Integrating Ethical, Legal, and Technological Safeguards in Space-Focused Cyberbiosecurity: AI, Cloud, and Crew Considerations

Dominique Dove[1], Kenneth Chamberland[2], Sotirios Karathanasis[3] Lucas Potter[4] and Xavier-Lewis Palmer[4]

[1]The George Washington Law School, Washington, D.C., USA
[2]Capella University, Minneapolis, Minnesota, USA
[3]Independent Researcher
[4]BiosView Labs, Dayton, Ohio, USA

dominique.dove.esq@gmail.com
ken.chamberland@gmail.com
sfk@use.startmail.com
biosview1@proton.me

Abstract: Long-duration crewed missions and orbiting habitats such as the International Space Station (ISS) present unique intersections of biological and cybersecurity risks. Cyberbiosecurity, a hybrid field that combines biosecurity and cybersecurity in the investigation of system vulnerabilities, is being addressed across multiple domains of Earth but remains underexplored in space environments. The closed-loop life-support, modular robotics, and telemetric control systems aboard space stations create novel attack surfaces, while microgravity and radiation alter microbial behavior in ways that could exacerbate bio-contamination risks. Additionally, the use of artificial intelligence (AI) for equipment health monitoring, autonomous robotics, and crew support introduces new vulnerabilities, as adversarial inputs or model poisoning could compromise critical diagnostics and decision-making aids. Cloud-based infrastructures used for off-board data storage, analytics, and command relay further expand the threat surface, requiring rigorous cloud security, encryption, and isolation protocols to prevent unauthorized access or data exfiltration. This paper explores potential attack vectors in both cyber- and bio-informed arenas across launch, transit, and orbital habitats, and proposes forward-looking countermeasures for these proposed attacks. We outline a framework that incorporates ethical and legal considerations, including crew privacy rights and compliance with international space treaties and biosafety regulations. By combining AI-robust design principles, secure cloud architectures, and clear legal guidelines, our approach aims to present ideas to safeguard space-based biological operations, uphold crew well-being, and ensure mission resilience against emerging cyberbiological threats.

Keywords: Space, Space station, Cyberbiosecurity, Biocybersecurity

1. Introduction

Human presence in space (from government ventures) to emerging commercial habitats depends on the tight integration of life-support, command-and-data handling, robotics, and biomedical research modules (Everroad et al, 2024). Space-station systems are highly interdependent and are projected to become more intertwined: novel proposed systems include encrypted telemetry of experimental samples with specialized hardware, remote maintenance using robotic arms, and crew health parameters fed through environmental controls (Putz, 1999; Fink et al, 2014; Mora et al, 2016; Khodadad et al, 2021; Overbey et al, 2024). While these systems face significant implementation challenges, the evaluation of their security is underdiscussed in the literature. Conventional cyber threats could disrupt environmental or command systems, and biological risks may be expedited by an attacker maliciously manipulating life-support protocols (Skopik et al, 2012; Elgabry, 2023; Sreejalekshmi, 2024; Khan et al, 2024; Oh et al, 2025). For instance, a fungal bloom caused by airflow stagnation on a hypothetical mission in space could allow *Cladosporium* to accumulate near avionics panels, and if an attacker alters filter replacement schedules via a compromised digital or cyber-physical interface, both crew health and critical systems could be jeopardized.

This interface between biosecurity and cybersecurity has been extensively discussed, but their use is over-represented in terrestrial environments since 2018 and under-discussed in the context of space (Elgabry and Johnson, 2024; Potter & Palmer, 2023). Considerable amounts of literature treat space cybersecurity and biological control separately, and incident reports (e.g., software resets, environmental-control failures) may find themselves operating with an insufficiently unified vulnerability assessment. This work bridges that gap by exploring cyberbiosecurity in a representative space habitat environment and proposes practical mitigations and policy recommendations. We conclude with directions for future research and operational practice. This work is by no means fully inclusive, but it aims to offer a conversation starter; we cannot assume that these matters are not already being discussed, after all. Simplified versions of terms will be used to increase

accessibility among our audience, which we expect to be diverse among those in aerospace, biology, and cybersecurity. This position paper emphasizes both the practice and law of biocybersecurity relevant to the theater of space, and provides appropriate practical preparation as well as proposed legal frameworks to guide the development of this exciting, nascent field.

