# NewSpace, New Threats – Exploring the Influence of New Entrants to the Space Industry on Cybersecurity


**Sara Cannizzaro**
**Department of Sociological Studies**
**University of Sheffield, UK**
**s.cannizzaro@sheffield.ac.uk**

**Matthew Bradbury**
**School of Computing and Communications**
**Lancaster University, UK**
**m.s.bradbury@lancaster.ac.uk**

**Sam Maesschalck**
**Nexova Group**
**Place de l'ESA 1**
**Redu, Belgium**
**s.maesschalck@nexovagroup.eu**

**Gregory Epiphaniou**
**Cyber Security Centre, WMG,**
**University of Warwick, UK**
**Gregory.Epiphaniou@warwick.ac.uk**

**Carsten Maple**
**Cyber Security Centre, WMG,**
**University of Warwick, UK**
**cm@warwick.ac.uk**



***Abstract*—The space sector is changing from state-supported space exploration to commercial space exploration, giving rise to NewSpace. The role of small to medium sized enterprises (SMEs) in this rapid growth is increasing, but experience in other sectors shows SMEs may not be sufficiently focused on cyber security issues. In this exploratory study, we investigated the Influence of New Entrants to the Space Industry on Cybersecurity, according to industry stakeholders. To explore this question, we carried out 8 semi structured interviews with NewSpace organisations directly involved in the design, development or review of space system devices and services, including SMEs, large businesses, governmental and not for profit, non-governmental organisations (NGOs). Our findings highlight crucial areas in cybersecurity which may be influenced by the advent of new entrants to the space industry, such as technology infrastructure, philosophical approaches to cybersecurity maturity, vulnerability disclosure culture, and regulatory aspects. These are the areas where intervention to promote healthy cybersecurity practices can be directed and be achieved through collaborations amongst the developers, end users and regulators.**


## TABLE OF CONTENTS



## 1. INTRODUCTION

The space industry is currently undergoing substantial change, with new opportunities for development as a wide variety of organisations are exploring commercial opportunities of services facilitated by in-orbit deployments of devices. As Gonzalez put it, a new "techno-economic paradigm" is emerging in the space economy [2].

Historically, only government, defence and well-resourced telecoms could afford to put satellites in space due to high launch costs from high mass satellites. However, launching satellites has become much more accessible. Technological advances are facilitating cheaper cost space activities through improved electronics, advanced materials, batteries and computational and design tools [3], large folding antennas [4] and the ability to deploy large satellite swarms. Satellite components have been standardised and miniaturised to be small enough to be held in one hand [5], and commercial satellite builders have an increased number of launch options.

This is facilitated by the emergence of mobile ground stations, which has improved access, increased launch facilities offer and thus decreased the cost of launches. Improvements in the capabilities of satellites have prompted a range of satellite microbusinesses, increasing the accessibility of space to organisations like educational institutions, small businesses and individual researchers who previously did not have access [5]. Furthermore, changes in international space policy have incentivised and widened access to commercial space activities, such as via the allocation of new radio spectra for commercial satellite communications and the allowance of higher imagery

resolution for commercial remote sensing [7].
These changes have facilitated the entrance of small to medium sized enterprises (SMEs) in space, with a significant effect on the sector. Particularly, the structure of these businesses and the flattening of hierarchical structures has shown to influence innovation and new product development in the space sector and thus supported 'open innovation' [6]. This further affects other actors in space, including larger businesses, particularly from a security viewpoint.

These smaller companies do not always have significant funding and have a long research and development cycle [8], potentially leading to a focus on functionality and leaving cybersecurity as an afterthought during development. Particularly, SMEs have lower capital and profit margins, and therefore face higher risks than larger organisations and intergovernmental organisations that used to be the main players within the space sector. SMEs have also been shown to underestimate cybersecurity threats leading to an increase in vulnerabilities and risks [9]; this can impact other actors, especially if they rely on SME-developed commercial off-the-shelf (COTS) components for operations.

Due to these changes, space exploration increasingly sees new entrants to the sector and its associated supply chain. The emerging space sector was initially dubbed as *NewSpace* [10] and more recently NextSpace [11]. There have also been calls for a renaming of the space industry highlighting the ever-increasing commercialisation of the space dubbing this the 'big space' [12].

As new entities begin to understand and exploit the business opportunities presented by the NewSpace market, there emerges various concerns about the consequences of such a development. The change that we focus on in this work, is the expected influence of new entrants to the space industry on cybersecurity. To this end, we investigated 1) what is known by industry stakeholders about the threats of NewSpace, 2) how these threats are perceived by entrants to the industry themselves, and 3) what mitigation strategies are being put in place in the sector.

Our primary contributions are as follows:

1. **Analysis of Cybersecurity Challenges in NewSpace**: We explore the complex cybersecurity risks that have emerged with the entry of SMEs into the commercial space sector. Our analysis provides a nuanced understanding of the changing security landscape in the NewSpace industry.
2. **Stakeholder Interviews and Perspectives**: Utilising semi-structured interviews, we gather insights from a broad spectrum of stakeholders, including SMEs, large corporations, government agencies, and not for profit, Non-Governmental Organisations (NGOs), thus presenting a multifaceted view of the cybersecurity challenges in the space sector.
3. **Identification of Key Areas of Expected Influence**: Our research identifies crucial areas which may be influenced by the advent of new entities in the space industry, such as technology infrastructure, cybersecurity maturity, vulnerability disclosure culture, and regulatory aspects. Highlighting these areas, we pinpoint where targeted efforts and resources are most needed to address cybersecurity risks.
4. **Focus on SME-specific Cybersecurity Challenges**: We specifically address the distinct cybersecurity challenges faced by SMEs in the NewSpace sector. Our emphasis on these challenges sheds light on the specific needs and strategies that SMEs can employ to bolster their cybersecurity postures.

Through these contributions, our paper aims to advance the understanding of cybersecurity in the NewSpace era, inform strategies for responsible development of space exploration systems by effectively managing cybersecurity risks in this rapidly evolving domain. In particular, we aim to highlight the perspective of companies new to the space sector, which often have limited understanding of the risks involved and how to mitigate them. By understanding this perspective, cybersecurity experts can enhance the level of support they provide to these companies.

## 2. Literature Review

*Cybersecurity in the private sector*

NewSpace is a decentralised set of space companies that emerged after the cancellation of the NASA Space Shuttle program [13]. As indicated by Anderson [14]:

> "When we say NewSpace, we are not talking merely of the general commercialisation of space, as there has been a commercial element in space activities for decades, but rather the cultural and philosophical shift toward greater private entity participation."

The growth of the sector is concentrated amongst very large enterprises (56% of overall growth) and larger SMEs (28%), with the latter growing particularly fast (31% p.a., compared to very large enterprises at 2% p.a.) [15]. The need for SMEs within the sector has been highlighted as a requirement for the development of the European space market and NewSpace [16]. The new entrants' success in the NewSpace market relies on aggressive strategies such as "an ability to decide more quickly, on increased risk-taking, on a tolerance

for failure, on acceptance of lower levels of reliability, but also, for most of them, on innovations in usage of systems and not in products (with the possible exception of micro- and nano-satellites)" [17]. Gonzales [2] dubs these new entrants as 'astropreneurs' and finds they consist of three types: in-space, on earth, and space spin-off entrepreneurs.

Considering cybersecurity in the general private sector (not necessarily in space exploration) reveals an area of substantial challenge, as firms have been found to invest in cybersecurity activities at a level below what would be optimal – the private sector has been dubbed a "reluctant partner in cybersecurity" [18]. For example, over four in ten businesses (43%) in the UK experienced a cybersecurity breach or attack in 2018 [19]. SMEs are potentially the ones most at risk of cybersecurity threats [20] because SMEs often have a low security budget [21], neglect cybercrime prevention [22], do not possess adequate knowledge in cybersecurity [23], and at a time of increased remote work following the Covid-19 pandemic, face an increase in cyber-attacks [21].

These issues can seriously impact an SME's competitiveness and even compromise the value chain they are connected to [21]. They can become a significant point of vulnerability in the supply chain networks in which they participate [24]. Each of these issues could apply to SMEs in the space sector. Thus, against the context of techno-economic change in NewSpace as dubbed by Gonzales [2], one ought to consider the "social and institutional changes … necessary to bring about a better 'match' between the new technology and the system of social management of the economy" [25], in this case, the influence that sector changes brough about by new entrants, may have for cybersecurity.

*Why is critical national infrastructure in space unique?*

The integration of cyber-to-physical and cyber-to-cyber interactions has led to new threat actors and more complex threats within the space ecosystem. The private and public sectors will have to deal with novel kinetic-physical, electronic, cyber and Earth-based threats that likely to need changes to risk management and security controls [29]. Barriers to entry are lowered as new technological advancements such as reusable rockets and small satellites facilitate cost-effective access to these infrastructures [28]. Thus, there is a need to understand the degree of influence new entrants might have, especially when a profit-based policy decision goes beyond the authority of a state to control and audit activities in space and cyberspace [29].

