entertainment or limited AR applications.	Holographic communication becomes more widespread for business and specialised applications, with improvements in resolution and depth.	Full-body, ultra-realistic holographic telepresence is widely used, making remote collaboration as effective as in-person meetings.	A potential area for leadership for Scotland is to create holographic space operations centres, where holography allows real-time collaboration between Earth-based space agencies and interplanetary operations, ensuring efficient space mission management.

Recommendations for Scotland

As Scotland rises as a global leader in space and cybersecurity, it will face challenges from international competition, particularly from spacefaring nations such as the United States, China, and India. Furthermore, ethical, and geopolitical concerns surrounding space resource extraction and interplanetary governance may lead to tensions that require careful navigation. Scotland will need to work closely with global frameworks, such as the Artemis Accords and the Outer Space Treaty, or those which replace them to ensure that space exploration remains a fair and sustainable endeavour.

1. Establish a Future Foresight Initiative in Space Cybersecurity

Rationale: Anticipating future challenges is crucial as the space sector continues to grow. A foresight initiative will enable Scotland to proactively identify and address emerging trends in space and cybersecurity, helping to secure a competitive edge.

Action: Develop a dedicated team to conduct horizon scanning and scenario planning, collaborating with academic institutions, government agencies, and private sector partners. This team would assess potential risks, technological advancements, and geopolitical shifts that may impact Scotland's space infrastructure over the next few decades.

2. Develop Advanced Space Cyber Training and Education Programs

Rationale: Building a workforce with specialised skills in space cybersecurity is essential for Scotland's future growth. Advanced training and education programs will prepare the next generation to handle the complexities of emerging space technologies.

Action: Expand existing programs to include topics like quantum encryption, AI-driven cybersecurity, and space-specific cyber risk management. Partner with international organisations to offer hands-on learning experiences, simulations, and advanced practical exercises that equip students and professionals for the future of space cybersecurity.

3. Prioritise Ethical Frameworks and Governance in Space Cybersecurity

Rationale: As space operations and commerce grow, developing ethical frameworks will be critical to promoting responsible conduct and securing Scotland's role as a leader in ethical space practices.

Action: Collaborate with global space agencies, academic institutions, and ethics organisations to establish ethical guidelines for data privacy, space resource management, and AI usage. This initiative can position Scotland at the forefront of responsible space exploration, ensuring that future missions align with global ethical standards and promote sustainable practices.

4. Invest in Cross-Disciplinary Research and Innovation in Emerging Technologies

Rationale: Emerging technologies like AI, quantum computing, and blockchain will reshape space cybersecurity. Cross-disciplinary research will enable Scotland to remain at the cutting edge of technological advancement.

Action: Encourage collaboration across academia, industry, and government to support research addressing critical space cybersecurity challenges. Target funding programs to drive innovation in autonomous security systems, adaptive threat detection, and next-generation encryption, allowing Scotland to develop solutions for future space missions.

5. Build a Global Collaborative Network for Space Cybersecurity

Rationale: International collaboration is essential for advancing cybersecurity in space as threats grow increasingly complex and cross-border. A collaborative network can enhance Scotland's role in shaping global space cybersecurity policies and practices.

Action: Form partnerships with international space agencies, cybersecurity organisations, and research institutions for knowledge exchange and joint projects. Scotland could lead or participate in global initiatives focused on establishing security standards, R&D, and information-sharing networks, helping to create a unified approach to space cybersecurity.

6. Promote Public-Private Partnerships for Sustainable Space Investment

Rationale: Robust public-private partnerships can provide both financial support and technical expertise necessary for secure and resilient space systems, especially as space-cybersecurity requirements continue to grow.

Action: Facilitate partnerships between government agencies, private companies, and research institutions to fund space cybersecurity projects. Focus on developing foundational infrastructure, supporting innovative start-ups, and creating a thriving space sector ecosystem, ensuring Scotland remains at the forefront of investment and technological innovation.

Conclusion

By 2050, Scotland could be set to become a global leader in space and cybersecurity, using cutting-edge technologies such as quantum-resistant cryptography, AI-driven security systems, and self-healing nanotechnology to protect space operations. Through its education, leadership in space cyber training, and role in securing the future of space exploration, Scotland could be at the heart of the next frontier—both in space and in the cybersecurity landscape that supports it, if it acts now.

This chapter aligns with the United Nations Sustainable Development Goals:

SDG 9 – Industry, Innovation, and Infrastructure:

SDG 8 – Decent Work and Economic Growth

SDG 17 – Partnerships for the Goals:

Conclusion: Scotland's Role in the Evolving Space and Cybersecurity Landscape

As the global space race and the cybersecurity landscape evolve, Scotland is uniquely positioned to play a significant role in shaping the future of these sectors. This report has highlighted how space and cybersecurity, once separate domains, are now intricately linked, and how global power dynamics are shifting as nations seek to assert dominance in these critical areas. Scotland's strengths such as Scotland's geographic advantage, growing space industry, and burgeoning expertise in cybersecurity place it at the crossroads of these developments. Scotland's contributions to satellite manufacturing, data analytics, and spaceports provide a strong foundation for Scotland to emerge as a leader in space technology. However, weaknesses such as the cybersecurity skills gap and the limited capacity of SMEs to implement robust cybersecurity measures pose significant challenges. As space assets become increasingly vulnerable to cyber threats, the future of Scotland's space sector depends on embedding cybersecurity at the heart of all space operations.

Looking ahead, opportunities are plentiful. By aligning with the UK's national security strategy and strengthening international partnerships, Scotland can not only protect its space assets but also contribute to global efforts in securing the space domain. Moreover, investing in AI-driven threat detection, quantum encryption, and fostering innovation offers Scotland the chance to lead globally in space-cybersecurity advancements. But at the same time, Scotland must be live to and confront the threats posed by the militarisation of space, cyber warfare, and increased geopolitical competition. These challenges present both risks and opportunities for Scotland to lead through innovation, ensuring that its space sector remains competitive and secure in an increasingly contested global arena.

Expanding the Future of Space Cybersecurity: A Strategic Imperative for Scotland

As the report has illustrated, cybersecurity will be at the heart of the space sector by 2050. Scotland's ability to integrate AI-driven threat detection, quantum encryption, and space cyber education into its space ambitions will not only protect its infrastructure but could also establish it as a global leader in this emerging frontier. The development of secure, interplanetary financial systems, autonomous resource chains, and self-healing materials will offer Scotland the chance to position itself at the forefront of the space-cyber convergence.

The previous chapter on future-proofing space cybersecurity demonstrates that innovation and collaboration should be the cornerstones of Scotland's strategic approach. By pioneering cutting-edge technologies—from quantum-resistant cryptography to neural interfaces for controlling space systems—Scotland could be equipped to lead in the defence of global space assets. However, this also means that international collaboration and partnerships will be critical. Scotland must therefore continue to foster ties with organisations such as NASA, the European Space Agency, and leading space companies, ensuring that it remains a central player in both securing and shaping the future of space.

By focusing on education and workforce development, Scotland can close the existing skills gap in cybersecurity and prepare a generation of professionals who are ready to tackle the cyber threats of tomorrow. This forward-looking approach will be essential for creating a sustainable space economy, where cybersecurity is embedded into every layer of space operations—from satellite communications to spaceports and mining. By embracing its strengths and addressing its weaknesses, Scotland can harness the opportunities while mitigating threats to solidify its role as a leader in the space-cyber nexus.