2. Space-Station Biocybersecurity: The Architecture and Vulnerabilities of an Integrated Cyber-Biologic Threat Landscape

The central feature of cyberbiosecurity is that biological assets are used as intermediaries or targets in attacks that involve computerized systems (Murch et al., 2018; Elgabry & Johnson, 2024; Potter & Palmer, 2023). Space stations are an excellent example of high-risk, high-value cyberbiosecurity targets: they are significantly automated, long-duration human biological habitats used in the hostile environment of space and are fundamentally cyberbiological. One essential space habitat feature that exemplifies this cyberbiological nature is the Environmental Control and Life Support System (ECLSS) (Traweek & Tatara, 1998; Berger, 2008; Sorokin & Markov, 2008; Messerschmid & Bertrand, 2013). The ECLSS is the combined on-board hardware, software, and biochemical support system used to simulate Earth's natural, regenerative life-sustaining resource supply - it predominantly recycles water via waste reclamation and filtering and revitalizes air using flow through filtration chambers and oxygen generation by electrolysis (Cowan et al, 2022). However, the elegance of the ECLSS belies its risk as a high-value target: it is an essential automated biophysical network where any lapse in security can be exploited by attackers. For example, an ECLSS operating on legacy *command and data handling (CDH)* protocols, using firmware updates that do not have a verifiable origin and without encryption, may prove deadly for the crew: sophisticated air and water control systems could be modified or halted outright, and astronauts could be held hostage for ransom payment or political motives (Asaju et al, 2024; Hazra et al, 2024; Ivey, 2024; Badke et al, 2025). Even miscommunication of resource status, biomass, waste, atmosphere stabilization, or improper utilization could be disastrous, as significant planning and coordination is required to maintain closed-loop regeneration onboard a space habitat (Caraccio et al, 2014). An attacker may seek to exploit insufficiently protected CDH protocols while disguised as an approved user, either by repeating prior commands at an inappropriate time (replay attack) or inputting their own malicious commands (uplink spoofing) (Torabi et al, 2021; Lai et al, 2022; Martínez et al, 2023). Limited time to fix software errors, especially for space missions far from Earth, and stringent reliability requirements further magnify these risks, as solutions can be delayed despite immediate mission-critical needs.

Consequences of an attack may not be immediately obvious: over days, closed-loop habitats can dramatically expedite genetic drift and small-scale evolution. If not closely monitored, microbial genetic selection pressure may increase virulence, favor one species over another, and increase biofilm formation (Nnaji et al., 2024; Osta-Ustarroz et al., 2024; Onofri et al., 2025). This has implications for automated water-processing filters on space stations; scheduled biocidal treatments, necessary for regular filter cleaning, can be targeted in an attack to delay or cease function. This would allow many known contaminant microbes aboard space biohabitats to multiply out of control, as many form biofilms that increase their virulence and decrease their vulnerability to conventional biocidal products (Vance et al., 2022; Justiniano et al., 2024; Beitle et al., 2024; Herrera-Jordan et al., 2024). Similarly, maliciously reprogrammed automated microbial monitoring systems could suppress contamination alerts, promote resistant strains of microbes, or skew biomass estimates, delaying crew interventions until risks become unmanageable. For example, human immune system dysregulation is a well-known consequence of space travel (Lv et al, 2023). Fecal-oral transmission of endemic diseases can spread rapidly among crew if filtration of reclaimed wastewater is tampered with, and an entire crew affected by a diarrheal disease when potable water is scarce could prove lethal (as was common among terrestrial expeditions in the past) (Barrila et al, 2021). The same goes for any undetected upper respiratory infections in a crew member, whether already on a team or joining a space station from Earth: tampered air filtration could render quarantining ineffective, and the aforementioned immune weakening could put astronauts at increased risk of life-threatening pneumonia (Mermel, 2013). Reprogrammed robotic manipulators in astrobiology experiments may mishandle containment units, releasing engineered or opportunistic microbes into the habitat's air or water systems. Unauthorized access to sequencing devices further enables exfiltration and tampering with genomic data, masking emerging infections, or facilitating the engineering of novel biothreats. Another attack vector exists along maintenance of microbial populations essential for broader life support function: altering micro-environmental controls may so dramatically disrupt microbial ecology that populations become unstable and ultimately collapse, leaving a broken link in the ECLSS recycling chain. In addition to crew safety, mission success is at risk, as numerous experiments could be

compromised: an attacker intercepting encrypted sensor data could spoof readings, altering experimental results in a way that may not be detected until after the mission is over.

Emerging commercial habitats may create new security issues if they use third-party payload racks and specialized interfaces without proper interoperability, governance, and security. Vulnerabilities may emerge from undiscovered flaws in programming that are found by malicious actors; the mix of connected, disparate electronic and biocentric hardware presents unique risks, especially within microgravity. This includes personal devices like smart inhalers and glucose monitors, especially if they connect to station systems. The supply chain poses risks, as well: third-party hardware or firmware may hide dangerous payloads that could activate once in orbit. For example, insiders might change microbial monitoring schedules or system settings to conceal a biothreat or cause system malfunction (Zafar et al, 2021; Panunzio et al, 2021; Nahar et al, 2022; Pietraru et al, 2023; Seiden et al, 2023). Each part of the network can be a potential entry point for attacks (Babajide et al, 2025; Babcinschi, 2025; Saroka et al, 2025). Together, these cyber and biological threats form a deeply intertwined attack landscape that demands unified, layered defenses combining cryptographic hardening, network segmentation, anomaly detection, supply-chain attestation, and bio-containment protocols to protect both the digital and biological integrity of space habitats.

3. Cloud Infrastructure in Space Habitats: Threat Surfaces and Resilience

Cloud computing enables remote analytics, telemetry processing, and data sharing across sensors and servers (Aderinto, 2025; Kua et al., 2021; Wang et al., 2025). In space habitats, onboard computers can collect and perform lightweight preprocessing on critical data, then transmit to Earth-based cloud platforms for more intensive computations. Insights gleaned from the terrestrial processing can then be sent back to the space habitat for interpretation. Yet all transmissions hold the potential for man-in-the-middle attacks, sensor spoofing, data exfiltration, and artificial intelligence (AI) model poisoning (Ahmed & Kashmoola, 2021; Bajcsy et al, 2025; Korada, 2024).

