OPEN ACCESS
International Journal of Applied Research in Social Sciences
P-ISSN: 2706-9176, E-ISSN: 2706-9184
Volume 6, Issue 3, P.No. 254-266-, March 2024
DOI: 10.51594/ijarss.v6i3.854
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/ijarss

CYBERSECURITY ANALYTICS IN PROTECTING SATELLITE TELECOMMUNICATIONS NETWORKS: A CONCEPTUAL DEVELOPMENT OF CURRENT TRENDS, CHALLENGES, AND STRATEGIC RESPONSES

Enyinaya Stefano Okafor[1], Olatunji Akinrinola[2], Favour Oluwadamilare Usman[3], Olukunle Oladipupo Amoo[4], & Nneka Adaobi Ochuba[5]

[1]Independent Researcher, Phoenix Arizona, USA
[2]Independent Researcher, New York, USA
[3]Hult International Business School, USA
[4]Department of Cybersecurity, University of Nebraska, USA
[5]Independent Researcher, UK

Corresponding Author: Enyinaya Stefano Okafor
Corresponding Author Email: stefanenyinna@gmail.com

Article Received: 05-01-24 **Accepted:** 10-02-24 **Published:** 08-03-24

ABSTRACT

Cybersecurity is a critical concern in satellite telecommunications networks, given their vulnerability to cyber threats. This abstract presents a conceptual development of current trends, challenges, and strategic responses in using cybersecurity analytics to protect these networks. The paper discusses the increasing reliance on satellite telecommunications, making them attractive targets for cyber attacks. It explores the role of cybersecurity analytics in detecting and mitigating these threats, highlighting the importance of proactive monitoring and threat intelligence. Challenges in cybersecurity analytics for satellite networks are identified, including the complexity of satellite systems, the limited visibility into network traffic, and the evolving nature of cyber

threats. The paper discusses strategic responses to these challenges, such as the use of advanced analytics techniques, machine learning, and artificial intelligence to enhance threat detection and response capabilities. Key trends in cybersecurity analytics for satellite networks are examined, including the growing adoption of cloud-based security solutions, the rise of insider threats, and the need for collaboration between satellite operators and cybersecurity experts. The paper also discusses the importance of regulatory compliance and the role of industry standards in ensuring the security of satellite networks. In conclusion, the paper emphasizes the importance of cybersecurity analytics in protecting satellite telecommunications networks and recommends a proactive approach to cybersecurity that includes continuous monitoring, threat intelligence sharing, and collaboration with cybersecurity experts.

Keywords: Cybersecurity, Analytics, Satellite, Telecommunications, Conceptual Development.

INTRODUCTION

Cybersecurity is a paramount concern in the satellite telecommunications industry, given the critical role satellites play in global communication networks. Satellite telecommunications networks are susceptible to cyber threats, including data breaches, network intrusions, and denial-of-service attacks, which can disrupt services and compromise sensitive information. In response to these challenges, the industry is increasingly turning to cybersecurity analytics to protect satellite networks from cyber threats (Manulis, et. al., 2021, Tedeschi, Sciancalepore & Di Pietro, 2022, Varadharajan & Suri, 2023).

Cybersecurity analytics involves the use of advanced data analysis techniques to detect, monitor, and respond to cyber threats. By analyzing network traffic, user behavior, and system vulnerabilities, cybersecurity analytics helps identify potential threats and vulnerabilities in satellite networks, allowing for timely and effective mitigation measures (Nassar & Kamal, 2021, Sarker, 2023, Ullah & Babar, 2019).

The purpose of this paper is to discuss the current trends, challenges, and strategic responses in cybersecurity analytics for satellite networks. It will explore the increasing sophistication of cyber threats targeting satellite networks, the adoption of machine learning and artificial intelligence in cybersecurity analytics, and the integration of cloud-based security solutions. Additionally, the paper will highlight the importance of threat intelligence sharing and collaboration among satellite operators and cybersecurity experts in addressing cybersecurity challenges.

Overall, this paper aims to provide insights into the evolving landscape of cybersecurity in satellite telecommunications and to offer recommendations for enhancing cybersecurity practices in satellite networks. By understanding the current trends, challenges, and strategic responses in cybersecurity analytics, satellite operators can better protect their networks from cyber threats and ensure the continued reliability and security of satellite telecommunications services.