Space is considered one of the CNI sectors by several bodies, such as the UK NPSA [30] and the Council of the European Union in the NIS2 Directive [31]. The US CISA [31] also views space as part of critical infrastructure due to its importance to the communication sector, but unlike the UK and the European Union the US does not view space as sector itself. As such, it is important to consider if lessons learnt in Terrestrial CNI sectors apply to space. Terrestrial CNI have undergone significant changes, such as opening operational technology networks to the Internet and IT networks [32], leading to an increase in the complexity of threat actor and threats seen in terrestrial Critical National Infrastructure (CNI) [27].

When examining the technology used in terrestrial CNI, such as nuclear power stations and the water sector, we see that the that most critical systems are part of the Operational Technology (OT) environment. These systems (e.g., industrial control systems) are specifically designed to focus on reliability and availability and have been used for many decades [32]. The OT systems used are critical to the operation of most terrestrial CNI sectors and are significantly different from IT systems. However, the interconnection of IT systems with the OT environment has become a recent trend. A similar shift can also be seen within the space sector.

Furthermore, the increased usage of COTS solutions brings threats from the IT environment to space [33]. And, although the critical systems in terrestrial CNI are still bespoke, the interconnectivity opened the sector up to the vulnerabilities and threats of traditional IT, similar to what is happening in space. For example, resource constraints and ownership issues due to multiple organisations' involvement are also seen in space [34]. Additionally, once a satellite is launched into space, there are challenges such as the traditional high costs [35], easily disrupted communication links [36] and limited resources of the system [37]. These issues exist in and cause concern for terrestrial CNI sectors as well [26].

Within the terrestrial CNI sector, much emphasis is placed on physical security, although in recent times, that has shifted [38], [39]. Now we see the adaptation of cyber security and techniques such as honeypots [32] entering the sector. In the space sector, physical security has been less of a focus as the focus has been on the security of ground communications to the satellites [40]. This is unsurprising as physical access to systems in space has historically only been within the capabilities of nation states, but this is changing as can be seen with companies such as Starlink and OneWeb [3] and D-Orbit. Hence, unlike terrestrial CNI, where physical and direct access has been a staple and a significant concern for decades NewSpace must now consider direct access to the satellite in their threat models.

The terrestrial CNI sector comprises of a small number of organisations, partially due to the high cost of entry, specialised knowledge required, and the heavy regulation

[41]. However, in NewSpace, we see a higher number of new entrants, due to the current push to use COTS equipment and the lowering entry costs. This is a significant difference from terrestrial CNI, where there is more collaboration between organisations. In contrast, dynamics are yet to be discovered in the NewSpace sector. The space sector has also been less regulated than the terrestrial CNI sector, and the national laws related to space vary extensively worldwide [42].

Additionally, most laws related to commercial space activities that have been investigated [42] focus on public health, national security and property. This raises the question of how to adequately oversee and regulate activities within the space sector if the regulations differ in each country. Further issues exist, as these regulations do not necessarily focus on cyber security. However, it also raises the question of establishing who can provide comprehensive legislation for commercial activities in this area if there is no sovereignty in space under the UN Outer Space Treaty [43]. This issue is specific to NewSpace; in terrestrial CNI, the question of sovereignty and regulation can be answered clearly.

There are existing efforts to reduce the risk related to these new threat vectors in space, including the design and implementation of secure software engineering (SSE) procedures for protecting these high-value critical mission systems. The European Space Agency (ESA) has recognised the importance of SSE practices and the need to be standardised by the design and implementation of an appropriate Generic Application Security Framework (GASF) [44]. However, the investigation into a secure software development lifecycle and verification requirements for safety, correctness and security might be needed to protect space systems successfully [71].

In summary, there are new opportunities for commercial exploitation in the space sector. But there is also potential for unexpected cybersecurity consequences due to these new entrants to the space market and a higher cybersecurity risk for SMEs. While there are similarities between terrestrial CNI and space CNI, there are also significant differences that changes how space cybersecurity needs to be approached. Therefore, in this work we sought to answer the following question:

How have new entrants to NewSpace altered the practice of cybersecurity according to industry stakeholders?

## 3. METHODOLOGY

*Sampling*

To understand the expected influence of new entrants to NewSpace on cybersecurity according to perceptions in the industry, we conducted a series of semi-structured interviews with members of organisations involved in the design, development or review of space systems devices and services. As adopted in the UK Cybersecurity Standards Report [45], the sample included both commercial and non-commercial organisations (including both governmental actors and NGOs), and in terms of size, it ranged from startups and SMEs through to large or global organisations. Organisation size was judged based on the convention adopted in the UK Cyber Security Breaches Survey 2018 [19], which split the organisations into micro-businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees), and large businesses (250 employees or more). The sample of interviewees was reached through suggestions from the Future Artificial Intelligence and Robotics for Space (FAIR-SPACE) research hub. Some interviewees are members of the FAIR-SPACE consortium, and others have been identified through a subsequent phase of snowball sampling where participants recruit other interview participants among their acquaintances. The sample is a cohort of 8 participants (see Table 1) consisting of experts from businesses involved in providing space systems products and/or services and organisations representing space sector regulatory or standards bodies.

**Table 1 Background information on the 8 organisations' interviewee participants, including organization type, organisation size, expertise and country where the organisation is based.**

| Respondent code | Organisation type | Organisation size | Expertise | Country |
|---|---|---|---|---|
| [1] | NGO/Governmental* | Large | Policy | UK |
| [2] | NGO/Governmental | Small | Cybersecurity | US |
| [3] | Commercial | Large | Cybersecurity | Canada/UK |
| [4] | Commercial | Small | Space system engineer | Canada/UK |

| | | | | |
|---|---|---|---|---|
| [5] | Commercial | Large | Academic and research | UK |
| [6] | NGO/Governmental | Large | Cybersecurity | UK |
| [7] | Commercial | Medium | Space system engineer and cybersecurity | Japan |
| [8] | Commercial | Small | Space system engineer | Mainland Europe |
| *NGO/Governmental" refers to the organisation being *either* a not-for profit non-governmental organisation (NGO) *or* a governmental organization. | | | | |

Overall, the sample consisted of 5 businesses and 3 NGO/Governmental organisations. Of these, 4 were large organisations, 3 small, 1 medium. Furthermore, in recruiting our study's participants, we actively strived to include at least a non-Western representative because an underestimation of cultural diversity in cybersecurity leads to less awareness and weaker practices and higher risk [46]. Hence, the countries whose views were covered in our sample include Mainland Europe, UK, US, Canada, and Japan (Table 1).

This study involving Human Subject Research received full approval by the University of Warwick's Biomedical & Science Research Ethics Committee on the 5th of February 2020 (ref. no. BSREC 52/19-20).

*Risk factors questionnaire and approach to thematic analysis*

To plan a rigorous thematic analysis, we followed the guidelines set by [47]. In devising the interview questionnaire, we first outlined the scientific method for the analysis and opted for a broadly deductive approach. The questionnaire was therefore constrained by the concepts we set from the start, namely NewSpace *risk factors* in innovation in commercial space, which are illustrated as follows:

- Satellites are built with components from a *global supply chain* [49] which means that the components making up space systems are often designed, operated and maintained by different organisations, each providing an opportunity for cybersecurity vulnerabilities. Hence, cybersecurity responsibility is complicated by the complexity of space asset development, management, use and ownership [34].

- *Dual-use technologies*, where space systems can provide functionality for both military and civilian applications. Dual-use systems (e.g., autonomous debris deorbiting) could be used maliciously (e.g., deorbiting rival satellites). Dual-use technologies make it more challenging to ascertain whether a country is doing military operations through seemingly civilian activities [48]; hence security risks posed by dual-use must be evaluated and mitigated.

- Another risk factor are the *orbital paths and the location of terrestrial communication stations* as the large number of satellites orbiting the Earth traverse many territories and satellite communications are transmitted to ground stations across many regions. This means that ground stations facilities are shared across multiple organisations [49], and hence security become more difficult to implement due to multiple influences and security cultures.

- The rising popularity of *satellite constellations* [34], [48] as a technology trend may impact cybersecurity as, in 2017, it was estimated that there were about 700 small cube-sized satellites (Cubesats) in orbit [34]. At the technological level, it is much easier and cheaper to attack a satellite than to block an attack, mainly when there are many satellites to defend. Satellite constellations can increase risk as the attack surface also increases, but it is in terms of (i) reducing processing power for individual satellites, (ii) satellite-to-satellite communication that can be attacked, (iii) increased need to trust other satellites to do the work and handle errors in other satellites appropriately. However, it is also important to note that constellations also

introduce redundancy which reduces operational risks in terms of availability.

- *The logistics of software updates* is another risk factor. One of these difficulties is timing, as satellite firmware updates may require more than a single fly-by and can only perform the update when the satellites are visible to ground stations [50]. Also, performing software updates is a necessity given the prolonged life cycle of the space system, as a mission can last decades [34].

- The relevance of *advanced persistent threats (APT)* [50]. An APT is a stealthy threat actors that acts over a long period of time. APTs are often used to exfiltrate vital information from a business or government target over a long time without detection. Given the interest of both actors in space ownership, APTs may become particularly prominent in NewSpace.