For instance, adversarial interference in microbial sensor data could suppress contamination alerts, delaying mitigation (Usynin et al, 2025). Cloud-based environmental monitoring algorithms utilizing compromised inputs can place crew safety at risk. In the current commercial cloud infrastructure environment, this risk is compounded due to the sharing of computational resources among several independent users, a cost-saving measure known as “multitenancy.” Multitenancy becomes a risk when sensitive mission data is stored and processed on servers also used by independent (and possibly malicious) users. Sophisticated attackers could erode barriers within virtualized tasks, expose data that may lead to inferring mission operations, extract restricted data, or sabotage hardware operation by feeding automated controls incorrect information for their function (Javeed et al, 2023; Lou et al, 2024). Of course, the collection and processing of health-related information in cloud systems raises legal and ethical challenges related to patient privacy, data sovereignty, and regulatory compliance (Chakilam et al, 2025; Shafik et al, 2025).

To mitigate the risks associated with terrestrial cloud integration in space operations, encouraging continuous authentication is essential, ensuring that every interaction, from onboard subsystem communication to remote mission controller contact, undergoes permission validation, encryption, and authorization. By incorporating federated learning, model training can be distributed across platforms without centralizing sensitive data, preserving the confidentiality of crew health, genomic, and environmental telemetry while reducing transmission exposure. Audit trails that cannot be altered, supported by systems based on distributed, but cryptographically linked, data structures used to record events (such as those seen in blockchain-based ledgers) can further strengthen accountability. This can provide tamper-evident tracking of system access and configuration changes; the choice of blockchain ledger would need to be developed with space-based stakeholders in mind. Next, quantum computing has potential to undermine existing encryption standards; the adoption of cryptographic algorithms that are quantum-resilient must become standard for all mission-critical communications. Accompanying this concern is the fact that most cloud infrastructure is physically located on Earth. Both jurisdictional and geopolitical concerns in terms of data sovereignty and state-sponsored interference present additional challenges for the deployment of the technology mentioned here. Further, mismanagement of privilege escalation during mission transitions, where users retain unnecessary access across cloud environments, can exacerbate vulnerabilities. Despite these risks, cloud computing remains invaluable for its scalability, redundancy, and ability to alleviate onboard processing demands. Its secure implementation depends on dynamic access management, real-time auditing, and adherence to stringent, jurisdiction-aware governance frameworks that balance operational agility with uncompromising biocybersecurity.

4. Countermeasures and Resilience Strategies

Having discussed how an attacker might exploit space habitat systems, it is worthwhile to turn our attention to methods of preventing such an intrusion. First, communications channels must be secured: data transmission to and from the spacecraft must be cryptographically hardened to prevent snooping by unauthorized parties or timing delays, as either opens the space crew to harm by way of malfunctioning equipment. Additionally, firmware images must carry digital signatures that are verified by hardware-rooted, ID-based, system-specific bootloaders. Critical on-board networks must be sandboxed with firewalls, so that life-support and bio-monitoring systems are isolated from payload and crew internet; this reduces the ability for attackers to gain unprivileged access to sensitive systems. To this end, biological analysis platforms (whether scientific or clinical) should operate using only necessary network connectivity, and any removable storage should undergo fingerprinting that checks against corruption before analysis. Any introduction of third-party modules needs clear, consistent digital watermarking and hardware attestation, with an immutable ledger of component provenance and firmware hashes that tracks all physical and digital components allowed to join any (isolated) network. Following good security practice includes that physical and digital third-party components are not installed or enabled without a clear rationale and appropriate permissions.

Besides securing and isolating avenues for an attack, an addition security can be provided by active surveillance of networks: lightweight machine-learning monitors (or even simple activity thresholds) can establish baseline telemetry patterns for ECLSS, robotics, and bio-sampling subsystems, flagging deviations that suggest sensor spoofing or schedule manipulation. Insider-threat management relies on multi-person authorization for critical commands, such as filter-change scheduling and tamper-evident audit logs, which can only be accessed by independent safety officers.