Recommendations:

1. **Develop a Scotland-Specific Space Cybersecurity Strategy:** Create a comprehensive, cohesive strategy that incorporates cybersecurity across all stages of space development, ensuring robust protection against cyber threats unique to Scotland's space industry. This strategy should align with UK-wide security initiatives to bolster Scotland's position within the broader national space framework and international context (*Chapter One*).
2. **Embed Cybersecurity into All National Space Projects:** Ensure cybersecurity is a foundational element in all Scottish space ventures, from satellite launches to data transmission. Integrating cybersecurity from the start will align with broader UK strategies, ensuring space assets and operations are protected from emerging threats (*Chapter Two*).
3. **Enhance Cyber-Physical Systems (CPS) Security:** Invest in securing cyber-physical systems that underpin both space and ground operations, safeguarding critical infrastructure from cyber threats and ensuring the continuity of space operations (*Chapter Two*).
4. **Support SMEs with Targeted Funding and Advanced Cybersecurity Training:** Provide dedicated funding and specialised cybersecurity training to small and medium-sized enterprises (SMEs) in the space sector. This support will enable SMEs to adopt strong cybersecurity measures, helping them become resilient and competitive on a global scale (*Chapter Three*).
5. **Establish a Space Security Certification Programme:** Develop a certification programme to ensure Scottish space companies meet internationally recognised cybersecurity standards. This will foster trust, attract high-value partnerships, and open doors for defence and aerospace contracts (*Chapter Three*).
6. **Address the Skills Gap with Specialised Education and Apprenticeships:** Implement educational initiatives, such as tailored programmes, apprenticeships, and partnerships with universities, to develop the skilled workforce needed to support Scotland's space-cyber ambitions (*Chapter Four*).
7. **Promote Innovation in Space-Cybersecurity Technologies:** Encourage the development and adoption of advanced technologies like AI-driven threat detection, quantum encryption, and blockchain for secure space communications. Fostering innovation will help Scotland build a leadership position in space cybersecurity (*Chapter Five*).
8. **Align Investment and Insurance Incentives with Cybersecurity Standards:** Offer financial incentives and align investment strategies to promote strong cybersecurity practices across Scotland's space sector. By

connecting investment with cybersecurity, Scotland can attract both domestic and international investors while ensuring a resilient infrastructure (*Chapter Five*).

9. **Advance Future-Focused Space Cybersecurity Training and Ethics Initiatives:** Establish training programmes that emphasise future-oriented skills and incorporate ethical frameworks to guide space-cyber practices. This approach will ensure Scotland's workforce is prepared for the challenges of tomorrow, while aligning with ethical standards essential for sustainable space development (*Chapter Six*).
10. **Collaborate on International Space Cybersecurity Norms and Policies:** Actively participate in shaping global norms for space cybersecurity, positioning Scotland as a leader in establishing a secure, ethical international environment for space assets. This collaboration will enable Scotland to contribute meaningfully to the international space-cyber community (*full report*).

United Nations Sustainable Development Goals

Throughout this report, the United Nations Sustainable Development Goals (SDGs) have been identified in each chapter. The alignment of SDGs with space cybersecurity is vital for Scotland, highlighting the importance of secure space systems in promoting sustainable economic growth and environmental protection. As Scotland continues to develop its burgeoning space industry, prioritising cybersecurity in accordance with the SDGs enhances national security while supporting global sustainability efforts.

Conclusion

This report has explored how Scotland's potential at the intersection of space and cybersecurity can be fully realised by adopting a strategic approach that integrates cybersecurity into the core of its space ecosystem. By fostering collaboration across government, industry, and academia, Scotland can strengthen its strategic resilience and secure its place as a key player in the global space economy.

Scotland stands on the brink of a new frontier—where space exploration and cybersecurity converge to define the next era of technological and geopolitical influence. With its unique strengths, from a burgeoning space industry to an emerging cybersecurity ecosystem, Scotland has the opportunity not only to safeguard its future but also to shape the global narrative. As space becomes the new battleground for both economic and security dominance, those who invest in resilience and innovation will lead the way. By embedding cybersecurity at the core of its space ambitions and fostering international collaboration, Scotland can rise as a pioneer in a rapidly evolving world. The future is being written in the stars and coded in cyberspace—Scotland has both the vision and the tools to help lead humanity into this new era, where security, collaboration, and innovation will determine the leaders of tomorrow. The decisions made today will echo across generations, solidifying Scotland's place as a key player in the global space economy.

References

Aerospace. (2024). ‘Chinese hackers breach US satellites: Terra and Landsat-7 compromised’. *Aerospace Security Journal*, 15(3), pp. 20-28.

Aerospace (2024). Counterspace Timeline, 1959 - 2022. Available at: Aerospace Security.

Aerospace (2024). The US Defence Space Strategy and Cyber Threats. Aerospace Publishing.

Alcântara Space Center (2024)- SpaceNews. Available at: https://spacenews.com/alcacntara-space-center/.

Associated Press. (2022). US Keeps Eye on China's Space Activities for Potential Risks. Voice of America News. Available at: https://www.voanews.com/a/us-keeps-eye-on-china-s-space-activities-for-potential-risks/6869565.html.

AXA Investment Institute. (2023). Cybersecurity: A potentially vast investment opportunity as technology evolves. Available at: https://www.axa-im.co.uk/research-and-insights/investment-institute/future-trends/technology/cybersecurity-potentially-vast-investment-opportunity-technology-evolves.

Allan, K (2023) Orbital Data Centres, Data Centre Magazine, accessed online here: https://datacentremagazine.com/articles/orbital-data-centres-a-revolutionary-concept

Atlantic Council, (2024). *Cybersecurity and Geopolitical Risks: Taiwan's Vulnerability in the Global Supply Chain*. [online] Available at: https://www.atlanticcouncil.org

Attatfa, A., Renaud, K., and De Paoli, S., (2020). Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science*, 176, pp.60-69. Available at: https://doi.org/10.1016/j.procs.2020.08.007

Atler, E (2024) Cyber Risk: Uncorked Cyber & AI Risk – Now & the (near) Future Presentation at Space: Securing our Entrepreneurial Future conference, University of Strathclyde

BAE Systems (2024). The strategic importance of dual-use capabilities in space cybersecurity. *Journal of Space Policy*, 13(2), pp.146-160.

Babikian, D. & Nesheiwat, J. (2024). NATO needs a strategy to address Russia’s Arctic expansion. Atlantic Council. Available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-a-strategy-to-address-russias-arctic-expansion/.

Bansal, G. & Axelton, Z. (2024). The Role of Leadership Characteristics in IT Security Compliance: A Gender-Based Analysis. *Information Technology & People*.

Bates, P. (2024). ESA Contract Allocations in Scotland: Correspondence to the Scottish Affairs Committee. UK Space Agency.

BBC. (2011). Suspected US Satellite Hacking Attacks: Reaction. Available at: https://www.bbc.co.uk/news/technology-15749139.

BBC. (2018). NATO Military Exercise GPS Jamming. *BBC News*.

Bremmer, I. (2021). "The Technopolar Moment: How Digital Powers Will Reshape the Global Order." *Foreign Affairs*, foreignaffairs.com/articles/world/ian-bremmer-big-tech-global-order

Broadbent, D. (2024). Comments on the U.S. Army's Managed Satellite Communication Services Pilot Project. Potomac Officers Club's GovCon International Summit.

Brown, A. (2023). 'Investors and Cybersecurity', *Oklahoma Law Review*, 73, p. 420.

Brown, D. & Pytlak, A. (2020). Why Gender Matters in International Cyber Security. Retrieved from the uploaded document.

Brown, D. & Pytlak, E. (2021). Integrating Gender-Sensitive Approaches in Space Cybersecurity. *Journal of Cybersecurity*, 29(3), pp.27-35.

Business Gateway. (2018). Funding to boost Cyber security. Available at: https://www.bgateway.com/news/half-a-million-pounds-of-funding-to-help-businesses-and-charities-with-cyber-security.

Byres, M. (2024). Outer Space and the Arctic Connections, Opportunities, Challenges. CIGI. Available at: https://www.cigionline.org/static/documents/no.303.pdf.

CDL Space. (2024). About CDL Space Programme. Creative Destruction Lab. Available at: https://creativedestructionlab.com.

CEOWORLD Magazine (2024) *Revealed: Number of operational satellites in orbit, 2024*, July 2024. Available at: https://ceoworld.biz

Chavagnac, V., et al. (2024). The diplomatic processes of space activities. *Journal of Space Policy*, 56, pp. 112-130.

Chen, S. (2022a). Chinese Scientists Build System to Identify Satellite Security Flaws. *South China Morning Post*. Available at: https://www.scmp.com/news/china/science/article/3173638/chinese-scientists-build-system-identify-satellite-security.