History of Cybersecurity Analytics in Satellite Telecommunications

The history of cybersecurity analytics in protecting satellite telecommunications networks is a story of adaptation and innovation in response to evolving cyber threats (Pavur, 2021, Pavur & Martinovic, 2022, Petrenko, 2022). This article provides a conceptual development of the history, current trends, challenges, and strategic responses in cybersecurity analytics for satellite networks. The history of cybersecurity analytics in satellite telecommunications can be traced back to the

early days of satellite communication when security threats were relatively limited. However, as satellite networks became more complex and interconnected with terrestrial networks, the need for cybersecurity analytics became increasingly apparent.

In the early days, cybersecurity measures for satellite networks primarily focused on encryption and authentication protocols to secure data transmission. However, as cyber threats evolved, satellite operators began to adopt more sophisticated cybersecurity analytics techniques to detect and mitigate these threats. One of the key milestones in the history of cybersecurity analytics in satellite telecommunications was the development of intrusion detection systems (IDS) and intrusion prevention systems (IPS) (Manulis, et. al., 2021, Tedeschi, Sciancalepore & Di Pietro, 2022, Wu, et. al., 2023). These systems use advanced analytics techniques to monitor network traffic and detect anomalies that may indicate a potential cyber attack. Another important development was the use of machine learning and artificial intelligence in cybersecurity analytics. These technologies enabled satellite operators to analyze large volumes of data and identify patterns that may indicate a cyber threat.

In recent years, cybersecurity analytics for satellite networks has evolved rapidly to keep pace with the increasing sophistication of cyber threats. One of the key trends is the adoption of cloud-based security solutions, which enable satellite operators to leverage the scalability and flexibility of the cloud to enhance their cybersecurity capabilities. Another trend is the integration of threat intelligence sharing and collaboration among satellite operators and cybersecurity experts (Ben Farah, et. al., 2022, Pavur, 2021, Van Camp & Peeters, 2022). This allows satellite operators to benefit from the collective knowledge and experience of the cybersecurity community in identifying and mitigating cyber threats.

Despite the advancements in cybersecurity analytics, satellite networks still face several challenges. One of the key challenges is the complexity of satellite systems, which can make it difficult to detect and mitigate cyber threats. Additionally, the limited visibility into network traffic in satellite networks poses a challenge for cybersecurity analytics. Regulatory and compliance issues also present challenges for cybersecurity analytics in satellite networks. Satellite operators must comply with various regulations and standards, which can impact their cybersecurity practices (Diro, et. al., 2024, Manulis, et. al., 2021, Tedeschi, Sciancalepore & Di Pietro, 2022).

To address these challenges, satellite operators are adopting several strategic responses. One response is the use of advanced analytics techniques, such as machine learning and artificial intelligence, to enhance threat detection and response capabilities.

Another response is the implementation of secure-by-design principles in satellite system design. This involves building security features into satellite systems from the ground up, rather than adding them as an afterthought. Additionally, satellite operators are investing in employee training and awareness programs to educate their workforce about cybersecurity best practices.

In conclusion, the history of cybersecurity analytics in protecting satellite telecommunications networks is a story of adaptation and innovation. From the early days of encryption and authentication protocols to the current trends of cloud-based security solutions and threat intelligence sharing, cybersecurity analytics has evolved to meet the challenges of protecting satellite networks from cyber threats. By understanding the history, current trends, challenges, and strategic responses in cybersecurity analytics for satellite networks, satellite operators can better

protect their networks and ensure the continued reliability and security of satellite telecommunications services.

Current Trends in Cybersecurity Analytics for Satellite Networks

Cybersecurity analytics plays a critical role in protecting satellite networks from cyber threats. With the increasing sophistication of cyber threats, satellite operators are adopting new technologies and strategies to enhance their cybersecurity capabilities. This article explores the current trends in cybersecurity analytics for satellite networks, including the increasing sophistication of cyber threats, the adoption of machine learning and artificial intelligence, the integration of cloud-based security solutions, and the emphasis on threat intelligence sharing and collaboration (Carlo, et. al., 2023, Matei, 2021, Van Camp & Peeters, 2022).

Cyber threats targeting satellite networks are becoming increasingly sophisticated, posing a significant challenge for satellite operators. Hackers are using advanced techniques such as malware, ransomware, and phishing attacks to compromise satellite systems and steal sensitive information. These attacks are often highly targeted and difficult to detect using traditional security measures. To address this challenge, satellite operators are turning to cybersecurity analytics to enhance their threat detection and response capabilities. By analyzing network traffic, user behavior, and system vulnerabilities, cybersecurity analytics can help identify and mitigate cyber threats before they cause significant damage.