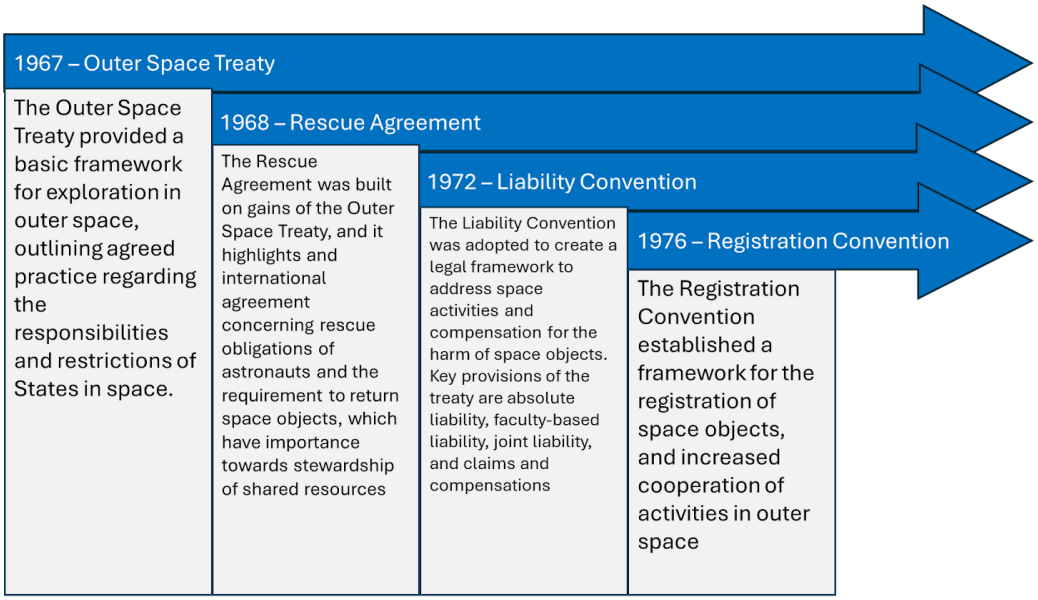
In the event of a breach or intrusion, one last line of defense is preparing a crew to operate a space habitat under a compromised network. For example, subsystem redundancy and manual override capabilities, such as mechanical valve bypasses for life support, ensure that the crew can maintain essential functions without network connectivity.

5. Limitations

A thorough discussion of cyberbiological threat assessment and preparation is incomplete without acknowledging the limitations of our analysis. Several factors constrain our understanding of spaceflight cyberbiological risks: first is data availability. Both private and public space programs restrict access to their data under proprietary agreements or classified status. This makes open analysis of cyberphysical system architecture, incident investigations, and even interoperability queries difficult. The rapid pace of system evolution through hardware upgrades, software patches, and architectural overhauls also means that any known vulnerability solution can become outdated within months.

6. Ethical and Legal Implications

Space activities are expected to grow tremendously within the next few years: this is bolstered by both the emergence of new cost-effective satellite systems and the incorporation of automated systems control (Gal et al, 2020). The use of automated systems in space highlights a series of important ethical considerations, considering the shift from “computer-assisted human choice and human-ratified computer choice” to non-human analysis, decision, and action selection (Gal et al, 2020). We previously described the physical and ethical risks of automated system control in space, recommending scrutiny of all deployed systems, and highlighted the rapid and varying development timelines such automated systems possess. An advanced legal framework is recommended to match with the emerging developments of AI. (Soroka & Kurkova, 2019). Space law, the branch of law that governs the activities and technologies relating to space, can be used to establish this framework; in particular, multiple international laws were put forth from 1967 to 1979 to guide conduct in space, including The Outer Space Treaty of 1967, The Rescue Agreement of 1968, The Liability Convention of 1972, The Registration Convention of 1976, and the Moon Agreement of 1976 (Dempsey, 2015; Pagallo, Bassi, & Durante, 2023). Four treaties are noteworthy and are highlighted in this paper. The agreements mentioned within Figure 1 were significant in developing not only the responsibilities of States' obligations regarding astronauts but also in addressing the complexities of space tourism (Dempsey, 2015).



(Dempsey, 2015; Pagallo et al, 2023)

Figure 1: A Primer on Space Law

The increasing use of purely autonomous AI systems to analyze and make decisions in space is controversial. Additionally, there are several issues concerning AI in space which includes fault liability, due diligence, and several other legal standards and should all be revisited (Lyall & Larsen, 2017; Pagallo et al, 2023). However, most state parties have developed their own regulatory frameworks regarding space-related activities. However, two issues arise from allowing States to regulate themselves. First, there is no coordination nor autonomy in the development of the legal framework. Second, there will be varying levels of accountability for private organizations based on where they are incorporated. Therefore, the law should reinforce strict liability regulations with an extension of current tortious liability to "tackle compensation gaps in accidents" caused by AI. Furthermore, the unique challenge of outer space lends the recommendation of the adoption of specific standards, e.g. standards implemented for every space mission (Pagallo et al, 2023).

6.1 Suggested Legal Framework

The suggested legal framework for AI in space, in Figure 2, mirrors the framework established by NASA. Any AI developed for space should be fair, explainable and transparent, accountable, secure and safe, human-centric and societally beneficial, and scientifically and technically robust. Our focus, for this paper, is the accountable aspect of the framework. (McLarney et. al. 2021). AI deployment in space systems needs clear attribution of fault, paired with scrutiny of design and deployment; legal framework selection benefits stakeholders when weighted heavily towards the impact of the developed and deployed system (Walia, 2024). Organizations should be legally required to: respect intellectual property rules; develop AI systems that have a documented framework; develop monitoring systems and report their findings; and register the AI system with applicable space agencies. Helpful areas of development that can strongly serve humanity as we step boldly into the stars include (1) advocating for policy changes that declassify non-critical incident data and mandate standardized reporting frameworks, (2) developing open-source terrestrial testbeds that replicate station subsystems to enable public security research, (3) convening interdisciplinary working groups of cybersecurity specialists, biologists, and aerospace experts to co-develop integrated guidelines, and (4) implementing adaptive monitoring regimes that continuously update risk assessments in step with system upgrades (Murch et al, 2018; Guise et al, 2023; Zimmerman et al, 2025).