Chen, S. (2022b). Chinese Physicists Simulate Nuclear Blast Against Satellites. *South China Morning Post*. Available at: https://www.scmp.com/news/china/science/article/3173639/chinese-physicists-simulate-nuclear-blast-against-satellites.

Chavagnac, A., et al.(2024). Cyber Vulnerabilities in Space Systems: Lessons from the Starlink Breach. *Journal of Space Technology*, 12(2), pp. 56-70.

Clarke, A. C. (1968). *2001: A Space Odyssey*. New American Library.

CISA. (2019). Phishing Attack on NASA Compromises Employee Credentials. Cybersecurity and Infrastructure Security Agency.

CNN. (2022). "Elon Musk says Starlink will ask for Pentagon funding after Ukraine request." *CNN*, October 14, 2022. Available at:

https://edition.cnn.com/2022/10/14/tech/starlink-ukraine-pentagon-funding-request/index.html

Cooney, C. (2024). Russia vetoes UN vote on stopping arms race in outer space. *BBC*. Available at: https://www.bbc.com.

Cummings, J. (2019). Emerging trends in space technology and investment. *International Journal of Space Economy*, 6(1), pp. 34-45.

CSIS (2024) Significant Events https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Dawson, L (2018) War in Space The Science and Technology Behind Our Next Theater of Conflict, Springer, Accessed online here 978-3-319-93052-7.pdf

Davis, R. (2023). Understanding the investment challenges in high-risk technology sectors. *Business Innovation Journal*, 29(4), pp. 22-28.

Delgado López, L. & Valdivia Cerda, V. (2024). Space security in the Americas can no longer go overlooked. *Space News*, 5 January.

Deloitte. (2023). Cybersecurity in Space Operations: The Role of MFA and AI. Available at: https://www.deloitte.com.

Deloitte. (2024). POV Reimagined: Women in Cybersecurity. Deloitte Global and The Female Quotient.

Demarest, C., 2023. *China Developing Own Version of JADC2 to Counter US*. C4ISRNET. [online] Available at: https://www.c4isrnet.com/global/asia-pacific/2023/04/04/china-developing-own-version-of-jadc2-to-counter-us/ [Accessed 16 October 2024].

Department for Digital, Culture, Media and Sport. (2024). Cyber Security Skills in the UK Labour Market 2024. Available at: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024.

Department of Space Defense (DSD). (2020). Space Policy Directive-5 (SPD-5): Cybersecurity Principles for Space Systems. Retrieved from the Department of Space Defense archives.

Drummond, M (2024) Warfare is changing: Is space the new military frontier?, Sky News, Accessed online here: Warfare is changing: Is space the new military frontier? | World News | Sky News

DIST. (2024). UK Cyber Security Breaches Survey. Department for Science, Innovation, and Technology. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024.

Erwin, S. (2024). Cybersecurity a top priority for military satellites as threats loom. *Space News*. Available at: https://spacenews.com/cybersecurity-a-top-priority-for-military-satellites-as-threats-loom/.

European Commission. (2019). Galileo incident of July 2019: Independent Inquiry Board provides final recommendations. Available at: https://single-market-economy.ec.europa.eu/news/galileo-incident-july-2019-independent-inquiry-board-provides-final-recommendations-2019-11-19_en.

European Commission. (2024). Digital Europe Programme. Available at: https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

European GNSS Agency. (2019). Galileo satellite system experiences technical issue.

European Space Agency (ESA). (2024). Cyber Security and Space Based Services. Available at: https://business.esa.int/funding/invitation-to-tender/cyber-security-and-space-based-services.

European Space Agency (ESA)., 2023. Cyberattacks on Space Systems: Lessons from the Russia-Ukraine Conflict. *European Space Agency*. Available at: https://www.esa.int

European Space Agency (2023). ESA's Space Shield Initiative. European Space Agency. Available at: ESA.

European Space Security Report. (2023). Security Standards in European Space Missions. *European Space Agency*.

Falco, G., Korth, L., Custer, P., Schofield, R.N. & Pocock, C. (2023). How to Scrub a Launch: Spaceport Cybersecurity.

Farrell, H. (2018). "Mark Zuckerberg runs a nation-state, and he's the king." *Vox*, April 10, 2018. Available at: https://www.vox.com/the-big-idea/2018/4/10/17220190/facebook-mark-zuckerberg-government-king

Fidler, D. P. (2018). Cybersecurity and the New Era of Space Activities. *Council on Foreign Relations*. Available at: https://www.cfr.org/report/cybersecurity-and-new-era-space-activities.

Financial Times. (2023). The economic impact of cybersecurity in the UK space sector. Available at: https://www.ft.com.

Ford, C.,(2022). Conceptualising Cyberspace Security Diplomacy. *The Cyber Defense Review*, 7(2), pp. 35-54

Fortune Business Insights (2023). Cyber Insurance Market Size, Share & Industry Analysis. Available at: Fortune Business Insights.

Fox News (2024). Companies Prepare Next-Generation Space Stations in Orbit. Available at: Fox News.

Foust, J. & Berger, B. (2022). SpaceX shifts resources to cybersecurity to address Starlink jamming. *SpaceNews*. Available at: SpaceNews.

Foust, J., (2024). *Dominican Republic signs Artemis Accords*. Space News,

Fox, C. H., & Probasco, E. S. (2022). "Big Tech Goes to War: To Help Ukraine, Washington and Silicon Valley Must Work Together." *Foreign Affairs*, October 19, 2022. Available at: https://www.foreignaffairs.com/ukraine/big-tech-goes-war.

Future Market Insights (2024). Space Insurance Market Size, Trends and Forecast. Available at: Future Market Insights.

Gallagher (2024). Space Insurance Market Navigates Uncertain Terrain in 2024 Amid Capacity Shifts. Available at: reinsurancene.ws.

Garrett, L. (2023). Investment trends in space and cybersecurity integration. *Space Investment Review*, 12(3), pp. 14-26.

Gartner. (2022). Spending on cloud-application SaaS expected to grow to $232.3 billion by 2024. Available at: https://www.gartner.com/en/newsroom/press-releases/2022.

Glenn, J.C. and Gordon, T.J. (1999), "The world in 2050: a normative scenario", *Foresight*, Vol. 1No.5,pp.453465. https://doi.org/10.1108/14636689910802340

Global Entrepreneurship Monitor (2024). GEM 2023/2024 Global Report: 25 Years and Growing. GEM Global Entrepreneurship Monitor.

Grillot, S. & Méndez, F., 2024. The Evolving Landscape of Space and Cyber Diplomacy. *Global Policy Review*, 15(1), pp. 78-92.

Goldman Sachs, (2022). Global Economic Shifts and the Future of Space Governance. *Goldman Sachs Report*.

Gompert, D. C. & Libicki, M. (2023) The Future of Warfare in the Space and Cyber Age. *International Security Journal*.

Government Accountability Office (GAO). (2024). Cybersecurity and Space Operations: Addressing Vulnerabilities in NASA's Design and Development Processes. Washington, DC: GAO.

Government (2018) Space Industry Act [2018]

Government. UK (2024) Invest 2035 the UKs Modern Industrial Strategy Accessed online: https://www.gov.uk/government/consultations/invest-2035-the-uks-modern-industrial-strategy/invest-2035-the-uks-modern-industrial-strategy

Government.UK (2024) UK Space Command Successfully Launches First Military Satellite Accessed online here:https://www.gov.uk/government/news/uk-space-command-successfully-launches-first-military-satellite

Government.UK (2019). COSMOS satellite network cyber-attack: Government response. Available at: UK Government.

Government.UK (2020). Chatham House Research Paper on Space and Cybersecurity. Available at: UK Government.

Government.UK (2021). Global Britain in a competitive age: the integrated review of security, defence, development and foreign policy. Available at: UK Government.

Government.UK (2022). Size and Health of the UK Space Industry 2022. *UK Space Agency*. Available at: UK Government.

Government.UK (2022). UK Defence Space Strategy. London: HMSO.

Government.UK (2023). National Space Strategy in Action. Available at: UK Government.

Government.UK (2024). Consultation on Orbital Liabilities, Insurance Charging, and Space Sustainability. Available at: UK Government.