- Another issue is the *wider implications of attacks* on space systems. The criticality of space systems is acknowledged, and governments are working to mitigate issues. For example, the UK has proposed the world's first National Timing Centre to protect the country from risk of satellite failure [51]. As [34] argues, space systems are a single point of failure for various industry sectors. For example, the route for compromising US commerce would be to target satellites instead of attacking Amazon.

- Commercial interests favour *market-pull* technology developments where ideals of 'security by design' [52] are not contemplated and development is sped up to create a competitive advantage. This issue is exemplified by low-cost space missions where the commercial price of implementing cybersecurity measures rivals the value of the mission and makes little economic sense to the operator [49].

- The *organisation of the workforce* is a challenge to the cybersecurity of space systems because this needs to be highly specialised and diverse. Cybersecurity requires funding for specialised staff [34], without which, systems engineers are left to address security vulnerabilities without adequate training.

- There is a general lack of cybersecurity *standards and regulations* in space systems across the world [34], [48]. Much regulation is limited to the International Telecommunication Union (ITU) [34], which only regulates frequencies but does not prevent, for example, a satellite being used as a base to launch cyber-attacks. [48] underlines the lack of definitions in national policy, e.g. there is no internationally accepted definition of a *space weapon,* and anything could be used as a weapon in space. For example, a civilian satellite could be used as a weapon to collide with and destroy another satellite.

- According to some, cybersecurity is a victim of its own secrecy, which constitutes its *methodological limitations*. Knez et al state, "historically, threat data has tended to be … often highly classified, limiting its availability to many system security engineers" [53]. Hence there is a tension between the need to share cybersecurity practices and disclosing vulnerabilities in an emerging space sector and the need to protect intellectual property or classified information. Making it easier for adversaries to use the same exploits across organisations, as these might not be patched due to this secrecy.

Our questionnaire was developed based on these risk factors, which allowed us to formulate a question guide (see Appendix). Each question topic was formed of guiding questions and follow-up questions to enable the respondents to provide illustrative examples and facilitate the interviewer understanding the responses [54]. These were selected rotated according to the background of the respondents. These initial risk factors allowed us to isolate the first layer of themes in the dataset, i.e., 'technology and infrastructure', 'cybersecurity maturity', 'market incentive', 'regulation, guidelines and standards' and 'vulnerability-sharing culture'.

We adopted delineation of essentialism and constructionism as the research principles guiding how themes are analysed. As [47] put it, in an essentialist approach, one can theorise "meaning in a straightforward way, because a simple, largely unidirectional relationship is assumed between meaning and experience and language". In contrast, in a constructionist approach, "meaning and experience are socially produced and reproduced" rather than being inherent in individuals [47]. Applying these principles meant that alongside technical considerations, we considered the wider cultural contexts such as different culture(s) of cybersecurity practices and the divergence in culture(s) of vulnerability-sharing and elements of economics (through the workings of the cybersecurity market). Regarding conventions for representing prevalence in thematic analysis, we use the expressions such as 'the majority' of participants [55] 'many' participants [56] or 'a number of' participants [47].

Lastly, to mitigate the research and researcher bias that may impact on qualitative research, we used a multidisciplinary approach in which separate research enterprises come together for approaching common problems [57]. Cross-disciplinarity has been researched as a way to suggest advancements in the NewSpace age, and its capacity to provide solution to complex space-related [58]. The multi-disciplinary approach we used – consisting of tackling the research brief from the point of view of sociological sciences, computer science, cybersecurity, space cybersecurity, and systems engineering – ensured a diversity of inputs coming from a team of 4 researchers, flowing into both the design, analysis and review of the results of the research. We used NVivo 12 to manually code the data as this allowed us to preliminarily isolate quotes under (deductively pre-set) key themes and re-organise material under (inductively) emerging sub-themes in several iterations of analysis until saturation was reached.

To address the credibility of our results we discussed and critically evaluated them in our multidisciplinary researchers' team – as the example set by [58] – in order to both interpret and assess their meaning against the various disciplinary backgrounds the different researchers brought to this research. The challenge we had was to steer a path between the abstract theoretical approaches of the humanities concerning, for example, choices of methods of textual analysis, the emphasis on blind economic growth as often unilaterally found in technology adoption and much of innovation studies, or the lack of political or cultural perspective found in hard sciences and technical topics. The current work is the result of extensive cross-disciplinary dialogue over our methods, results, as well as ways of presenting them in a balanced manner for a varied public, in order to ensure both research trustworthiness but also to promote ethically responsible relations between researchers and subject research [59] for further, and hopefully responsible, advancements in NewSpace research.

## 4. Analysis

We grouped the results of our analysis led by the above-listed risk factors, under three emerging key themes: 1) Technology and Infrastructure, 2) Cybersecurity Maturity, and 3) Regulation, Guidelines and Standards. The presentation of results under these three themes follows the structure laid out in Fig. 1.

### *Technology and infrastructure*

*Dual-use technology*—Dual-use technology is perceived as a beneficial challenge. A respondent explains that the "dual market between military and domestic" [P1] will improve security standards because if companies "want to … be able to sell their goods to the military market, then they've got to have a level of cybersecurity" [P1].

However, the uptake of commercial off-the shelf (COTS) components may affect the dual market for entrants in NewSpace. A participant from a large commercial organisation states that "the cyber threat has increased considerably … and part of that … may want to use commercial off-the-shelf components" [P5]. COTS are already built and must be adapted to be secure for space and the cybersecurity threats unique to the area. But this is strict because "Cyber is very difficult, to reverse engineer into technologies that essentially have already been built" [P6].

*Ground station communications*—A critical cybersecurity and security threat is due to enhanced access for new entrants to the ground station. A respondent declares a ground station as "possibly being a single point of failure for multiple critical systems in the event that it is hacked/spoofed/jammed etc." [P3].

A reason concerns securing downlink communications: "it's quite possible to intercept communication security between the satellite and the ground, and if a satellite doesn't have a good security measure, then it's absolutely possible to hijack it and terminate the mission" [P8]. Uplink communications and general security are also surface areas of vulnerability since "if someone were to communicate with our satellite from ground … that would be a threat" [P8]. Thus, shared ground stations facilities constitute a cybersecurity threat that is specific to new entrants in NewSpace. So does the growth of mobile ground stations. A participant from a NewSpace startup explains that "there's a lot of people making their own ground stations today … if maybe people have mobile ground stations, they just need to know where the satellite is, know the encryption key and in theory should be able to communicate with the satellite" [P8].

*Supply chain*—Within the threat area of 'technology and infrastructure', the supply chain is also considered a key area of cybersecurity vulnerability.

> "supply chains are probably our biggest area of risk [because at this time] we can't assure ourselves [that] we've not got any chips in satellites that aren't suddenly gonna be able to come live five years down the line and do something drastic … and we'd like to get ourselves to a position where 80 percent [of chips] we can say were safe" [P1].

Along this line, a respondent specifies that the country of origin of space systems components is, in fact, a concern, as "most of the circuit boards that are used in support of processing come from Asia – [there is a] significant risk of embedding sensors from China - lots of examples" [P3]. However, it is not only the country of origin of component

matters in the supply chain, but "also everything else within that, you know, how is it built… How does that country assure themselves … [that] their supply chain is secure" [P1].

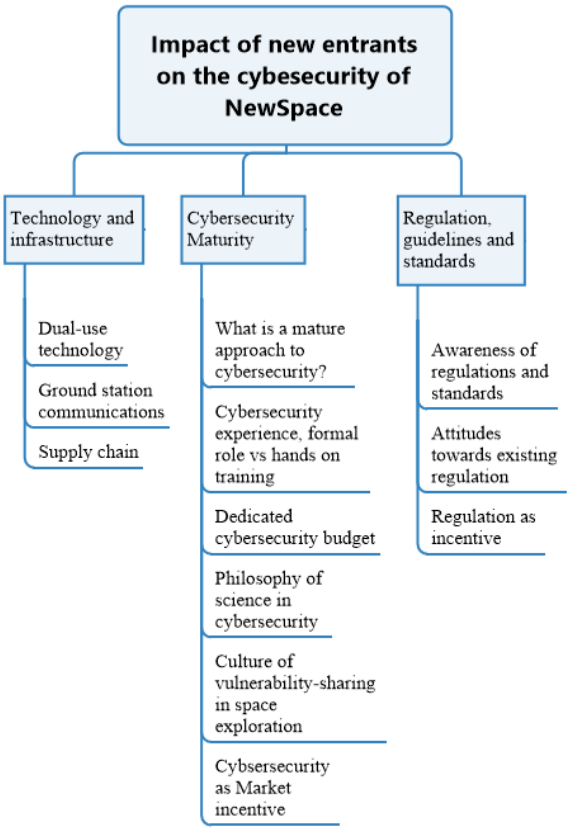


**Figure 1. Summary of the key findings concerning the expected influence of new entrants to the space sector and showing the cybersecurity challenges of NewSpace**

Supply chain security is a key issue in these environments. Respondent [P1] states that the cheapest way to attack a space system is to embed someone in the process of building the satellite to

> "change the software on the ground because then you … infiltrate the team or whatever or you make sure the software isn't really the version issued" [P8].

This is a prime example of how, for example, disgruntled employees or other actors with direct access to the organisation or any of the organisations in the supply chain can impact the operation of systems in space. Like other critical sectors, a strict and water-tight process needs to be used both with internal development and with technology developed externally.