IP and Health Rule Compliance	Ensure all deployed AI systems and data usage comply with applicable Health and IP laws.
Documented Framework Development	Parties should create and maintain formal records outlining AI system goals, risks, and safeguards. Risks to life should be emphasized.
Monitoring & Reporting	Parties should implement for continuous evaluation and the means to submit findings to applicable regulatory authorities.
AI Registration with Applicable Space Agencies	AI systems deployed in or for space missions should be registered, and this should be mandated.
Continuous Policy Evolution	Periodically revise legal and technical frameworks as AI technology and their reach into life outcomes for life aboard spacecraft advances.

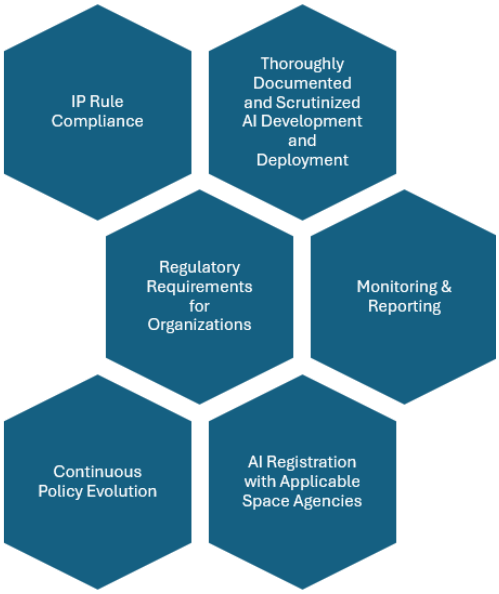


Figure 2: Suggested Framework

7. Conclusion

We have outlined several cyberbiological attack vectors, from remote tampering of on-board environmental monitors to unauthorized critical systems access via Earth-linked cloud computing infrastructure. To counter these threats, we proposed a suite of multilayered controls tailored for spaceflight: cryptographic hardening of communication, network, and biological segmentation to isolate critical networks, active surveillance of telemetry data, and a legal framework to ensure proper development and utilization. Despite significant gaps in understanding arising from government security, vendor non-disclosure restrictions, and the rapid evolution of station configurations, advancing space cyberbiosecurity will demand coordinated efforts. As humanity ventures beyond low-Earth orbit to lunar bases, Mars transit habitats, and eventually to deep space exploration, embedding robust cyberbiosecurity measures from the design phase will be essential to safeguarding crew health, ensuring mission success, and recruiting confidence towards building the exhilarating future of humans exploring beyond Earth. The pathway to that secure future begins today.

Ethics declaration: Not Applicable.

AI declaration: AI was not used in the final product of this paper. Use was limited to organization of initial drafts.

References

Aderinto, A.B., 2025. Next generation cloud and edge computing architectures for Real-Time Space Data Processing and Analytics. World Journal of Advanced Research and Reviews, 25(3), pp.152-170.

Ahmadi, S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports, 26(2), 215–228.

Ahmed, I.M. and Kashmoola, M.Y., 2021, August. Threats on machine learning technique by data poisoning attack: A survey. In International Conference on Advances in Cyber Security (pp. 586-600). Singapore: Springer Singapore.

Asaju, B.J., Wakili, A.A. and Jung, W., 2024. Cybersecurity for Internet of Medical Vehicles (IOMV): Stopping Attacks and Protecting Data Infrastructures. Available at SSRN 5263471.

Babajide, A., Wakili, A., Barnett, M., Potter, L., Palmer, X.L. and Jung, W., 2025. Safeguarding Smart Inhaler Devices and Patient Privacy in Respiratory Health Monitoring. arXiv preprint arXiv:2504.03730.

Babcinschi, M., 2025. Interoperable and integrated robot based cyber physical production systems (Doctoral dissertation, Universidade de Coimbra).

Bajcsy, Peter, Antonio Cardone, Philippe Dessauw, Michael Majurski, Derek Juba, Timothy Blattner, and Walid Keyrouz. "Explaining poisoned AI models." In Bi-directionality in Human-AI Collaborative Systems, pp. 55-73. Academic Press, 2025.

Barrila, J., Sarker, S.F., Hansmeier, N., Yang, S., Buss, K., Briones, N., Park, J., Davis, R.R., Forsyth, R.J., Ott, C.M. and Sato, K., 2021. Evaluating the effect of spaceflight on the host–pathogen interaction between human intestinal epithelial cells and Salmonella Typhimurium. npj Microgravity, 7(1), p.9.

Beitle, E., Kemp, A. and Justiniano, Y.A.V., 2024, December. Biofilm Mitigation in Spaceflight Utilizing Phytoremediation. In American Society for Gravitational and Space Research 2024 Conference.

Bhadke, S., Suryawanshi, S., Parate, P., Tirpude, S. and Nanwatkar, A., 2025. IOT Based On Building the Future: Designing the Consistent Space Stations & Moon Colony/Mars Colony. International Journal on Advanced Computer Theory and Engineering, 14(1), pp.289-295.

Caraccio, A., Poulet, L., Hintze, P.E. and Miles, J.D., 2014. Investigation of bio-regenerative life support and trash-to-gas experiment on a 4-month Mars simulation mission (No. KSC-E-DAA-TN17765).