Government.UK (2024). Cyber Security Breaches Survey 2024. *Department for Digital, Culture, Media & Sport*. Available at: Cyber security breaches survey 2024 - GOV.UK (www.gov.uk).

Government.UK (2024). Space Regulatory Review 2024. Available at: UK Government.

Government.UK (2023). Cybersecurity Incidents in UK Small Businesses. Available at: https://www.gov.uk/government/statistics/.

Government.UK (2024). SME Contributions to the UK Space Sector and Associated Risks. Available at: https://www.gov.uk/government/statistics/

Hannan, N. (2018). Supply-chain cyber resilience for the International Space Station (ISS). *RUSI Journal*, 163(2), pp. 58-66.

Hannan, N. (2022) 'Cyber Resilience and the ISS: Challenges in the Space Domain', *RUSI Journal*.

Harrison, T., Johnson, K., and Roberts, T., (2019). *Space Threat Assessment 2019*. Centre for Strategic and International Studies. [online] Available at: https://aerospace.csis.org/wp-content/uploads/2019/04/SpaceThreatAssessment2019-compressed.pdf

Harrison, T., Johnson, K., and Roberts, T., (2022). *Space Threat Assessment 2022*. Centre for Strategic and International Studies. [online] Available at: https://www.csis.org/analysis/space-threat-assessment-2022

Hart, B.L., 2007. Anti-Satellite Weapons, Threats, Laws and the Uncertain Future of Space. *McGill University Press*.

Hart, J., 2007. The Outer Space Treaty: A Reassessment. *Space Law Journal*, 2(4), pp. 45-67.

Holleran, M., Eze, N. & Mendez, J. (2024). The Intersection of Cybersecurity and Space Operations: A Holistic Approach. *Journal of Cyber Policy*, 5(1), pp.5-15.

House of Commons Library (2021). The UK Space Industry. Available at: UK Parliament.

House of Lords Library (2023) China: Security challenges to the UK. Available online: House of Lords Library.

Howells, M. (2022). The role of international law in addressing space security issues. *The International Lawyer*, 55(1), pp.82-104.

IBM Security (2019). DeepLocker: How AI is transforming malware. Available at: IBM.

Ishaq, A (2001) On the Global Digital Divide, International Monetary Fund, Accessed online here: https://www.imf.org/external/pubs/ft/fandd/2001/09/ishaq.htm

ISU. (2023). ISC2 Reveals Workforce Growth but Record-Breaking 4 Million Cybersecurity Professionals. Available at: https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals.

Inglesant, P; Jirotka, M; Hartswood, M (2018) Responsible Innovation in Quantum Technologies applied to Defence and National Security, NQIT, Accessed online https://nqit.ox.ac.uk/sites/www.nqit.ox.ac.uk/files/2018-11/Responsible%20Innovation%20in%20Quantum%20Technologies%20applied%20to%20Defence%20and%20National%20Security%20PDFNov18.pdf

Jafarnia-Jahromi, A. et al. (2012) 'GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques', *International Journal of Navigation and Observation*.

Johnson, T. (2023). 'Regulatory Frameworks in Space', *ScienceDirect*, 24(6), p. 53.

Jones, Andrew (2024) South Korea Space Agency Mars Landing, Space, Accessed online:https://www.space.com/south-korea-space-agency-mars-landing-2045

Jones, R. (2023). 'Due Diligence in Space Investments', *Oklahoma Law Review*, 73, p. 416.

Ji, S., Lu, X., Wang, S., & Luo, C. (2021). Security of China's quantum communication satellite and its implications for global cybersecurity. *Journal of Space Policy*, 35(1), pp. 52–60.

Jurgens, J. & Burkhardt. (2024). Space: The $1.8 Trillion Opportunity for Global Economic Growth Insight Report. Available at: https://www3.weforum.org/docs/WEF_Space_2024.pdf.

Kavallieratos, G. & Katsikas, S. (2023). An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space. *International Journal of Critical Infrastructure Protection*, 43. doi: 10.1016/j.ijcip.2023.100640.

Kang, C. (2023). AI Integration in Cybersecurity: Balancing Automation and Human Expertise. In: *Advances in Cybersecurity*. Springer, Cham, pp.123-138. Available at: springer.

Krelina, M (2023) The prospect of Quantum Technologies in Space for Defence and Security, Space Policy, V65, Accessed online here: https://www.sciencedirect.com/science/article/abs/pii/S0265964623000255

Kirshner, M. (2023). Model-Based Systems Engineering Cybersecurity for Space Systems. Available at: link_to_paper.

KPMG (2023). Expanding frontiers: The down-to-earth guide to investing in space. Available at: pwc.co.uk.

KPMG. (2024). Data Security: Safeguarding the High-Quality Development of Digital Economy. Available at: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2024/10/data-security-safeguarding-high-quality-development-of-the-digital-economy.pdf.

KPMG,(2024). *Cybersecurity Law of the People's Republic of China (2017) and Data Security Law (2021) Overview*. [online] Available at: https://home.kpmg/cn/en/home/insights/2021/06/overview-of-cybersecurity-and-data-security-law.html

Krelina, M (2023) The prospect of Quantum Technologies in Space for Defence and Security, Space Policy, V65, Accessed online here: https://www.sciencedirect.com/science/article/abs/pii/S0265964623000255

Kuhn, D.R. (2021). Space policy and the US military: Evolution and trends. *Air & Space Power Journal*, 35(6), pp.10-27.

Pace, S (2023) IAC-23-E3.Global Space Futures – 2050, Space Policy Institute, Elliott School of International Affairs, George Washington University, 1957 E St., NW Suite https://bpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/7/314/files/2023/10/Global-Space-Futures-2050-Pace-final.pdf

Lamine, W., Anderson, A., Jack, S.L. & Fayolle, A. (2021). Entrepreneurial space and the freedom for entrepreneurship: Institutional settings, policy, and action in the space industry. *Strategic Entrepreneurship Journal*. Available at: wiley.com.

Lavinder, K.,(2016). *Cyber Attacks: Is Latin America Prepared?* Air & Space Power Journal.

Lee, J., (2023). *China's Cyber Strategy and its Impact on Taiwan's Technology Sector*. Journal of International Security, 12(3), pp.45-67.

LaFrance, A. (2021). "The Largest Autocracy on Earth: Facebook is acting like a hostile foreign power." *The Atlantic*, September 27, 2021. Available at: https://www.theatlantic.com/magazine/archive/2021/11/facebook-authoritarianism/620168

Liebermann, O. & Peter, B., (2024). Transparency in Cyber Warfare: Challenges and Strategies. *Cybersecurity & International Relations*, 6(2), pp. 56-74.

Lin, P. (2024). To guard against cyberattacks in space, researchers ask 'what if'. *The Conversation*. Available at: theconversation.

Lemac-Vincere. (2024). US Military Project Aims to Prevent Hackers Targeting Satellites. Available at: https://theconversation.com/us-military-project-aims-to-prevent-hackers-targeting-satellites.

Liebermann, M., & Peter, H. (2024). *Cyber Governance in the Age of AI*. Oxford: Oxford University Press.

Luxembourg Space Agency. (2024). Luxembourg's Quantum Communications Infrastructure (LuxQCI). Available at: https://space-agency.public.lu/en.html.

Maulana, Y and Fajar, I (2023) Analysis of Cyber Diplomacy and its Challenges for Digital Era Community, IAIC Transactions on Sustainable Digital Innovation, Accessed online: https://aptikom-journal.id/itsdi/article/view/587

Martin, A.S. (2023). Outer Space, the Final Frontier of Cyberspace: Regulating Cybersecurity Issues in Two Interwoven Domains. Available at: link_to_paper.

Martin, G. (2016). NewSpace: The Emerging Commercial Space Industry.

Marsh (2023). Cyber Self-Assessment (CSA). Available at: Marsh.

McKinsey & Company (2023). Space: The $1.8 trillion opportunity for global economic growth. Available at: McKinsey.

McKinsey & Company (2023) Blockchain in Space and Cybersecurity: Trends for 2023. Available at: https://www.mckinsey.com.

Meyer, C., (2021). The Need for Specialised Diplomats in Cyber and Space. *International Journal of Diplomatic Studies*, 10(1), pp. 11-28.