One of the key trends in cybersecurity analytics for satellite networks is the adoption of machine learning and artificial intelligence (AI). These technologies enable satellite operators to analyze large volumes of data and identify patterns that may indicate a cyber threat. Machine learning algorithms can learn from past cyber attacks and improve their ability to detect and respond to new threats in real-time (Fourati & Alouini, 2021, Nair, Deshmukh & Tyagi, 2024, Shaukat, et. al., 2020). For example, machine learning algorithms can be used to detect anomalies in network traffic that may indicate a potential cyber attack. By analyzing patterns in network traffic, machine learning algorithms can identify deviations from normal behavior and alert operators to potential threats.

Another trend in cybersecurity analytics for satellite networks is the integration of cloud-based security solutions. Cloud-based security solutions offer scalability, flexibility, and cost-effectiveness, making them an attractive option for satellite operators looking to enhance their cybersecurity capabilities. Cloud-based security solutions can provide real-time threat detection and response capabilities, as well as advanced analytics tools for analyzing security data. By integrating cloud-based security solutions into their networks, satellite operators can improve their ability to detect and respond to cyber threats quickly and effectively. In addition to adopting new technologies, satellite operators are placing a greater emphasis on threat intelligence sharing and collaboration (Ali & Ditta, 2024, Alturki, et. al., 2023, Meyer, 2022).

By sharing information about cyber threats and vulnerabilities with other operators and cybersecurity experts, satellite operators can improve their collective ability to detect and respond to cyber attacks. Threat intelligence sharing enables satellite operators to learn from each other's experiences and adopt best practices for cybersecurity. Collaboration with cybersecurity experts can also help satellite operators stay ahead of emerging cyber threats and develop more effective cybersecurity strategies.

In conclusion, cybersecurity analytics plays a crucial role in protecting satellite networks from cyber threats. By adopting new technologies such as machine learning and artificial intelligence, integrating cloud-based security solutions, and emphasizing threat intelligence sharing and collaboration, satellite operators can enhance their cybersecurity capabilities and protect their networks from evolving cyber threats. As cyber threats continue to evolve, satellite operators must continue to innovate and adapt their cybersecurity strategies to ensure the security and reliability of satellite telecommunications services.

Challenges in Cybersecurity Analytics for Satellite Networks

Cybersecurity analytics plays a crucial role in protecting satellite networks from cyber threats. However, satellite networks face unique challenges that can make cybersecurity analytics more challenging. This article explores the key challenges in cybersecurity analytics for satellite networks, including the complexity of satellite systems, limited visibility into network traffic, regulatory and compliance challenges, and insider threats and human error (Carlo, et. al., 2023, Unal, 2019, Wu, et. al., 2023).

One of the primary challenges in cybersecurity analytics for satellite networks is the complexity of satellite systems. Satellite networks are composed of multiple interconnected components, including satellites, ground stations, and communication links. This complexity can make it difficult to detect and mitigate cyber threats, as attackers can exploit vulnerabilities in any part of the system. Additionally, satellite systems often rely on legacy technologies that may not have been designed with cybersecurity in mind. These legacy systems can be difficult to secure and may lack the necessary security features to protect against modern cyber threats (Ahmad, et. al., 2022, Bird, 2019, Cao, et. al., 2020).

Another challenge in cybersecurity analytics for satellite networks is the limited visibility into network traffic. Unlike traditional networks, which can use network monitoring tools to capture and analyze network traffic, satellite networks often have limited monitoring capabilities. This limited visibility can make it difficult to detect and mitigate cyber threats, as malicious activity may go unnoticed until it causes significant damage.

Satellite networks are subject to regulatory and compliance requirements, which can pose challenges for cybersecurity analytics. Satellite operators must comply with various regulations and standards, including those related to data protection and privacy. Ensuring compliance with these regulations while also maintaining a high level of cybersecurity can be challenging, as regulations may not always align with best practices in cybersecurity (Chawki, 2023, Falco, 2019, Popova, 2023).