Chakilam, C., Kannan, S., Recharla, M., Suura, S.R. and Nuka, S.T., 2025. The impact of big data and cloud computing on genetic testing and reproductive health management. American Journal of Psychiatric Rehabilitation, 28(1), pp.62-72.

Cope, H., Willis, C. R., MacKay, M. J., Rutter, L. A., Toh, L. S., Williams, P. M., Herranz, R., Borg, J., Bezdan, D., Giacomello, S., & Muratani, M. (2022). Routine omics collection is a golden opportunity for European human research in space and analog environments. Patterns, 3(10), 100550.

Cornejo, J., Vargas, M., Rivera, M.V., Palomares, R., Barreto, R. and Cornejo, J., 2024, November. Space Life Support Engineering and Biomechatronics Towards the Moon and Mars: A Scoping Review. In 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-6). IEEE.

Cowan, D.T., Broyan, J.L., Williams, D.E., Abney, M.B., Perry, J.L., Melendez, O., Delzeit, L.D. and Meyer, M.E., 2022, July. A Guide for Evaluating Spacecraft Environmental Control & Life Support Systems (ECLSS) Technology Developments. In 51st International Conference on Environmental Systems (No. ICES-2022-71).

Dempsey, P.S., 2015. The emergence of national space law. *Available at SSRN 2692639*.

Elgabry, M., 2023. Towards cyber-biosecurity by design: An experimental approach to Internet-of-Medical-Things design and development. Crime Science, 12(1), pp.1-5.

Elgabry, M., & Johnson, S. (2024). Cyber-biological convergence: A systematic review and future outlook. Frontiers in Bioengineering and Biotechnology, 12, 1456354.

Everroad, R.C., Foster, J.S., Galazka, J.M., Jansson, J.K., Lee, J.A., Lera, M.P., Perera, I.Y., Ricco, A.J., Szewczyk, N.J., Todd, P.W. and Zhang, Y., 2024. Strategies, Research Priorities, and Challenges for the Exploration of Space Beyond Low Earth Orbit. Gravitational and Space Research, 12(1), pp.18-40.

Fink, W., Popov, A. and Hess, A., 2014, March. Planning a pilot project on the ISS for crew health management & maintenance beyond LEO. In 2014 IEEE Aerospace Conference (pp. 1-9). IEEE.

Gal, G.A., Santos, C., Rapp, L., Markovich, R. and van der Torre, L., 2020. Artificial intelligence in space. arXiv preprint arXiv:2006.12362.

Guise, N., Pattie, D., Yeh, K.B., Talley, K. and Fezzie, R.F., 2024. 2023 cyberbiosecurity summit underscores challenges associated with cybersecurity and the rapidly growing bioeconomy. Global Security: Health, Science and Policy, 9(1), p.2401164.

Hazra, R., Chatterjee, P., Singh, Y., Podder, G. and Das, T., 2024. Data encryption and secure communication protocols. In Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning (pp. 546-570). IGI Global.

Herrera-Jordan, K., Pennington, P. and Zea, L., 2024. Reduced Pseudomonas aeruginosa cell size observed on planktonic cultures grown in the international space station. Microorganisms, 12(2), p.393.

Ivey, D.B., 2024. Environmental Control and Life Support Systems: Review, Concept, Design, Build, Test of a Carbon Dioxide Removal Testbed to Investigate Degradation and Maintenance in Space Habitats. University of California, Davis.

Javeed, A., Yilmaz, C. and Savas, E., 2023. Microarchitectural side-channel threats, weaknesses and mitigations: a systematic mapping study. IEEE Access, 11, pp.48945-48976.

Justiniano, Y.A.V., Ledford, M.E., Castro-Wallace, S.L., Nguyen, H.N., Li, W., Irwin, T. and Sysoeva, T.A., 2024, July. More than a decade of international space station microbial sampling in the environmental control and life support systems. In 53rd International Conference on Environmental Systems.

Khan, S.K., Shiwakoti, N., Diro, A., Molla, A., Gondal, I. and Warren, M., 2024. Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions. International Journal of Critical Infrastructure Protection, 47, p.100724.

Khodadad, C.L., Oubre, C.M., Castro, V.A., Flint, S.M., Roman, M.C., Ott, C.M., Spern, C.J., Hummerick, M.E., Maldonado Vazquez, G.J., Birmele, M.N. and Whitlock, Q., 2021. A microbial monitoring system demonstrated on the International Space Station provides a successful platform for detection of targeted microorganisms. Life, 11(6), p.492.

Korada, L., 2024. Data Poisoning-What Is It and How It Is Being Addressed by the Leading Gen AI Providers. European Journal of Advances in Engineering and Technology, 11(5), pp.105-109.

Kua, J., Loke, S.W., Arora, C., Fernando, N. and Ranaweera, C., 2021. Internet of things in space: A review of opportunities and challenges from satellite-aided computing to digitally-enhanced space living. Sensors, 21(23), p.8117.

Lai, Z., Liu, W., Wu, Q., Li, H., Xu, J. and Wu, J., 2022, May. SpaceRTC: Unleashing the low-latency potential of mega-constellations for real-time communications. In IEEE INFOCOM 2022-IEEE Conference on Computer Communications (pp. 1339-1348). IEEE.