Meyer, P., (2016). Prospects for Progress on Space Security Diplomacy. *Room, The Space Journal*, 4(10), pp. 43-47.

Meyer, P,(2021). Diplomacy: The Missing Ingredient in Space Security. *In*: Steer, C., and Hersch, M. (Eds.), *War and Peace in Outer Space: Law, Policy, and Ethics*. New York: Oxford University Press.

Ministry of Digital Affairs (MODA), (2023). *Taiwan's Cybersecurity Initiatives and Defense Strategies*. [online] Available at: https://www.moda.gov.tw [Accessed 23 October 2024].Miller, S. (2023). 'The Role of Investors in Space Tourism', *Oklahoma Law Review*, 73, p. 440.

MITRE. (2019). Benefits of Neurodiverse Talent in Cybersecurity. Available at: https://www.mitre.org/neurodiversity.

Mukhtar, F. (2024) Personal Communication, Email Security and the Threat of Human Error. UK Space Agency

Muncaster, P. (2024). Cybersecurity Skills Report: Gender Diversity and Workforce Growth. *Infosecurity Magazine*.

Mukherjee, S., Islam, S. & Hu, H. (2021). Cyber resilience in the commercial space sector: Best practices for SMEs. *International Journal of Cyber Security*.

Nadi, B. & Brooks, R. (2023). Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise. *arXiv*.

NASA (2018). NASA Cyberattack. Available at: NASA.

NASA (2021). Joint cybersecurity protocols for satellite operations. Available at: NASA.

NASA (2023). International cooperation. Available at: NASA.

NanoAvionics (2024) *How many satellites are in space?*, May 2024. Available at: https://nanoavionics.com

National Cyber Security Centre (2023). Cyber Security in Space: Protecting the Final Frontier. Retrieved from NCSC Website.

National Cyber Security Centre (NCSC) (2022). Cyber Security for Small and Medium-Sized Enterprises. Available at: NCSC.

National Cyber Security Centre (NCSC). (2024). Cyber Essentials. Available at: https://www.ncsc.gov.uk/cyberessentials/overview.

National Cyber Security Centre (2024). Cyber Threats to Space Infrastructure. London: National Institute of Standards and Technology (NIST). (2013). NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: NIST.

National Institute of Standards and Technology (NIST). (2023). *Interagency Report (IR) 8270: Introduction to Cybersecurity for Commercial Satellite Operations.* Gaithersburg, MD: NIST.

Nye, J.S., (2004). Soft Power: The Means to Success in World Politics. New York: Public Affairs.

Nye, J.S., (2010). Cyber Power. *Harvard University, Belfer Center for Science and International Affairs*.

Office for Outer Space Affairs (2021). Space treaties and principles. Available at: UNOOSA.

Orhun Guldiken, M.R. Mallon, S. Fainshmidt, W.Q. Judge, C.E. Clark (2021). Women in top management teams and the gender diversity–performance link: An integration of two research views. *Strategic Management Journal*. Available at: 10.1002/smj.3049.

Outer Space Cyberattacks: Generating Novel Scenarios to Anticipate Surprise. Available at: arxiv.

Pan, J.-W., Chen, Y.-A., Yin, J., Zhang, Q., Ren, J.-G., & Liang, H. (2017). Satellite-based quantum key distribution in China. *Nature*, 549(7670), pp. 43–47.

Phillips, A., & Sharman, J. C. (2015). "The Expansion of Diversity and Competition Under Heteronomy, 1600–1650." *International Order in Diversity: War, Trade and Rule in the Indian Ocean*. Cambridge University Press. Available at: https://www.cambridge.org/core/books/international-order-in-diversity/expansion-of-diversity-and-competition-under-heteronomy-16001650/54433EAF62A0F417FD52C136CF97D1D3

Pahvlavu, P (2003) Cyber-Diplomacy: A New Strategy of Influence, Canadian Political Science, Accessed online here: https://universityofleeds.github.io/philtaylorpapers/pmt/exhibits/1822/pahlavi.pdf

Pobjie, E; Ortega, A, (2024) Outer Space and the Use of Force: Geopolitical and Cybersecurity Challenges. United Nations Institute for Disarmament Research.https://unidir.org/wp-content/uploads/2024/09/UNIDIR_Outer_Space_and_Use_of_Force.pdf

Polkowska, M., 2019. Space Situational Awareness for Providing Safety and Security in Outer Space: Implementation Challenges for Europe. *Space Policy Journal*, 51, pp. 1-10.

Polkowska, A., 2019. Navigating the Complexities of Cyber and Space Diplomacy. *Diplomacy and Security Studies*, 8(2), pp. 109-125.
Potter, E (2002) Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century, McGill-Queen's University Press.

PwC, (2017). The World in 2050: The Long View. *PricewaterhouseCoopers*, London.

Radanliev, P (2024) Cyber Diplomacy: Defining the opportunities for cybersecurity and risks from Artificial Intelligence, IOT, Blockchains, and Quantum Computing, Journal of Cyber Security Technology, 1-5, Full article: Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing

RAND Corporation. (2023). Why National Security Needs Neurodiversity. Available at: https://www.rand.org/.

Rainbow, J. (2024). Dominican Republic considering its own commercial spaceport. *Space News*, May 22.

Reis, E., and Menezes, J., (2019). The Impact of Gender Diversity on Team Performance in High-Stakes Environments. *Journal of Business Research*, 92, pp.117-125. Online

Roberts, R. (2023). *AI and Diplomatic Strategies in the Digital Age*. Wilton Park.

Roberts, R., 2024. Science Diplomacy in Space Cybersecurity: Enhancing Global Cooperation. *Space and Cybersecurity Review*, 4(1), pp. 15-30.

Rose, J. & Stone, B. (1989). Commercial Development of Space - A National Commitment.

Santiago, H (2023) No Fight. No Flight. Just Innovation! How the Most Pressing Need in Cybersecurity Today Could Propel the Development of Quantum Computing, , Accessed online here: https://www.worldscientific.com/doi/abs/10.1142/9789811271984_0010

Saperstein, J. D. (2020) 'Opening the Black Box of Outer Space: The Case of Jason-3', *Geopolitics*, 25(4), pp. 729-746.

Scottish Government (2023) Scottish Space Strategy 2023. Available at: https://www.gov.scot/publications/space-sector-ministerial-statement-27-april-2023/.

Schmidt, A., 2024. Quantum Encryption Technologies: Future Implications for Space Security. *Journal of Cyber and Space Law*, 5(3), pp. 99-114.

Schmidt, E., 2024. Quantum Computing and AI in Space: Opportunities and Threats. *Journal of Space Technology*, 10(1), pp. 22-38.

Schmidt, J. (2024). *AI, Cybersecurity, and Space Operations*. London: Cyber Press.

Schmidt, H. (2024). The Evolving Landscape of Space Cybersecurity: Challenges and Opportunities. *Hague Journal of Diplomacy*. Available at: brill.

Scottish Government. (2024). Scotland's ambitions in the global space economy. Available at: https://www.gov.scot.

Scottish Science Advisory Council (2024). Scotland's Space Sector: Exploring potential future opportunities. Available at: scottishscience.org.uk.

Seraphim Capital (2023) Annual Investment Report. Available at: https://seraphim.vc/

Sharfman, P. & Visner, S. (2021). Development of Cybersecurity Norms for Space Systems

Shimbun, A. (2024) 'Japan Aerospace Exploration Agency's 2023 cyberattack'. Available at: https://www.asahi.com/ajw/articles/15314492.

Shove, C. (2005). Emerging Space Commerce and State Economic Development Strategies.

Siciliano, G., et al. (2024). Insurance Market Provide New Effective Solutions for Newspace Technologies and Services. In: *Space Insurance Market*, Taylor & Francis. Available at: Taylor & Francis.

Singh, J.D., Kaswan, K.S., Kumar, S., Sood, K. & Grima, S. (2024). Cybersecurity and Insurance. In: *Cybersecurity and Insurance*, Taylor & Francis. Available at: Taylor & Francis.

Smith, J. (2020). Cybersecurity in Space: Emerging Threats and Solutions. *ScienceDirect*..