*Cybersecurity Maturity*

*What is a mature approach to cybersecurity?*— Cybersecurity maturity emerged as an area directly influenced by the new entrants to the space market:

> "in a NewSpace environment in the last, let's say, five/six/seven years, the potential for having … cyber weakness in the system has grown substantially and, at the same time, the practicality of having a much larger group of people who could start to access your spacecraft has also grown." [P5]

New entrants to the commercial space sector focus on product development, not necessarily on how things can be attacked and what impact they can have. One respondent states that

> "the concern I've got is how high in the consciousness of our emerging space players … who are this proliferation of start-ups and small businesses and business coming in from an adjacent sector into space, [are] their cyber security skillset, like when they say, for example, 'Hang on, … I want to be developing my telescope or my little radar thing'. Do they have a mind of, 'And I wonder what the vulnerabilities of that would be and what that means to my mission and the missions of others as well.'?" [P6]

Cybersecurity is a very specialised discipline, but with a lot of new players jumping into production, everyone saying, "I can build a satellite, I can, you know, I can do this" [P6], there emerges "a wide disparity of the understanding of risk and cybersecurity … about what are the outcomes if something bad happens" [P6]. Here, levels of cybersecurity's maturity effectively generate a cultural clash between smaller and larger organisations:

> The difference in cybersecurity readiness in amateur versus commercial players heightens the need for "a more … widespread and mature … approach to cybersecurity" [P6].

Cybersecurity maturity as "a more mature approach would be a uniform approach, so everyone … involved in developing space-related technologies at least has some … form of … understanding of the risks involved by attacks or degradations manifested through the electronic domain" [P6].

*Cybersecurity experience, formal vs hands-on training*— Unsurprisingly then, there are discrepancies in practices following from cybersecurity maturity. For example, the

length of involvement in cybersecurity varies according to whether an organisation is an NGO/Governmental organisation, or a business. Participants from NGOs and governmental organisations show a mix of longstanding experience in cybersecurity dating "all the way back to about 1997" [P6] as well as the more recent experience of "18 months" [1]. Large and medium organisations showed a long-standing, hands-on involvement with cybersecurity dating back to the 1990s [P3] or "since about 1985/1980…" [P5]. On the contrary, small organisations showed a mix of longstanding experience, e.g. 11 years [P2] and less experience "This is something new we are entering … So [cybersecurity] it's very novel" [P8].

In terms of the type of involvement, NGOs, and governmental organisations show a predominance of formal, dedicated cybersecurity roles across different governmental departments [P1] and [P2]. On the other hand, small, medium and large commercial organisations prefer a hands-on experience of cybersecurity rather than a direct or dedicated cybersecurity role. A respondent illustrates this point: "My experience and my knowledge come from applying security to the ground segment and the system we develop" [P7].

Also, cybersecurity training is referred to as self-development that is down to an individual, rather than as formal training embedded in workforce management practices:

> "I am largely self-taught and have gained my background primarily through practical experience gained via participation and responsibility for many programmes" [P3].

*Dedicated cybersecurity budget*—The lack of a cybersecurity budget is one of the biggest areas of risk for commercial organisations. A respondent from a SME confirms that despite taking security very seriously [P7], they have no dedicated cybersecurity budget. However, the lack of a dedicated budget emerges as a sector approach, not the characteristic of the SMEs entrants only. A respondent asserts that "I know very few companies have a cybersecurity [budget] on board" since "I've been working for the big companies, too" [P7].

The justifications concerning the lack of cybersecurity budget concern trade-offs between cybersecurity expenses and security:

> "it's a balance between how much it costs…to implement security" [P5].

Additionally, from our interviews, it emerges that it is difficult to understand what effective cyber security is and what a sufficient cyber security budget is, if one does not understand it well.

> "There is a wide disparity of the understanding of risk, and cyber security about what are the outcomes if something bad happen … Now, let's say a CubeSat which costs £100,000, you know, to build and to launch …you would say, 'How much of that my budget am I going to spend_? Am I gonna spend £100,000 on cyber for £100,000 mission?' the answer is no that doesn't make sense. You know, you might say, 'Right, I need…' Let's say £2,000. So, what would that cover, you know, an assessment of your little company" [P6].

*Philosophy of science in cybersecurity*—As part of illustrating levels and features of cybersecurity maturity of NewSpace entrants, we identified different *cybersecurity philosophies*. That is, NewSpace actors would entertain inductive, deductive or abductive approaches to cybersecurity. We found that respondents from small to medium businesses showed a more marked propensity towards experiment-based approaches (inductive) to cybersecurity, where 'experiment' refers to mission preparation:

> "From our work progressively […] we can formulate requirements, requirements for the cybersecurity […] the solution is, you know, work in progress" [P4].

However, this inductive, experiment-based approach is considered by NGO/Governmental organisations as having a potentially negative outcome:

> "you could have some companies, okay, who don't do any cyber, they launch their satellite, it gets hacked, and it falls out of the sky or stops functioning or, or gets held to ransom and that company will go bust […]".

This view suggests that for some, experiments may, in fact, lead to what a participant referred to as "a Darwinian approach" [P6] in the sector, where entrants to the NewSpace self-select themselves out of the market by failing through cybersecurity accidents. This participant's judgement towards' an experiment-based approach to cybersecurity, is that of a less mature approach.

Generally, participants from all organisation types, from both NGO/Governmental as well as large and small businesses, claimed to adopt a deductive or management approach to cybersecurity. This approach would include management procedure to cybersecurity such as producing regulations, asking and following expert advice, collaborating and co-creating systems with experts. For

example, a small NGO/Governmental also states they are also working on a cyber-readiness level and a series of evaluation criteria for space systems [P2].

A third approach that has emerged is abduction, as found in semiotic approaches to philosophy of science. This type of reasoning amounts to an *intuition about whether a something may be the case* [72] and is hypothetical in nature. Thus, in the context of cybersecurity of space, abduction could describe the kind of hypothetical reasoning behind guessing whether a vulnerability *might* be the case. In this view, speculation can help space organisations hypothesise potential vulnerability issues and be anticipatory. For example:

> "that is generally a question of a potential vulnerability rather than where we've seen somebody actually do something, and we're trying to counteract it. So, on the spacecraft that's very rare, but, you know, we do periodically look at it and say, 'Hmm, we think there might be a vulnerability there,' or the [expert] would come in and say, 'Look, we've seen this happening, we think this might generate a vulnerability for you, can you look into it?'" [P5]

Approaches to security – whether inductive, deductive or abductive – are usually business-specific. Therefore, even a clear yet generic understanding of the possible impact of IT systems being hacked, does not automatically include an understanding of the impact of a cybersecurity incident in the space environment.

> "most of our effort goes on cyber security issues relating to access to our company, systems from outside, not necessarily the spacecraft" [P5]

*Culture of vulnerability-sharing in commercial space exploration*—We then uncovered attitudes towards vulnerability-sharing. First of all, perceptions emerged about what 'the others' may be doing in the NewSpace industry in the event of a vulnerability.

In general, the majority of companies felt that other companies in NewSpace would not disclose vulnerabilities, or they would do it only partially. A respondent feels that businesses do not share information and are very reluctant to share their vulnerabilities [P1]. Another respondent adds that however, government also will not disclose that sort of issues [P7]. In other words, it emerged that the NewSpace industry is not much keen on sharing anything [P4], concerning vulnerabilities. A large business respondent underlines how some sharing takes place mostly on the 'cyber side' but not enough on the physical integrity of space platforms against threats such as physical damage, e.g., via cyber-kinetic attacks, directed energy weapons, electromagnetic pulse, jamming etc. [P3].

Secondly, there emerged reflections on what new entrants would do if they discovered a vulnerability in their space systems. Respondents provided differing opinions concerning whether new entrants feel the moral obligation to share vulnerabilities. A respondent from a large commercial organisations agreed that they would disclose vulnerabilities because moral principles do not leave a choice as to whether to disclose or not: "as a matter of principle […] we always would look at the safety before the reputational damage [P5]". A participant from a NewSpace startup, shared a similar cybersecurity ethics:

> "I grew up in the space era of where everyone's fair and honest, I think we would have to be fair and honest to say, 'Look, this is what happened, this is the implementation we did to fix it,' or,'"This is the risk,' or, 'We've decommissioned our satellite'." [P8]

On the other hand, some respondent's view on vulnerability-sharing is guided not by moral principles but by practical ones:

> "Sharing and disclosing information about vulnerabilities is definitely not a universally accepted practice … it may be actually the best approach, but not everyone may agree with that or not everyone may accept it … so it's kind of perfect world solution … [but] the real world … you know, real world is not perfect" [P4].

A practical concern of vulnerability disclosure is that it could advertise a vulnerability and ultimately serve as an invitation to attack.

Also, we found that vulnerability-sharing is also considered as a cultural or almost subcultural choice, as disclosing a software vulnerability "is only true for certain groups of people, who are more closely related to software developer as a lifestyle than software developer as a business" [P4].

There was uncertainty regarding what businesses they think they would do if they discovered a vulnerability in their space systems. A respondent states, "if we suffer an attack, honestly, I don't know what we will do [P7]". In a mediating position, another respondent states that maybe they would discuss it with other applications on the ground, the European Space Agency and others [P8].