Lou, X., Chen, K., Xu, G., Qiu, H., Guo, S. and Zhang, T., 2024, June. Protecting Confidential Virtual Machines from Hardware Performance Counter Side Channels. In 2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 195-208). IEEE.

Lv, H., Yang, H., Jiang, C., Shi, J., Chen, R.A., Huang, Q. and Shao, D., 2023. Microgravity and immune cells. Journal of the Royal Society Interface, 20(199), p.20220869.

Lyall, F., & Larsen, P. B. (2017). Space Law: A Treatise. Routledge

Martin, A.S., 2022. Human-Robotic Cooperative Space Exploration. In Oxford Research Encyclopedia of Planetary Science.

Martínez, G., Hernández, J.A., Reviriego, P. and Reinheimer, P., 2023. Round trip time (rtt) delay in the internet: Analysis and trends. IEEE Network, 38(2), pp.280-285.

Messerschmid, E. and Bertrand, R., 2013. Space stations: systems and utilization. Springer Science & Business Media.

McLarney, E., Gawdiak, Y., Oza, N., Mattmann, C., Garcia, M., Maskey, M., Tashakkor, S., Meza, D., Sprague, J., Hestnes, P. and Wolfe, P., 2021. NASA framework for the ethical use of artificial intelligence (AI).

Mermel, L.A., 2013. Infection prevention and control during prolonged human space travel. *Clinical infectious diseases*, *56*(1), pp.123-130.

Mora, M., Mahnert, A., Koskinen, K., Pausan, M.R., Oberauner-Wappis, L., Krause, R., Perras, A.K., Gorkiewicz, G., Berg, G. and Moissl-Eichinger, C., 2016. Microorganisms in confined habitats: microbial monitoring and control of intensive care units, operating rooms, cleanrooms and the International Space Station. Frontiers in microbiology, 7, p.1573.

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. Frontiers in Bioengineering and Biotechnology, 6, 39.

Nahar, M., Kamal, A.H.M., Hassan, M.R. and Moni, M.A., 2022. Novel algorithm for multi-time data implantation in a special cyber-manufacturing architecture. Algorithms, 15(10), p.335.

Ney, P., Koscher, K., Organick, L., Ceze, L., & Kohno, T. (2017). Computer security, privacy, and DNA sequencing: Compromising computers with synthesized DNA, privacy leaks, and more. In 26th USENIX Security Symposium (USENIX Security '17) (pp. 765–779). USENIX Association.

Nnaji, N.D., Anyanwu, C.U., Miri, T. and Onyeaka, H., 2024. Mechanisms of heavy metal tolerance in bacteria: A review. Sustainability, 16(24), p.11124.

Oh, I., Sahlabadi, M., Yim, K. and Lee, S., 2025. Threat Classification and Vulnerability Analysis on 5G Firmware Over-the-Air Updates for Mobile and Automotive Platforms. Electronics, 14(10), p.2034.

Onofri, S., Moeller, R., Billi, D., Balsamo, M., Becker, A., Benvenuto, E., Cassaro, A., Catanzaro, I., Cockell, C.S., Desiderio, A. and Ellis, T., 2025. Synthetic biology for space exploration. npj Microgravity, 11(1), p.41.

Osta-Ustarroz, P., Theobald, A.J. and Whitehead, K.A., 2024. Microbial colonization, biofilm formation, and malodour of washing machine surfaces and fabrics and the evolution of detergents in response to consumer demands and environmental concerns. Antibiotics, 13(12), p.1227.

Overbey, E.G., Kim, J., Tierney, B.T., Park, J., Houerbi, N., Lucaci, A.G., Garcia Medina, S., Damle, N., Najjar, D., Grigorev, K. and Afshin, E.E., 2024. The Space Omics and Medical Atlas (SOMA) and international astronaut biobank. Nature, 632(8027), pp.1145-1154.

Pagallo, U., Bassi, E. and Durante, M., 2023. The normative challenges of AI in outer space: law, ethics, and the realignment of terrestrial standards. Philosophy & Technology, 36(2), p.23.

Panunzio, N., Ligresti, G., Losardo, M., Masi, D., Mostaccio, A., Nanni, F., Tartaglia, G. and Marrocco, G., 2021, October. Cyber-tooth: Antennified dental implant for RFID wireless temperature monitoring. In 2021 IEEE International Conference on RFID Technology and Applications (RFID-TA) (pp. 211-214). IEEE.

Pietraru, R.N., Merezeanu, D.M., Ciofu, I. and Persu, C., 2023, November. Cyber-Physical Penile Implant: Necessity or Premature Technological Risk?. In International Conference on e-Health and Bioengineering (pp. 461-470). Cham: Springer Nature Switzerland.

Potter, L., & Palmer, X. L. (2023). Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination. In D. Greenbaum (Ed.), Cyberbiosecurity: A new field to deal with emerging threats (pp. 37–69). Springer International Publishing.

Putz, P., 1999. Space robotics. In Laboratory astrophysics and space research (pp. 547-596). Dordrecht: Springer Netherlands.

Racionero-Garcia, J. and Shaikh, S.A., 2024. Space and cybersecurity: Challenges and opportunities emerging from national strategy narratives. Space Policy, p.101648.