Smith, J. (2023). 'Cybersecurity as a Prerequisite for Investment', *Oklahoma Law Review*, 73, p. 413

Smith, J. (2024) 'WannaCry Ransomware Attack and Its Impact on Critical Infrastructure', *The Journal of Cybersecurity*.

Smith, R., 2020. The Rise of Private Actors in Space: Implications for Global Governance. *International Relations Quarterly*, 29(1), pp. 30-50.

Smith, J. (2024). Challenges and Strategies in Space Cybersecurity. *IEEE International Conference on Space Operations*. Available at: IEEE.

Smith, J. (2024). Understanding the Cybersecurity Threat Landscape for SMEs in the Space Sector. *Cyber Security Review*, 19(3), pp.233-245. Available at: tandfonline.

Smitherman, D. (1998). New Space Industries for the Next Millennium.

Space News (2007). Tamil Tigers hack into IntelSat communications feed. *Space News*.

Space News (2023). Space Force Coming to Grips with Cybersecurity Threats. Available at: SpaceNews.

Space News (2023). AI at a Crossroads: Cybersecurity in Space and National Security in the Digital Age

SolarWinds (2021). SolarWinds cyberattack: Detailed analysis. Available at: SolarWinds.

Sorensen, G., Jackson, R. & Sørensen, G. (2012). Introduction to International Relations: Theories and Approaches. Oxford: Oxford University Press.

Space Scotland (2023) Strategy for Space in Scotland. Available at: https://spacescotland.org/wp-content/uploads/2023/11/a_strategy_for_space_in_scotland.pdf.

Space Generation Advisory Council (2022). Insurance in the Space Sector. Available at: Space Generation Advisory Council.

Statista (2022) Global cybersecurity market size from 2022 to 2030. Available at: https://www.statista.com/statistics/617136/global-cyber-security-market-size

State Council Information Office of the People's Republic of China, 2016. *China's Space Program: A 2016 Perspective*. [online] Available at: http://english.www.gov.cn/archive/white_paper/2016/12/28/content_281475527159496.htm

State Council Information Office of the People's Republic of China, 2021. *China's Space Program: A 2021 Perspective*. [online] Available at: http://www.cnsa.gov.cn/english/n6465652/n6465653/c6813088/content.html

Statista. (2022). Global cybersecurity market size from 2022 to 2030. Available at: https://www.statista.com/statistics/617136/global-cyber-security-market-size.

Taiwan Semiconductor Manufacturing Company (TSMC), 2023. *Semiconductor Production and Its Role in the Space Industry*. [online] Available at: https://www.tsmc.com

Taylor, B. (2023). 'Government Support for Cybersecurity', *Oklahoma Law Review*, 73, p. 425.

Tech Insurance Review. (2023). The Role of Insurance in Securing Space Assets. *Tech Insurance Review*, 3(2), pp. 40-47.

UK Cyber Security Council. (2023). The UK's Cyber Security Skills Gap. Available at: https://www.cybersecuritycouncil.org/.

UK Cyber Security Strategy. (2024). Building Resilience in Space and Cybersecurity. National Cyber Security Centre. Available at: https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf.

UK Parliament (2021). Cyber Security in Space: A New Phenomenon or an Old Adversary. Available at: UK Parliament.

UK Parliament (2022). "National Security Implications of the Sale of OneWeb: Evidence to the Committee." UK Parliament Report, p. 29. Available at: https://publications.parliament.uk/pa/cm5802/cmselect/cmpubacc/135/13503.htm

UK Parliament (2024). Scotland's Space Sector. Available at: UK Parliament.

UK Space Agency (2023). Size and Health of the UK Space Industry. Retrieved from UK Government Website.

United Nations (2013) Study Series No. 34, 2013. Transparency and Confidence-Building Measures in Outer Space Activities. *UN Office for Disarmament Affairs*, New York: United Nations.

United Nations (1967). Outer Space Treaty.

United Nations (1984). Moon Agreement.

United Nations (2020). Report of the Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security. A/75/264. Available at: undocs.org.

United Nations (2022). A/RES/77/123. Available at: undocs.org.

United Nations (2023) Widening Digital Gap between Developed, Developing States Threatening to Exclude World's Poorest from Next Industrial Revolution, Speakers Tell Second Committee, Accessed online here: https://press.un.org/en/2023/gaef3587.doc.htm

United Nations Office for Outer Space Affairs (UNOOSA) (2024). Introduction to the Outer Space Treaty. Available at: UNOOSA.

U.S. Congress. (1984). *Commercial Space Launch Act*. Washington, DC: U.S. Government Publishing Office.

U.S. Congress. (2015). *Commercial Space Launch Competitiveness Act*. Washington, DC: U.S. Government Publishing Office.

U.S. State Department, 2023. *The U.S. Strategic Framework for Space Diplomacy*. Washington D.C.: U.S. State Department.

Van der Meer, P., 2011. Science Diplomacy: Balancing Scientific Collaboration and National Interests. *Global Policy Review*, 9(3), pp.455-475

Van Der Wees, (2024) Presentation on Autonomous Flying Cars, Space Securing our Entrepreneurial Future Conference, University of Strathclyde.

Varadharajan, V. & Suri, N. (2022). Cybersecurity issues in the space sector: A supply chain perspective. *Cybersecurity and Space Journal*, pp.1-10.

Vecellio S, P., (2024). *China's Role in Space Cybersecurity Standards*. *International Journal of Cyber Governance*. [online] Available at: https://www.cybergovernancejournal.org/articles/chinas-role-in-space-cybersecurity-standards [Accessed 16 October 2024].

Verizon. (2023). Data Breach Investigations Report. Available at: https://www.verizon.com/business/resources/reports/dbi.

Wadhwa, V., & Salkever, A. (2022). "How Elon Musk's Starlink Got Battle-Tested in Ukraine." *Foreign Policy*, May 4, 2022. Available at: https://foreignpolicy.com/2022/05/04/starlink-ukraine-elon-musk-satellite-internet-broadband-drones

Wang, J., & Dubbins, A. (2024). *What Artificial Intelligence Means for Public Diplomacy*. CPD Publications.

Wang, X., Li, Y. & Chen, Z. (2024). Unified Frameworks for Space Cybersecurity. In: *Cybersecurity in the Age of Space Exploration*. Springer, Cham, pp.5-12. Available at: springer.

Weeden, B., (2019). *China's Anti-Satellite Capabilities*. Secure World Foundation. [online] Available at: https://swfound.org/media/206392/weeden_swf_report_anti-satellites_2019.pdf

Wess, M. (2021) Cyber exploitation in space operations. *Journal of Space Security*, 12(3), pp. 45-56. Available at: https://spacenews.com/space-security-americas-no-longer-overlooked/.

Werner, D. (2024). Who's in Charge of Preventing and Responding to Cyberattacks? *Space News*. Available at: https://spacenews.com/whos-in-charge-of-preventing-and-responding-to-cyberattacks/.

Wiederhold, B. K. (2024). Diverse Minds, Secure Networks: Embracing Neurodiversity in Cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, 27(9). doi:10.1089/cyber.2024.0413.

Wörner, J. (2023). Space diplomacy. *The Hague Journal of Diplomacy, 18*(4), 437-445.

Wood, N (2024) https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer

World Economic Forum & McKinsey & Company. (2024). Space: The $1.8 Trillion Opportunity for Global Economic Growth. Available at: https://www.weforum.org.

Wright, D. (2012). Future UK space policy - Indications from the UK Space Conference 2011. *Space Policy*. Available at: dx.doi.org.

Wright, D., Grego, L. & Gronlund, L. (2020). The Impact of Cybersecurity on Space Assets. *Cambridge University Press*. Available at: books.google.

Yankson, P. (2020). Space security: Understanding the cyber dimension. *Space Policy Journal*, pp.110-125.

Yazıcı, A. & Darici, S. (2019). The New Opportunities in Space Economy.

Zhang, B. & Smith, A. (2023). "Cybersecurity Strategies for Space Systems: An Overview," *IEEE Transactions on Aerospace and Electronic Systems*. Available at: IEEE.

ZDNet. (2018). **‘**Australian Defence Contractor Data Breach’ *ZDNet*.