*Cybersecurity as market incentive*—The market incentive for cybersecurity and the costs involved are linked to "reputation … and the financial cost of fixing or replacing whatever it is that's been damaged or lost [P1]". Therefore,

there is indeed an incentive for cybersecurity in the market, though this is a view predominantly held by NGO/Governmental organisations. The incentive constitutes a competitive advantage in the international market: "We want to meet our competitors' market, and if other countries have got a level of cybersecurity, we risk losing substantial ground within the sector" [P1]. Another respondent states, "paradoxically, [right now] it is cheaper to be more secure." [P2].

Non-commercial organisations, like military or defence departments, are likely cybersecurity customers. In working with the military sector, there is a higher requirement for cyber security [P1]. On the topic of providing space services for the military market, a respondent feels confident that they would be willing to pay 'extra':

> "if we were ever … to make a servicing satellite for the U.S Air Force … they would pay a lot more just to make sure that it's 100 percent secure and it's resilient, and the price could really increase significantly just because you can provide that level of extra security and resilience" [P8].

Indeed, a respondent perceives that defence might be the only likely customer for cyber secure space products and services.

> "The only case where [customers would be willing to pay more for cybersecurity] is if you're working with the Ministry of Defence or Department of Defence, where they may insist on having a higher level of security. Therefore, the manufacturer can justify a higher price than he would have done if he had gone with a commercial level" [P5].

New entrants to the space sector therefore seem to uphold cybersecurity by design as an ideal for competitiveness in their business model: "in regard the … question, whether [the customers] will pay more if we implement cybersecurity, no … they will assume that we implement by default …" [P7].

However, outside of the military market, there is uncertainty about cybersecurity's market appeal. A respondent claimed that small businesses would be unlikely to invest in cybersecurity "In a cost-constrained environment and with a lack of awareness, security is a tough sell … I would say [cybersecurity is] difficult for startups" [P3].

The view from a startup, however, is that cybersecurity may be worth the investment:

> "I think once our business model is up and running and they see the potential threat and revenue loss they could make if it were to be attacked, then they would change their mind …" [P8].

For startups as new entrants, offering cyber secure space systems and services may be indeed added value:

> "I'm pretty sure [potential customers] will be interested in paying [more for cybersecurity]" [P4].

However, a participant representing the point of view of a large NGO, is sceptical about whether large businesses may be interested in cybersecurity.

> "Having talked to them, they do say it's not something they are going to put their funding, they couldn't afford to spend X thousands of pounds on cybersecurity, so it's that investment. [the issue is] how we get ourselves past that and how they realise that this is a priority and you do need to invest in it…" [P1].

The reasons for such scepticism concern the difficulties involved in remaining competitive in a new market. Firstly, "the margins are very slim on the spacecraft manufacturing" [P5] because "upstream it's a very, very commercially tight and competitive business where the satellites are complex, they're high risk, they're technology demanding, and the customer always demands the lowest possible price" [P5]. The longer experience of the hardships of being in the space market was referred to by an interviewee [P5] as 'commercial tightness' and 'competitiveness'.

*Regulation, guidelines and standards*

*Awareness of regulation and standards*—Among the small organisations, both commercial and non-commercial organisations displayed an awareness of specific regulations and standards. An NGO/Governmental respondent [P2] mentioned Policy 12 from the Committee on National Security Systems and the law for the licensing of private remote sensing systems (15 CFR 960) (in the US). A small business respondent reports being aware of specific encryption regulations for amateur satellite owners [P4] by pointing the interviewer to internet links about the terms and conditions of OFCOM (UK) and the US's Experimental Licensing for Amateur Radio Frequencies. Another small business respondent shows awareness of standards concerning the autonomy of vehicles, that is, the European Cooperation for Space Standardization (ECSS) Autonomy Standard Four, published by the European Space Agency [P8]. The medium business respondent reports having implemented ISO 27000 standards at various workplaces, which in contrast to the autonomy standards mentioned above, "It's not space specific. I think this is security in general" [P7]. The same respondent mentions Advanced

Encryption Standard (AES) which reports having

> "used … for encryption over telemetry, encryption over tele-commanding, out an indication of the tele-commanding" [P7]. The respondent concludes that "this standard is the minimum, just to implement" but in the event of a military customer, "then sometimes they require you to encrypt everything, and they have … They install their own hardware in the spacecraft." [P7]

*Attitudes towards existing regulation*—Regarding attitudes towards regulation, the majority of organisations perceive existing cybersecurity support structures and communication links as having issues and needing improvement. A large NGO/Governmental respondent thinks that businesses should be reporting their cybersecurity issues to the National Cyber Security Centre, but is unsure whether this actually happens or not, "because NCSC won't share that with us" [P1]. Along the same line, amongst the businesses a perception emerges that National Cybersecurity Centres are useful only to an extent because "they can't disseminate [the vulnerability information] entirely given the classification of the material".

A small NGO/Governmental respondent perceives existing regulations as inadequate, a symptom of which is that they are too short, "there's, like, a number of sentences that you could probably count on one hand" [P2] and ineffective. This is because regulation is not utilised by the Department of Defence [P2] and because attempts to prescribe that space business should have a data protection plan contrast with the practice of "commercial organisations actively hid[ing] information on these data protection plans they submit" [P2].

Furthermore, the view of a large NGO/Governmental is that regardless of its level adequacy, regulation on its own is not enough since it "is very kind of tick box… you tick all the boxes saying, 'I'm 100 percent safe,' and then [a security incident still] happens" [P6]. The respondent adds that regulation on its own may leave gaps because "if you overly control, then everyone's waiting to be controlled" [P6]. The respondent holds the view that alongside regulation, a 'regime approach' stimulation is also required, as that which would

> "enable activity rather than control it…you do rely on much more understanding and awareness and education… in a complex environment with lots of stakeholders all of different capabilities and maturity in cybersecurity. You raise their knowledge and awareness… to actually get people to start thinking about cyber as almost an intrinsic or integrated part of their business planning" […].

The respondent also underlines the practice held by Scottish Business Resilience Centre (UK), which "encourages cybersecurity into the children curriculum at school, then to spread this knowledge and awareness out through specific organisations in Scotland" [P6] and can perhaps be seen as a best practice example of regime 'approach'.

There is also a perception of licensing processes needing improvement. A large business respondent states, referring to the use of dual-use technologies, that "the issue is becoming a greater consideration; however, the mechanics of government in terms of adjudicating the issuance of a licence based on this criterion is not yet sufficiently rigorous" [P3]. On the other hand, new entrants show a concern about not being able to fulfil the criteria "It's not that [the regulators] request and ask many, many things […] it's also whether our system is capable of doing that" [P7].

*Regulation as an incentive*— Respondents commented on the space regulators' role in incentivising cybersecurity. Regulation has so far been gentle, as a respondent states, "We haven't been putting any barriers up" [P1]. However, there are expectations with gentle regulation, there may be little incentive for cybersecurity. It is a respondent's opinion that businesses "won't invest in cybersecurity until […] the licensers, as the regulators, tell them they have to" [P1].

Regulators are perceived as having a strong potential for incentivising cybersecurity. A respondent states that "if someone hijacks one satellite… and the regulator says, 'Stop communication,' and you don't make revenue, then that's such a big loss and they would have thought, 'Oh, maybe we better invest in it'" [P8]. Furthermore, there is some evidence of the impact of regulation on cybersecurity practices. For a respondent these are "part of our requirements and it's also part of UK, in terms of obtaining the mission licence to operate the satellites" [P7]. Hence, regulation is perceived by new entrants to the space market as providing a key cybersecurity incentive through 'guardianship'.

In our data, we found some illustration of a regulator's concrete strategy for incentivising cybersecurity:

> "There's a, there's a toolkit that I'm producing for the industry, which will take them through supply chain mappings that they can identify vulnerabilities and then with that, assess their level of risk, and then based on their level of risk, and that's financial risk as well as reputational damage…there's a whole range of risks, a level of cyber security that we're suggesting that they adopt. But said, that will be voluntary at the moment. We're looking more in the future to

become mandatory, but at the moment, it will be voluntary" [P1].

So far, these strategies are not mandatory and also "not technical at all" [P1].

## 5. DISCUSSION

Most of the participants agreed that *communication links with ground station* was the most prominent threat area posed by technological advancements in the NewSpace sector. Secure links with ground stations appear to be more than a security concern, as [49] argue, but in fact, it is perceived as *one of the most difficult cybersecurity challenges* the sector faces. Also, the *supply chain* was seen as an area for concern, with the country of origin of space systems components being singled out as a specific issue. The rising use of COTS made it unclear whether the dual-use market is still valuable. These threats are also relevant to the terrestrial CNI sector, where research into mitigating these is also ongoing [60]. However, within NewSpace, there are many more elements to this such as the more openness of the sector and the move towards more interconnectedness.

Cybersecurity maturity has changed in recent years, and with NewSpace the potential for exploitation of weaknesses has increased. We found that new entrants in NewSpace need *to adapt to a new type of cybersecurity maturity.* Our findings defined cybersecurity maturity as emerging from specific cybersecurity expertise in the workforce, dedicated cybersecurity budget, philosophy of science, cultures of vulnerability sharing and market incentive.