Finally, insider threats and human error pose significant challenges in cybersecurity analytics for satellite networks. Insider threats can be difficult to detect, as malicious insiders may have legitimate access to network resources. Additionally, human error, such as misconfigurations or failure to follow security best practices, can inadvertently expose satellite networks to cyber threats.

To address these challenges, satellite operators can take several steps to enhance their cybersecurity analytics capabilities. These steps include: Implementing advanced analytics techniques, such as machine learning and artificial intelligence, to detect and mitigate cyber threats. Enhancing visibility into network traffic by deploying monitoring tools and implementing

robust logging and auditing practices. Establishing robust compliance programs to ensure compliance with regulatory requirements and standards. Educating employees about cybersecurity best practices and implementing security awareness training programs to reduce the risk of insider threats and human error (Abbasi, Shahraki & Taherkordi, 2021, Islam, 2023, Singh, et. al., 2020). In conclusion, cybersecurity analytics for satellite networks face several challenges, including the complexity of satellite systems, limited visibility into network traffic, regulatory and compliance challenges, and insider threats and human error. By implementing advanced analytics techniques, enhancing visibility into network traffic, and establishing robust compliance programs, satellite operators can enhance their cybersecurity analytics capabilities and better protect their networks from cyber threats.

Strategic Responses to Challenges

Cybersecurity analytics plays a critical role in protecting satellite telecommunications networks from cyber threats. However, these networks face unique challenges that require strategic responses to ensure their security and resilience (Caprolu, et.al., 2020, Gunduz & Das, 2020). This article explores the current trends, challenges, and strategic responses in cybersecurity analytics for satellite networks, focusing on the use of advanced analytics techniques for anomaly detection, implementation of secure-by-design principles in satellite system design, development of incident response plans and cyber resilience strategies, and investment in employee training and awareness programs.

One of the key strategic responses to the challenges of cybersecurity analytics in satellite networks is the use of advanced analytics techniques for anomaly detection. These techniques, such as machine learning and artificial intelligence, enable satellite operators to analyze large volumes of data and identify patterns that may indicate a cyber threat. For example, machine learning algorithms can analyze network traffic and user behavior to detect anomalies that may indicate a potential cyber attack. By using advanced analytics techniques, satellite operators can enhance their ability to detect and respond to cyber threats in real-time (Diro, et. al., 2024, Koroniotis, Moustafa & Slay, 2022, Zhuo, et. al., 2021).

Another strategic response to the challenges of cybersecurity analytics in satellite networks is the implementation of secure-by-design principles in satellite system design. Secure-by-design involves building security features into satellite systems from the ground up, rather than adding them as an afterthought. By implementing secure-by-design principles, satellite operators can reduce the risk of cyber threats and vulnerabilities in their networks. This approach involves considering security requirements at every stage of the satellite system design process, from initial concept to deployment and operation (Baker & Kholidy, 2020, Chen, et. al., 2023, Lam, et. al., 2021).

Developing incident response plans and cyber resilience strategies is another key strategic response to the challenges of cybersecurity analytics in satellite networks. These plans and strategies outline how satellite operators will respond to cyber threats and incidents, including how they will detect, contain, and mitigate cyber attacks. By developing incident response plans and cyber resilience strategies, satellite operators can minimize the impact of cyber attacks and ensure the continuity of their operations. These plans should be regularly tested and updated to ensure their effectiveness (Green, et. al., 2020, Lekota & Coetzee, 2021, Panda & Bower, 2020).

Investing in employee training and awareness programs is also crucial for addressing the challenges of cybersecurity analytics in satellite networks. Employees are often the first line of defense against cyber threats, so it is essential that they are trained to recognize and respond to potential threats. Training programs should cover topics such as cybersecurity best practices, threat awareness, and incident response (Annarelli, Nonino & Palombi, 2020, Chauhan & Shiaeles, 2023, Manulis, et. al., 2021). By investing in employee training and awareness programs, satellite operators can improve their overall cybersecurity posture and reduce the risk of human error leading to cyber incidents.

In conclusion, cybersecurity analytics in protecting satellite telecommunications networks face several challenges, including the complexity of satellite systems, limited visibility into network traffic, regulatory and compliance challenges, and insider threats and human error. By implementing strategic responses such as using advanced analytics techniques for anomaly detection, implementing secure-by-design principles in satellite system design, developing incident response plans and cyber resilience strategies, and investing in employee training and awareness programs, satellite operators can enhance their cybersecurity capabilities and better protect their networks from cyber threats.