Description of Laws, Regulations, and Policies

Commercial Space Launch Act (1984) and Commercial Space Launch Competitiveness Act (2015) – U.S. legislation that fosters private sector space activity by providing a regulatory framework for commercial space launches (U.S. Congress, 1984; U.S. Congress, 2015).

NIST SP 800-53 Security and Privacy Controls – A framework developed by the U.S. National Institute of Standards and Technology (NIST) for security controls, applied to space operations, with extended guidance in Interagency Report 8270 for commercial satellite operations (NIST, 2013).

Space Policy Directive-5 (SPD-5) – A 2020 U.S. directive outlining voluntary cybersecurity guidelines for space systems, highlighting the challenges of non-mandatory frameworks in ensuring space cybersecurity (DSD, 2020).

Commercial Augmentation Space Reserve (CASR) – A U.S. military program launched in 2024, aimed at integrating commercial space technologies into military operations.

Spacecraft Cybersecurity Act – Proposed U.S. legislation by Congressmen Maxwell Alejandro Frost and Don Beyer to enforce cybersecurity standards in NASA's space missions.

Government Accountability Office (GAO) Reports – Highlighted cybersecurity weaknesses in the U.S., specifically within NASA, pointing to vulnerabilities in the design phases of missions (Lemac-Vincere, 2024).

National Space Council (Canada, 2024) – A council established to oversee Canada's national space strategy, particularly concerning cybersecurity.

Critical Cyber Systems Protection Act (CCSPA) - Bill C-26 – A Canadian law mandating enhanced cybersecurity protocols for critical infrastructure, including space systems (Public Safety Canada, 2022).

Lunar Exploration Accelerator Program (LEAP) – Canada's investment initiative focusing on lunar exploration technologies, with significant cybersecurity considerations for international missions (Mortillaro, 2024).

China's Space Program: A 2021 Perspective – China's white paper on its space objectives, underscoring self-reliance, and the integration of cybersecurity in space infrastructure (State Council Information Office of the People's Republic of China, 2021).

Cybersecurity Law of the People's Republic of China (2017) and Data Security Law (2021) – Chinese laws aimed at protecting critical information infrastructure, including space assets (KPMG, 2024).

Mozi Quantum Communication Satellite (2016) – A Chinese satellite that facilitates quantum key distribution for secure communications in space (Pan et al., 2017).

European Space Policy (2007) – The EU's policy framework guiding collaborative space activities with integrated cybersecurity principles, with a pending EU Space Law by 2025 to include cybersecurity mandates.

General Data Protection Regulation (GDPR, 2018) and Network and Information Security (NIS) Directive (2016) – EU regulations for data protection and cybersecurity standards, applied to space activities (European Union, 2007; European Union, 2016).

France's Law on Space Operations (2008, amended 2023) – French regulation that includes provisions mandating cybersecurity measures in space operations (French Government, 2023).

Luxembourg's 2020-2030 Standardization Strategy – A framework embedding cybersecurity in Luxembourg's space infrastructure development to ensure resilience.

Federal Law on Space Activity (Russia, 1993) – Russian law on space activities, which lacks explicit cybersecurity measures (Lukowski, 2023).

Federal Law No. 187-ФЗ on the Security of Critical Information Infrastructure (2017) – Russian law mandating cybersecurity for critical infrastructure, including space, with a focus on domestic technology use.

Sovereign Internet Law (Federal Law No. 90-ФЗ, 2019) – Russian law establishing an independent internet within Russia, influencing its space-based communication systems.

Federal Law No. 152-ФЗ on Personal Data (2014) – Russian data localisation law, requiring storage of personal data within Russia, impacting space missions and data sharing.

Yarovaya Law (Federal Law No. 374-ФЗ) – Russian counterterrorism law enforcing data storage and decryptability, potentially extending to space-based systems.

IRIS² Satellite Program – An EU initiative for secure space communications as part of Europe's strategy for technological sovereignty in space.

IEEE SA P3349—Space System Cybersecurity Working Group – An international forum for standardising cybersecurity measures for space missions, with active participation from China.

Further Notes:Policies and Strategic Plans:

European Union Space Law – A comprehensive law being finalised to incorporate cybersecurity mandates by 2025.

France’s Law on Space Operations (2008, amended 2023) – Incorporates cybersecurity measures for France’s space activities.

Luxembourg’s Space Standardization Strategy (2020-2030) – Embeds cybersecurity into space infrastructure.

Appendix: Table: Global Actors in Space Cybersecurity

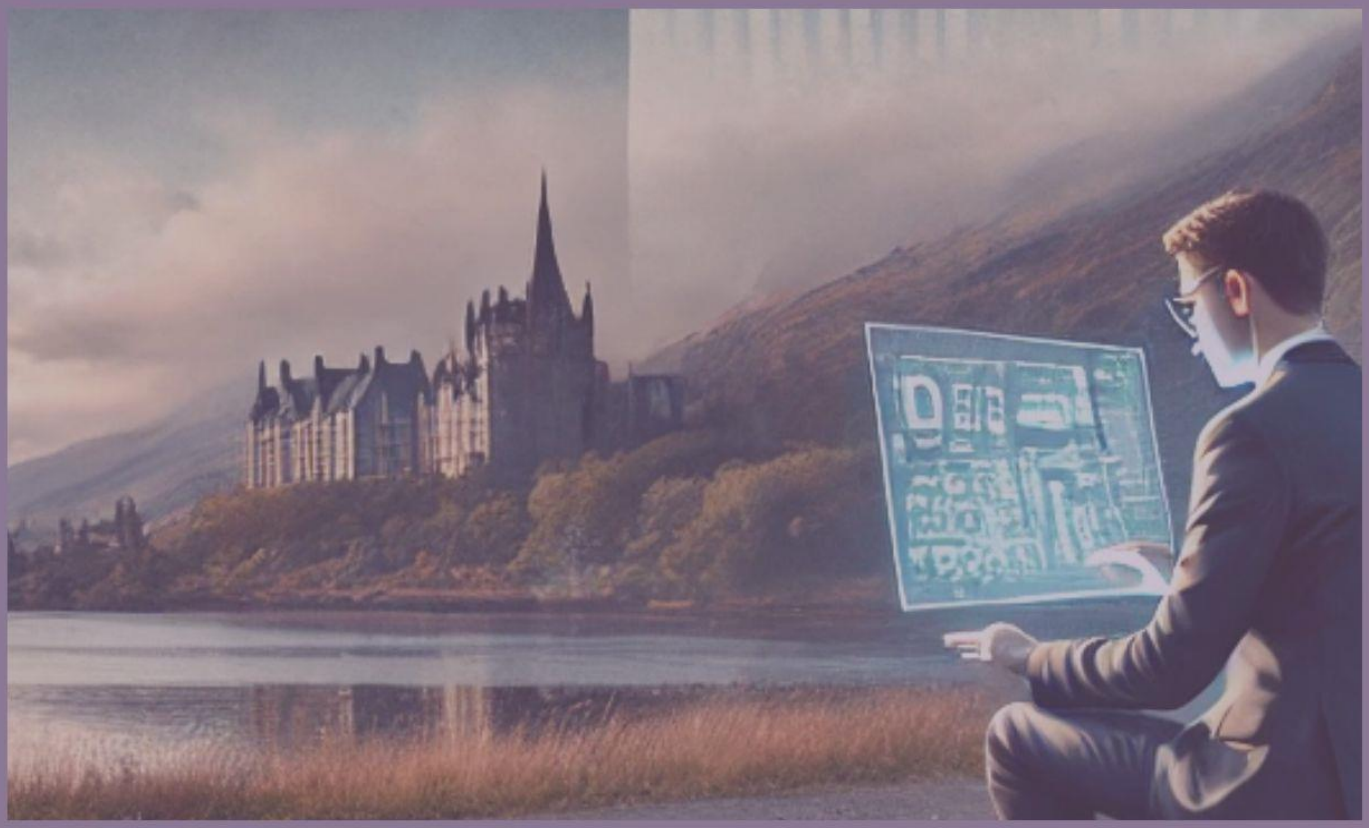
The table provides a selection of countries and regions that are actively involved in space cybersecurity. While it does not cover every nation, it highlights a variety of approaches taken by major space actors across the globe. These countries demonstrate differing levels of maturity, focus areas, and challenges, reflecting the unique strategic priorities of each region. The selection includes established space powers like the United States and emerging actors such as Luxembourg, showcasing a broad spectrum of policies from voluntary standards to fully integrated defence systems. This sample allows for an understanding of how different nations are navigating the growing challenges of space cybersecurity.