Concerning specific organisations workforce and dedicated roles, there was a discrepancy between NGO and governmental organisations, which showed a predominance of formal, dedicated cybersecurity roles across different government departments and commercial organisations, where cybersecurity as a dedicated role is not easily covered, and hands-on, ad-hoc training predominates as means to fill cybersecurity expertise gaps. However, this developmental approach may leave temporal gaps in filling cybersecurity needs or may not always provide a specialised solution for the particular function and threats of the system [34]. This finding confirms that the space industry and cybersecurity efforts are behind that of other high-technology sectors [34].

Also, we noted a general, sector-wide lack of a dedicated budget for cybersecurity, a finding that is still consistent with the literature [61]. This view is grounded in perceived trade-offs between direct costs and perceived gain (which are not immediately detected). But it is also tricky to justify cybersecurity investments, especially when one does not directly experience attacks - and this could be because there are none or because the security is indeed effective. It can be difficult to understand the threats of space and the difference in threats between space and Earth, especially for new entrants to NewSpace.

Regarding the reasoning underwriting different levels of cybersecurity maturity, we detected approaches that in philosophy of science would be called deductive, inductive, or abductive methods. The approaches detected within the deduction/management approach included producing regulations, asking and following expert advice, and collaborating and co-creating systems with experts. Inductive reasoning amounted to experiment-based approaches to cybersecurity, but this approach was constructed as being less 'mature' by larger businesses. Also, large organisations showed a marked propensity towards abductive or speculative approaches to cybersecurity. Being creative in nature [62], this approach was positively described as being anticipatory and predictive.

Our results showed that new entrants feel that others do not share vulnerabilities or do so only partially. This reluctance is not unlike other sectors and often also includes interoperability issues [63]. But when it came to reflecting on their practice (rather on what others in the sector do), we found differing views concerning the 'vulnerability disclosure debate' [64]. Practical argumentations for not disclosing vulnerability are reputational damage, and the loss of confidentiality; practical reasons for disclosing instead are about the lessons learned. We found that different approaches may reflect the split between software development as cultural and lifestyle choice, and business interests. In the event of discovering a vulnerability, larger businesses would seem to know who they may disclose to, whereas the SMEs were less certain about what to do or who to contact. This is a unique issue to NewSpace as the terrestrial CNI sector has many regulations covering the disclosure of incidents [65] The uncertainty confirms the difficulties with coordinated vulnerability disclosure (CVD), confirmed at the very least at the European level [66].

As part of cybersecurity maturity, we found that cybersecurity bears market incentive for space businesses mainly when it comes to the military being the customer. However, any system in space can potentially affect a military system, even a non-military one. As there is an emerging sector-wide conviction that cybersecurity is an added cost, rather than an intrinsic cost of space systems. Security has historically often been seen as an afterthought in system and software development before efforts have been made to integrate security as a significant part of the development [67]. The key issue here is that regarding the reputational impact of cybersecurity incidents, it is unclear whether it matters or is it mainly a physical cost.

Interestingly, despite cybersecurity being considered an 'added cost', the majority of businesses felt they ought to provide 'cybersecurity by default' to their customers.

In terms of regulation, there was an awareness of cybersecurity guidelines and standards, including encryption but we found that the majority of the standards known were not space-specific. Also, communications amongst existing cybersecurity support structures and licensing processes were perceived as needing improvement. We also found that new entrants to the space market think that regulation provides a key incentive for cybersecurity. This was particularly true for small businesses, which are likelier to position themselves in a learning position. However, examples of described regulation were found to be non-mandatory and non-technical. On the one hand, this may give the impression that organisations in charge are still unsure about how to regulate cybersecurity in space and other challenges, such as sovereignty in space that play a part in this as well [43].

The challenges to regulating this space are unseen in the other CNI sectors and pose a unique challenge to NewSpace that will require collaboration between many fields to solve. Also, the non-technical nature of these strategies could mean a missed opportunity for new entrants to implement cybersecurity within their systems promptly and ensure their survival in the market. This may weaken the cybersecurity incentive of regulators. However, one significant objection to mandatory cybersecurity regulation was that burdensome formal requirements might make the sector too regulation-dependent and not sufficiently self-motivated.

## 6. CONCLUSION

Space exploration and NewSpace commercialisation has been growing significantly over the past years raising new challenges for the cybersecurity of this domain. By conducting semi-structured interviews guided by NewSpace risk factors with a balanced mix of experts in the sector – including commercial organisations and NGO/Governmental organisations, as well as large and small, organisations and SMEs – we set out to explore and illustrate the perceived influence that new entrants to commercial space exploration may have on space cybersecurity practices.

We identified similarities with the challenges faced by terrestrial CNI. These can be as a starting point to address some cybersecurity challenges faced in the space sector, such as adopting a cybersecurity strategy and promoting awareness. But there are also many unsolved challenges for which one cannot rely on lessons learnt from terrestrial CNI. For example, the arrival and impact of a large numbers of small companies to the NewSpace market is not seen in other critical infrastructure sectors.

The implications of these findings for policymakers and businesses are several, but in broad terms, they may include the following:

1. collaboration between policymakers and NGOs should be used to develop cultural interventions aimed at changing the cultural values associated with cybersecurity by promoting a switch of meaning from 'added cost' to 'added value' through dedicated educational campaign;

2. regulators could incentivise businesses to offer cybersecure space systems by requiring them to meet basic cybersecurity criteria – as outlined in frameworks and standards such as the Code of Practice for Consumer IoT Security [68] and NIST SP 800-53 [73]– and envisaging strong penalties if businesses choose not to do so. However, regulators must keep in mind that enforcing regulation means that new entrants to space may expect to be regulated rather than be self-motivated;

3. since in NewSpace, reputation concerning the reliability of systems is crucial, businesses could take advantage of the market competitiveness harnessed by cybersecurity and channel their resources into offering their customers more secure packages than competitors; conversely market competitiveness and the necessity to avoid reputational damage may be an area fit for stimulation and/or intervention to increase levels of cybersecurity self-motivation, tackling the issue raised in point 2) above;

4. whilst regulation ensuring minimal cybersecurity level is underway, there needs also to be collaboration amongst businesses, regulators and NGO to form a long-term plan about approaching the more complex threats that NewSpace systems are subject to;

5. since it is more beneficial if all entrants disclosed vulnerabilities than if only a part did or none did, intervention can be specifically targeted at increasing vulnerability disclosure in the industry as a whole, so that every entrant can benefit from lessons learnt;

6. vulnerability disclosure is particularly relevant for COTS users so that if a vulnerability for these devices is shared, the whole NewSpace sector can benefit; the example set by new entrants in

NewSpace could then serve as role model for other sectors for which cybersecurity vulnerability disclosure is crucial e.g., CNI, thus promoting improvements in cybersecurity culture beyond the NewSpace sector;

7. Threat information-sharing is an important process to improve security awareness and resilience within specific sectors. This is a prime objective for Information Sharing and Analysis Center (ISAC) organisations, of which there are a few active in the space sector, such as Space ISAC and EU Space ISAC. Encouraging collaboration with relevant ISACs would be a useful step to improve understanding of and resilience to cyber threats within the sector. Particularly smaller organisations can benefit from the expertise and knowledge within these platforms;

Although our study examines the cybersecurity phenomenon in commercial space exploration and has identified challenges the sector faces in dealing with new and old security threats, the study has some limitations which can provide avenues for further research. Our sample's variety could be increased to include the voice of more space organisations from the global south [69] to balance and achieve a more culturally diverse sample. Of particular importance would also be to include representatives from developing countries, for whom the cybersecurity challenges of NewSpace will be no less prominent, if not more so. Also, further work could involve public participation in the form of citizens' views, to form a balanced triad of intergovernmental relations, private corporate involvement and active cyber citizenship to manage new and challenging security environments [70].

## ACKNOWLEDGEMENTS

This work is part of the Future AI and Robotics for Space (FAIRSPACE) with Tim Watson and Carsten Maple, WMG, the University of Warwick, and was partially funded by: EPSRC EP/R026092. Many thanks to Ann Swift, Innovation & Partnership Manager at the FAIRSPACE Hub, University of Surrey, for providing crucial support in reaching out to and helping us to recruit industry partners for interviews.

## DATA ACCESS STATEMENT

Participants of this study did not agree for their data to be shared publicly, so interview transcripts are not available.

## REFERENCES

[1] Kaya, H. P., & Uzay, Ş. (2017). The Risks That Will Threaten Going Concern And Control Recommendations: Case Study On SMEs. Journal of Accounting & Finance.

[2] Gonzalez, S., 2023. The Astropreneurial Co-creation of the NewSpace Economy. Space Policy, 64: 101552.

[3] Bryce Space and Technology (2017) Global Space Industry Dynamics, Research Paper for Australian Government, Department of Industry, Innovation and Science. Available from https://www.industry.gov.au/sites/default/files/2019-03/global_space_strategies_and_best_practices_-_research_paper.pdf

[4] Chen, Z., Shi, C., Guo, H., Liu, R. and Deng, Z., 2022. Design and optimization of NewSpace modular planar antenna. Aerospace Science and Technology, 123, p.107442.