Reed, J. C., & Dunaway, N. (2019). Cyberbiosecurity implications for the laboratory of the future. Frontiers in Bioengineering and Biotechnology, 7, 182.

Rinaldi, A. (2016). Research in space: In search of meaning: Life science research aboard the International Space Station has come under scrutiny for its costs and apparent lack of returns. EMBO Reports, 17(8), 1098–1102.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.

Saroka, A., Ekanayake, A., Kang, J.S., Maceo, C.P. and Sanders, M.H., 2025, March. A standardized solution to command and data handling between modular bus and payload for the future CubeSat missions. In Small Satellites Systems and Services Symposium (4S 2024) (Vol. 13546, pp. 1584-1592). SPIE.

Seiden, S., Baggili, I. and Ali-Gombe, A., 2023, November. I've Got You, Under my skin: biohacking augmentation implant forensics. In International Conference on Digital Forensics and Cyber Crime (pp. 315-332). Cham: Springer Nature Switzerland.

Seylani, A., Galsinh, A. S., Tasoula, A., I, A. R., Camera, A., Calleja-Agius, J., Borg, J., Goel, C., Kim, J., Clark, K. B., & Das, S. (2024). Ethical considerations for the age of non-governmental space exploration. Nature Communications, 15(1), 4774.

Shafik, W., Zakari, R.Y. and Kalinaki, K., 2025. Ethical and Privacy Concerns in Bioinformatics and Cyber-Physical Systems Integration in Healthcare. In AI-Driven Personalized Healthcare Solutions (pp. 333-364). IGI Global Scientific Publishing.

Shen, M., et al. (2020). Blockchain-based secure storage and access scheme for electronic medical records in IPFS. IEEE Access, 8, 59389–59401.

Skopik, F., Ma, Z., Bleier, T. and Grüneis, H., 2012. A survey on threats and vulnerabilities in smart metering infrastructures. International Journal of Smart Grid and Clean Energy, 1(1), pp.22-28.

Sobien, D., Yardimci, M. O., Nguyen, M. B., Mao, W. Y., Fordham, V., Rahman, A., Duncan, S., & Batarseh, F. A. (2023). AI for cyberbiosecurity in water systems. A survey. In D. Greenbaum (Ed.), Cyberbiosecurity: A new field to deal with emerging threats (pp. 217–263). Springer International Publishing.

Skopik, F., Ma, Z., Bleier, T. and Grüneis, H., 2012. A survey on threats and vulnerabilities in smart metering infrastructures. International Journal of Smart Grid and Clean Energy, 1(1), pp.22-28.

Soroka, L. and Kurkova, K., 2019. Artificial intelligence and space technologies: Legal, ethical and technological issues. Advanced Space Law, 3(1), pp.131-139.

Sreejalekshmi, K.G., 2024. Space biosciences: translational research for space, benefitting life on Earth. In Translational Research in Biomedical Sciences: Recent Progress and Future Prospects (pp. 31-43). Singapore: Springer Nature Singapore.

Thirsk, R., Kuipers, A., Mukai, C. and Williams, D., 2009. The space-flight environment: the International Space Station and beyond. Cmaj, 180(12), pp.1216-1220.

Torabi, A., Zarei, J., Razavi-Far, R. and Saif, M., 2021. Decentralized resilient output-feedback control design for networked control systems under denial-of-service. IEEE Systems Journal, 16(4), pp.5620-5629.Traweek, M.S. and Tatara, J.D., 1998. Overview of the environmental control and life support system (ECLSS) testing at MSFC. Life Support & Biosphere Science, 5(1), pp.5-12.

Usynin, D., Ziller, A., Makowski, M., Braren, R., Rueckert, D., Glocker, B., Kaissis, G. and Passerat-Palmbach, J., 2021. Adversarial interference and its mitigations in privacy-preserving collaborative machine learning. Nature Machine Intelligence, 3(9), pp.749-758.

Vance, J., Shaw, A. and Delzeit, L., 2022, July. Engineering polymers as structural materials in spacecraft water systems. In 51st International Conference on Environmental Systems.

Walia, I.K., 2024. Legal Implications of Artificial Intelligence in Outer Space Activities and Explorations. Braz. J. Int'l L., 21, p.193.

Wang, G., Wan, G., Su, Z., Wang, Y., Jia, Y., Li, G. and Liang, S., 2025. High-performance On-orbit Intelligent Computing and Real-time Services for Remote Sensing Satellites Based on Large-scale Computing Power in Space. IEEE Access.

Xu, J., Wang, Y., Chen, X., Wang, L., Zhou, H., Mei, H., Chen, S. and Huang, X., 2024. “Multi-layer” encryption of medical data in DNA for highly-secure storage. Materials Today Bio, 28, p.101221.

Zafar, S., Nazir, M., Bakhshi, T., Khattak, H.A., Khan, S., Bilal, M., Choo, K.K.R., Kwak, K.S. and Sabah, A., 2021. A systematic review of bio-cyber interface technologies and security issues for internet of bio-nano things. IEEE Access, 9, pp.93529-93566.

Zimmerman, E.H., Palmer, X.L., Frow, E., Johnson, A., Hodgson, A., Voight, C. and Elcock III, L.B., 2025. 1.3 Public Infrastructure for Analyzing and Assessing Beyond Biocontainment Biotechnologies.