Country/Region	Space Cybersecurity Focus	Key Contributions	Challenges	References
Argentina	Developing satellite technologies; focus on commercial and environmental space applications.	Investment in Earth observation satellites; growing role in Latin American space sector.	Limited regional collaboration on cybersecurity; faces resource constraints in securing space assets.	Latin American Space Report, 2023
Australia	Emerging space power with increasing cybersecurity focus; emphasis on collaboration with international partners.	Space cybersecurity is integrated into national defence strategies; strong collaboration with the United States and Five Eyes alliance.	Still developing its national space program; cybersecurity challenges for growing commercial space sector.	Australian Space Agency, 2023
Brazil	Emerging space power with slow progress in cybersecurity frameworks.	Developing national satellite cybersecurity framework; leading space power in Latin America.	Slow regulatory progress; cybercriminal activity on the rise in the region.	Brazil Cyber Strategy, 2022
Canada	Focus on securing communication satellites and Arctic surveillance systems.	Long history of satellite innovation and space exploration; active in securing space infrastructure.	Geopolitical tensions, particularly with Russia, create vulnerabilities in Arctic surveillance systems.	Canadian Space Agency, 2023
China	Focus on state assets and offensive cyber capabilities; cyber espionage activities.	Developing counterspace technologies and tools to disable enemy satellites.	Offensive strategies increase global tensions; potential for space militarization.	China Space Policy, 2022
Estonia	Leading development of space cyber range for testing and training in space-related cyber threats.	Created the world's first space cyber range in cooperation with ESA; strong cybersecurity expertise applied to space.	Small space sector but growing influence; potential reliance on international partnerships for scaling cybersecurity efforts.	Sten Hankewitz, 2023

France	Law on Space Operations (2008, amended 2023) mandates cybersecurity plans for satellite operators.	Strong regulatory framework for space operations, ensuring cybersecurity compliance.	Balancing public-private sector cybersecurity interests in the space sector.	CNES, 2023
Germany	Space Strategy (2023) acknowledges need for cybersecurity, collaboration with ESA on space cybersecurity.	Leading role in Europe for space cybersecurity, collaborating closely with the European Space Agency (ESA).	Fragmentation of responsibilities between national and European frameworks.	German Space Strategy, 2023 BSI Technical Guidelines for Cybersecurity.
India	Developing cybersecurity for space infrastructure, especially private sector satellite systems.	Developing a comprehensive cybersecurity framework for its growing space sector.	Rapid space sector growth presents challenges in regulating private space companies.	Indian IT Act
Iran	Cybersecurity measures largely unknown due to national security concerns.	National security considerations make it difficult to assess specific measures.	Limited transparency, making international collaboration difficult.	Iran Space Agency
Italy	Investing over €3 billion into cybersecurity for space systems, focusing on satellite and national space infrastructure protection.	Large-scale investment in cybersecurity for satellite systems.	Complex legal and regulatory landscape within the European Union.	Italian Space Cybersecurity Strategy, 2023
Liechtenstein	Recently passed space laws incorporating cybersecurity to protect emerging space sector.	Forward-thinking legislation incorporating cybersecurity from the outset; small but emerging player in the global space sector.	Small size limits resources; still in early stages of developing space infrastructure.	Liechtenstein Space Law, 2023
Luxembourg	Focus on integrating cybersecurity into aerospace technical standardization and space sector resilience.	Luxembourg Standardization Strategy 2020-2030 emphasizes cybersecurity in space; international collaborations with ESA.	Smaller space industry; requires stronger coordination with international space security efforts.	Luxembourg Standardization Strategy, 2023
Latin American and Caribbean Space Agency (ALCE)	ALCE is in early stages of development with limited specific focus on cybersecurity for space systems.	Collaboration on satellite deployment in Latin America; future cybersecurity strategies expected to evolve.	Limited experience and resources in cybersecurity for space systems.	ALCE Space Activities, 2023

New Zealand	Small but growing space sector; focus on responsible space use and cybersecurity.	Rocket Lab is a major private player; member of Five Eyes intelligence alliance, leading to strong collaboration on cybersecurity.	Small space industry; still developing independent cybersecurity frameworks.	New Zealand Space Agency, 2023
Russia	Focus on state-controlled space assets; offensive cyber capabilities aimed at disabling enemy satellites.	Cyberattack on Viasat during Ukraine conflict demonstrated the potential of space-related cyber warfare.	Lack of transparency; high potential for cyber conflict escalation.	Russian Space Policy, 2022
Saudi Arabia	Developing a multi-orbit satellite capacity for communications; focus on cybersecurity for space systems likely emerging.	Neo Space Group is playing a key role in Saudi Arabia's space ambitions, with a focus on resilience.	Still in the early stages of space cybersecurity efforts.	Neo Space Group, 2023 https://spacenews.com/saudi-arabia-plots-space-industry-transformation/
Scotland (UK)	Growing role in satellite manufacturing; relies on broader UK cyber efforts (no dedicated space cybersecurity yet).	Glasgow is a global leader in small satellite manufacturing; collaboration with UK Space Agency and NCSC for general cyber resilience.	No specific space cybersecurity framework; vulnerability in private sector satellite operations.	Scottish Government, 2023
South Africa (Africa)	Africa's largest space program; focus on Earth observation, communications, and cybersecurity.	South African National Space Agency (SANSA) prioritizes cybersecurity for Earth observation and satellite communication systems.	Regional challenges in space collaboration and cybersecurity frameworks; limited resources for broader space development.	South African National Space Agency, 2023
South Korea	Expanding space sector; strong focus on cybersecurity considering North Korean cyber threats.	Collaboration with the U.S. and Europe on space cybersecurity; growing satellite industry.	Constant threat from North Korea; needs further development in space-specific cybersecurity.	South Korean Cybersecurity Report, 2023
Spain	Establishing national security and defence capabilities for space, including space surveillance and collaboration with NATO.	New Spanish Space Command formed, coordinating with French, German, and U.S. counterparts for space defence.	Early stage of operational development; limited resources compared to other space powers.	Spanish Space Command, 2023
Taiwan	Strategic importance in global semiconductor supply chain; vulnerable to	Taiwan Semiconductor Manufacturing Company (TSMC) produces critical	Geopolitical tensions with China threaten the global supply chain	Taiwan Cybersecurity Law, 2023

	cyberattacks from China.	chips for satellite technology.	and space industry.	
United Kingdom	General focus on space and cybersecurity through collaboration between the UK Space Agency and the NCSC.	Collaboration between UK Space Agency and National Cyber Security Centre (NCSC); growing private sector space investment.	Lack of space-specific cybersecurity frameworks; heavy reliance on voluntary standards for private sector. Except for launch under the Space Industry Act [2018]	UK Space Agency, 2023 Space Industry Act [2018] Space Regulations Proposed Cyber Security Bill [2024]
United States	Voluntary cybersecurity standards (Space Policy Directive-5) for private sector; advanced state capabilities.	Major space power with advanced cyber defense; large private sector innovation.	Lack of enforceable regulations for private space companies leaves gaps in security.	White House SPD-5, 2020



Dr Sharon Lemac-Vincere
PhD (Socio-Legal), MSc (Crim), MSc (HRM), LLB (Hons), B.A (Coms)
Chartered FCIPD, FILM, FCMI, SFHEA, ESS

Hunter Centre of Entrepreneurship: Stenhouse Wing (Level 4)
Strathclyde University Business School,199 Cathedral Street,
Glasgow, G4 0QU
Research Areas: Space Entrepreneurship, Cyber Security in Emerging Markets, Emerging Technology

Visiting Academic: International Space University, Strasbourg
Podcast: Space No Rocket Required
Scottish Centre for Crime and Justice Research:
https://www.sccjr.ac.uk/person/sharon-lemac-vincere/

University of Strathclyde Glasgow