[5] Canis, Bill. 2016 "Commercial Space Industry Launches a New Phase,", Available from https://fas.org/sgp/crs/space/R44708.pdf

[6] Vidmar, M., Rosiello, A., Vermeulen, N., Williams, R., & Dines, J. (2020). NewSpace and Agile Innovation: Understanding transition to open innovation by examining innovation networks and moments. Acta astronautica, 167, 122-134.

[7] Moorman, Jr., T. 1998. "The Explosion of Commercial Space and the Implications for National Security." In 36th AIAA Aerospace Sciences Meeting and Exhibit. Reno,NV,U.S.A.: American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.1998-2.

[8] Chebukhanova, L. V., & Zimakov, A. M. (2022). Resource support of innovative small and medium-sized enterprises for space industry development in Russia. Acta Astronautica, 200, 626-634.

[9] Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA) (pp. 1-5). IEEE.

[10] Martin, Gary. (2015) "The Emerging Commercial Space Industry," 35.

[11]Airbus (2023) #NextSpace, Available from https://www.airbus.com/en/NextSpace

[12] Denis, G., Alary, D., Pasco, X., Pisot, N., Texier, D., & Toulza, S. (2020). From NewSpace to big space: How commercial space dream is becoming a reality. Acta Astronautica, 166, 431-443.

[13] Weinzierl, Matthew. 2018. “Space, the Final Economic Frontier.” Journal of Economic Perspectives 32 (2): 173–92. https://doi.org/10.1257/jep.32.2.173.

[14] Anderson, Chad. 2013a. “Rethinking Public–Private Space Travel.” Space Policy 29 (4): 266–71. https://doi.org/10.1016/j.spacepol.2013.08.002.

[15] LE 2019. Size & Health of the UK Space Industry 2018 A Report to the UK Space Agency https://assets.publishing.service.gov.uk/media/5c50691b40f0b625504f4583/LE-SHUKSI_2018-SUMMARY_REPORT-FINAL-Issue4-S2C250119.pdf

[16] Rodriguez-Donaire, S., Gil, P., Garcia-Almiñana, D., Crisp, N. H., Herdrich, G. H., Roberts, P. C., ... & Seminari, S. (2022). Business roadmap for the European Union in the NewSpace ecosystem: a case study for access to space. CEAS Space Journal, 14(4), 785-804.

[17] Rapp, L. (2020) 'Space Industry Faces Deep Transformations Post-COVID-19', Available from https://www.hec.edu/en/knowledge/instants/space-industry-faces-deep-transformations-post-covid-19

[18] Etzioni, A., (2014) The private sector: A reluctant partner in cybersecurity. Georgetown Journal of International Affairs. International Engagement on Cyber IV, 15: 69-78

[19] DCMS (2018a) UK Cyber Security Breaches Survey 2018, Available from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018.

[20] Bell, Shane. 2017 “Cybersecurity Is Not Just a ‘Big Business’ Issue.” Governance Directions, 69(9), 536–539. https://search.informit.org/doi/10.3316/informit.148981996216030

[21] Enisa (2022) SME cybersecurity, available from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme_cybersecurity

[22] Vakakis, Nikolaos, Odysseas Nikolis, Dimosthenis Ioannidis, Konstantinos Votis, and Dimitrios Tzovaras. 2019. “Cybersecurity in SMEs: The Smart-Home/Office Use Case.” In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 1–7. Limassol, Cyprus: IEEE.

[23] Kent, Cameron, Maureen Tanner, and Salah Kabanda. 2016. “How South African SMEs Address Cyber Security: The Case of Web Server Logs and Intrusion Detection.” In 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), 100–105. Mauritius: IEEE.

[24] Lewis, Riyana, Panos Louvieris, Pamela Abbott, Natalie Clewley, and Kevin Jones. 2014. “Cybersecurity Information Sharing: A Framework For Sustainable Information Security Management In Uk Sme Supply Chains.” Tel Aviv, 16.

[25] Freeman, C. and Perez, C., 1988. Structural crises of adjustment: business cycles. In: Dosi et al (eds.) Technical change and economic theory. Londres: Pinter.

[26] Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165

[27] Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. International Journal of Critical Infrastructure Protection, 35.

[28] Heracleous, L., Terrier, D., & Gonzalez, S. (2019). NASA's capability evolution toward commercial space. Space Policy, 50, 101330.

[29] Halimi, L. (2019) Cyber security and space security. Available from https://elitecyber-group.com/insights/cyber-security-and-space-security/

[30] UK NPSA (2023) Critical National Infrastructure, Available from https://www.npsa.gov.uk/critical-national-infrastructure-0

[31] US CISA (2015) CommunicationsSector-Specific Plan An Annex to the NIPP, Available from https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf

[32] Maesschalck, S., Giotsas, V., Green, B., & Race, N. (2021). Don’t get stung, cover your ICS in honey: How do honeypots fit within industrial control system security. Computers & Security, 102598.

[31] NIS2 Directive (2022). https://www.nis-2-directive.com/#:~:text=November%2028%2C%202022%20%2D%20the%20Council,transport%2C%20health%20and%20digital%20infrastructure.

[32] Marnerides, A. K., Giotsas, V., & Mursch, T. (2019). Identifying infected energy systems in the wild. In Proceedings of the Tenth ACM International Conference on Future Energy Systems (pp. 263-267).

[33] Nussbaum, B., & Berg, G. (2020). Cybersecurity implications of commercial off the shelf (COTS)

equipment in space infrastructure. Space infrastructures: From risk to resilience governance, 91-99.

[34] Falco, Gregory. 2019. “Cybersecurity Principles for Space Systems.” Journal of Aerospace Information Systems 16 (2): 61–70. https://doi.org/10.2514/1.I010693.

[35] Mrusek, B. M. (2019). Satellite maintenance: an opportunity to minimize the Kessler effect. International Journal of Aviation, Aeronautics, and Aerospace, 6(2), 2.

[36] Wang, P., Zhang, J., Zhang, X., Yan, Z., Evans, B.G. and Wang, W., 2019. Convergence of satellite and terrestrial networks: A comprehensive survey. IEEE access, 8, pp.5550-5588.

[37] Hu, Yurong, and Victor OK Li. "Satellite-based internet: a tutorial." IEEE Communications Magazine 39, no. 3 (2001): 154-162.

[38] Moteff, J., & Parfomak, P. (2004). Critical infrastructure and key assets: definition and identification. Library of Congress Washington DC Congressional Research Service.

[39] Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: a systematic literature review. Information & Computer Security, 29(5), 697-723.

[40] Shah, S. M. J., Nasir, A., & Ahmed, H. (2014). A survey paper on security issues in satellite communication network infrastructure. International Journal of Engineering Research and General Science, 2(6), 887-900.

[41] Clark-Ginsberg, A., & Slayton, R. (2019). Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. Science and Public Policy, 46(3), 339-346.

[42] Dempsey, P. S. (2016). National laws governing commercial space activities: Legislation, regulation, & enforcement. Nw. J. Int'l L. & Bus., 36, 1.

[43] Leib, K. (2015). State sovereignty in space: Current models and possible futures. Astropolitics, 13(1), 1-24.

[44] Fischer, D., Spada, M., Job, J.F., Leclerc, T., Mauny, C. and Thimont, J., (2015) The weak point: A framework to enhance operational mission data systems security. In 2015 IEEE Aerospace Conference, IEEE 1-17.

[45] BIS (2013) UK Cybersecurity Standards, Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf

[46] Kukkola, J., Nikkarila, J.P. and Ristolainen, M., 2017. Asymmetric frontlines of cyber battlefields. GAME CHANGER Structural transformation of cyberspace, p.69.

[47] Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3, 77-101

[48] Baylon, Caroline. (2014) “Challenges at the Intersection of Cyber Security and Space Security,” International Security. 53.

[49] Livingstone, David, and Patricia Lewis. 2016 “Space, the Final Frontier for Cybersecurity?” , Available from https://www.chathamhouse.org/publication/space-final-frontier-cybersecurity

[50] Hutchins, Ryan. (2016) “Cyber Defense of Space Assets”, Available from http://www.cs.tufts.edu/comp/116/archive/fall2016/rhutchins.pdf

[51] Gov.uk (2020) ' World's first timing centre to protect UK from risk of satellite failure' Available from https://www.gov.uk/government/news/worlds-first-timing-centre-to-protect-uk-from-risk-of-satellite-failure

[52] DCMS (2019) Secure by Design, Available from https://www.gov.uk/government/collections/secure-by-design

[53] Knez, Claudia, Thomas Llanso, Dallas Pearson, Tibor Schonfeld, and Kristin Sotzen. 2016. “Lessons Learned from Applying Cyber Risk Management and Survivability Concepts to a Space Mission.” In 2016 IEEE Aerospace Conference, 1–8. Big Sky, MT: IEEE. https://doi.org/10.1109/AERO.2016.7500812.

[54] Kvale, S. and Brinkmann, S., 2009. Interviews: Learning the craft of qualitative research interviewing. sage.

[55] Meehan, T., Vermeer, C. and Windsor, C. 2000: Patients’ perceptions of seclusion: a qualitative investigation. Journal of Advanced Nursing 31, 370-77.

[56] Taylor, G. W., & Ussher, J. M. (2001). Making sense of S&M: A discourse analytic account. Sexualities, 4(3), 293-314.

[57] Nicolescu, B., 2002. Manifesto of transdisciplinarity. suny Press.

[58] Tucker, B.P. and Alewine, H.C., 2023. Everybody's Business to Know About Space: Cross-Disciplinarity and the Challenges of the NewSpace Age. Space Policy, 66, p.101573.

[59] Denzin, N.K. and Lincoln, Y.S. eds., (2018) The Sage handbook of qualitative research. Los Angeles: Sage.

[60] Shukla, M., Johnson, S. D., & Jones, P. (2019). Does the NIS implementation strategy effectively address cyber security risks in the UK?. In 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-11). IEEE.

[61] Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou. 2015. "Increasing Cybersecurity Investments in Private Sector Firms." Journal of Cybersecurity, November, tyv011.

[62] Peirce, C. S. (1992 [1867-1893]) 'Deduction, induction and hypothesis' in N. Houser and C. J. W. Kloesel (eds.) The Essential Peirce, selected philosophical writings, Vol. 1. Indiana University Press, Bloomington and Indianapolis .

[63] Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability challenges in the cybersecurity information sharing ecosystem. Computers, 9(1), 18.

[64] EESC 2018. Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks, Available from https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/cybersecurity-ensuring-awareness-and-resilience-private-sector-across-europe-face-mounting-cyber-risks-study

[65] Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A cyber incident response and recovery framework to support operators of industrial control systems. International Journal of Critical Infrastructure Protection, 37, 100505.

[66] CEPS (2018) Software Vulnerability Disclosure in Europe, https://cdn.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf

[67] Khan, R. A., Khan, S. U., Khan, H. U., & Ilyas, M. (2022). Systematic literature review on security risks and its practices in secure software development. IEEE Access, 10, 5456-5481.

[68] DCMS (2018b) Code of Practice for Consumer IoT Security, Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

[69] Onwudiwe, M. and Newton, K., 2021. Africa and the Artemis Accords: A Review of Space Regulations and Strategy for African Capacity Building in the New Space Economy. New Space, 9(1), pp.38-48.

[70] Harknett, Richard J., and James A Stever. 2009. "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen." Journal of Homeland Security and Emergency Management 6 (1).

[71] Farrell, M., Bradbury, M., Cardoso, R. C., Fisher, M., Dennis, Louise A., Dixon, C., Sheik, A.T., Yuan, H., and Maple, C. 2023. Security-Minded Verification of Cooperative Awareness Messages. *IEEE Transactions on Dependable and Secure Computing*, December 2023.

[72] Peirce, C. S. (1992 [1867-1893]) 'Deduction, induction and hypothesis' in N. Houser and C. J. W. Kloesel (eds.) The Essential Peirce, selected philosophical writings, Vol. 1. Indiana University Press, Bloomington and Indianapolis .

[73] National Institute of Standards and Technology (2020), Security and Privacy Controls for Information Systems and Organizations, Special Publication (SP) 800-53 Rev 5. Available from: https://doi.org/10.6028/NIST.SP.800-53r5

## APPENDIX - INTERVIEWS' QUESTIONS GUIDE

### 1) General

- What is your role within your organisation and how long have you been in this role?
- What does your organisation do?
- What kind of space-related activities and products/services does your organisation provide? (for commercial organisations)
- What kind of space-related activities and strategic objectives does your organisation pursue? (for NGO/Governmental organisations)

### 2) Perception of change

General change

- What does the expression 'NewSpace' mean to you?

Business change

- What is the business opportunity that NewSpace represents for your company? (for commercial organisations)

Cybersecurity change

- Are you aware of any recent report of attacks on space systems in the news, anything that has caught your attention?

### 3) Global character of the space industry

Global orbits and uplinks and downlinks stations

- Do you operate a ground station which communicates with satellites? (for commercial organisations)
- What is the impact of sharing a ground station with other organisations in terms of security?
- Would it be an issue if the organisation that owns the ground station collected data you sent to and received from satellites? (for commercial organisations)

Global supply chain (for commercial organisations)

- Is your supply chain global? Are there any threats resulting from the global aspect of supply chain?
- Do you use commercial off the shelf (COTS)components? Do you know the country of origin of the components?

### 4) Space market (for commercial organisations)

- Do you have a dedicated budget for cybersecurity?
- Are your customers willing to pay for more for products where cybersecurity is a main feature?

### 5) Technology change

Dual-use technologies

- Is there any measure in place to minimise the risk posed by dual use technologies?
- What do you think could be the most dangerous technology to disrupt (your) space system service that one could cheaply purchase online?

### 6) Regulation

Regulation in practice

- Are there specific cybersecurity standards that your organisation follows? (for commercial organisations)
- Have you proposed/worked/contributed towards any cybersecurity standards? (for NGO/Governmental organisations)
- Does implementing cyber security in space systems differs from other sectors? E.g. automotive or IT technology?

Perception of regulation

- Would you welcome if the government or another regulatory body published 'secure by design' recommendations for the space industry? (for commercial organisatins)

Perception of regulation practice – what the others are doing

- What do you think space startups are doing to follow cybersecurity standards? (for large organisations)
- What do you think large and established space organisations do to follow cybersecurity standards? (for small organisations)

### 7) A heterogeneous culture of cybersecurity

- Do you think everyone should share vulnerabilities?
- Should there be a global way of thinking when it comes to cybersecurity or is there anything to gain from non-Western approaches to cybersecurity?

### 8) Organisation of workforce

- Do you believe there are sufficient employees or candidate employees with relevant skills to tackle cybersecurity of space systems?

### 9) Critical National Infrastructure

- What kinds of non-critical and critical services do you think depend on NewSpace systems?
- What threats do you think that these systems might be vulnerable to?

## BIOGRAPHY

***Sara Cannizzaro*** *obtained her PhD in biosemiotics from London Metropolitan University. She is currently a post-doctoral researcher at the University of Sheffield on the 'Public Voices in Artificial Intelligence' project as part of the ESRC-funded Digital Good Network. She has been a researcher on several externally-funded projects spanning responsible innovation, ethics of emerging technology, digital media platforms, cybersecurity and technology adoption projects, including: FAIR (Future Artificial Intelligence Research) Alma Mater Studiorum Università di Bologna, Italy; TECHETHOS (Ethics of new and emerging technologies with high socio-economic impact), de Montfort University, UK; EUMEPLAT (European Media Platforms), IULM University, Italy; PETRAS (Privacy, Ethics, Trust, Reliability and Adoption of the Internet of Things) and FAIRSPACE (Future AI and Robotics for Space), University of Warwick, UK.*

***Matthew Bradbury*** *is a Senior Lecturer in Cyber Security at Lancaster University. His research interests are on the security, privacy and trust of resource-constrained and distributed systems. This work has involved a range of domains including IoT, automotive and space-based systems. Current research projects focus on reducing the information revealed by cyber physical systems and providing better guarantees for the security of ultra-large scale systems.*

***Sam Maesschalck*** *received his MSc and PhD degrees in Cyber Security and computer science, respectively, from Lancaster University. He is currently a Senior Security Engineer at Nexova Group where he is responsible for the development and delivery of cyber security training for the European Space Agency's new Cybersecurity Centre of Excellence. Aside from his full-time role he is also a researcher in the School of Computing and Communications at Lancaster University. His main research area is the cyber security of critical infrastructure with a focus on operational technology and cyber deception.*

***Gregory Epiphaniou*** *is Reader in Security Engineering at the University of Warwick with over 20 years of experience in Information Security. He manages a team of 6 PhD students, 7 Research Fellows, and 3 Assistant Professors in the Cyber Security Centre. His research focuses on threat source characterisation, proactive cyber defense, and principles of physical layer security. He has led projects funded by EPSRC (RESICAV, BEARCAT, S-CAV), IUK (Cydon, VACCYNE), and local authorities, totalling over £\pounds 20M. Dr. Epiphaniou is the inventor of a patent in distributed ledger systems and has authored a book and several articles on DLT technologies. He is an associate editor for ACM DLT and a regional editor for Springer Nature Discover IoT journals. He has collaborated with the UK MoD, holds numerous industry certifications (CISSP, CEH, CISM), and has over 100 international publications. He is also a subject matter expert at the Chartered Institute for Securities and Investments and acted as a key member for developing WS5 in the formation of the UK Cybersecurity Council.*

***Carsten Maple*** *is Professor of Cyber Systems Engineering at the University of Warwick where he is the Principal Investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research. He is also a Professor and Fellow of the Alan Turing Institute, the National Institute for Data Science and AI in the UK, where he is a principal investigator on a $9 million project developing trustworthy digital infrastructure and co-investigator on the £13M Framework for Responsible AI in Finance project. Carsten is a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity and the Research Innovation Director at EDGE-AI, the National Edge Artificial Intelligence Hub. Carsten has published over 450 peer-reviewed papers and contributed to the development of a number of standards and guidelines for the Space Sector, working with the ESA, IEEE, NASA/JPL, Space ISAC and others. He has given evidence to government committees on a variety of issues concerning safety, security, privacy and identity and acted as an international expert for various agencies.*