Case Studies and Examples

Cybersecurity analytics plays a crucial role in protecting satellite telecommunications networks from cyber threats. This article presents case studies and examples of successful implementation of cybersecurity analytics in satellite networks, highlighting current trends, challenges, and strategic responses. It also discusses lessons learned from cybersecurity incidents in the satellite telecommunications industry (Ashraf, et. al., 2022, Manulis, et. al., 2021).

One example of successful implementation of cybersecurity analytics in satellite networks is the use of machine learning algorithms for anomaly detection. By analyzing network traffic and user behavior, machine learning algorithms can identify patterns that may indicate a potential cyber threat. This approach has been used by satellite operators to detect and mitigate cyber attacks in real-time, enhancing the security of their networks (Luo, et. al., 2021, Nassif, et. al., 2021, Saeed, et. al., 2023).

Another example is the use of cloud-based security solutions for threat detection and response. Cloud-based security solutions offer scalability and flexibility, allowing satellite operators to quickly adapt to changing cyber threats. These solutions can analyze large volumes of data and provide real-time threat intelligence, enabling operators to respond to cyber threats more effectively.

Despite the advancements in cybersecurity analytics, the satellite telecommunications industry has experienced several cybersecurity incidents that have highlighted the importance of robust cybersecurity measures. One such incident was the 2018 cyber attack on a satellite communications provider, which resulted in the compromise of sensitive customer data. This incident underscored the need for satellite operators to implement robust cybersecurity measures to protect their networks from cyber threats.

Another lesson learned from cybersecurity incidents in the satellite telecommunications industry is the importance of collaboration and information sharing. Cyber threats are constantly evolving, and no single organization can address them alone. By collaborating with other operators and

cybersecurity experts, satellite operators can gain valuable insights into emerging cyber threats and develop more effective cybersecurity strategies (Borowitz, 2019, Housen-Couriel, 2023).

Current trends in cybersecurity analytics for satellite networks include the increasing use of machine learning and artificial intelligence, the integration of cloud-based security solutions, and the emphasis on threat intelligence sharing and collaboration. These trends reflect the industry's efforts to enhance its cybersecurity capabilities and protect its networks from cyber threats.

Challenges in cybersecurity analytics for satellite networks include the complexity of satellite systems, limited visibility into network traffic, regulatory and compliance challenges, and insider threats and human error. To address these challenges, satellite operators are implementing strategic responses such as using advanced analytics techniques for anomaly detection, implementing secure-by-design principles in satellite system design, developing incident response plans and cyber resilience strategies, and investing in employee training and awareness programs (Al-Hawawreh, Moustafa & Slay, 2024, Bonnart, et. al., 2023, Breda, et. al., 2023).

In conclusion, cybersecurity analytics plays a crucial role in protecting satellite telecommunications networks from cyber threats. By implementing successful cybersecurity analytics solutions and learning from past cybersecurity incidents, satellite operators can enhance the security of their networks and ensure the continued reliability and security of satellite telecommunications services.

Future Trends in Cybersecurity Analytics for Satellite Networks

The future of cybersecurity analytics for satellite networks is shaped by emerging technologies and evolving cyber threats. This article explores the future trends in cybersecurity analytics for satellite networks, including the continued evolution of cyber threats, the integration of blockchain technology for secure data transmission, the adoption of quantum-safe cryptography, and the enhanced regulatory frameworks for satellite cybersecurity (Andås, 2020, Koroniotis, Moustafa & Slay, 2022, Ukwandu, et. al., 2022).

One of the key trends in cybersecurity analytics for satellite networks is the continued evolution of cyber threats. As satellite networks become more interconnected and reliant on digital technologies, they are increasingly targeted by sophisticated cyber attacks. These attacks are often highly targeted and can exploit vulnerabilities in satellite systems to compromise sensitive information. To address this trend, satellite operators must continually update their cybersecurity analytics capabilities to detect and mitigate emerging cyber threats. This may involve the use of advanced analytics techniques, such as machine learning and artificial intelligence, to identify patterns and anomalies that may indicate a cyber attack (AlSalem, Almaiah & Lutfi, 2023, Ben Farah, et. al., 2022).

Another trend in cybersecurity analytics for satellite networks is the integration of blockchain technology for secure data transmission. Blockchain technology offers a decentralized and secure way to transmit data, making it ideal for protecting sensitive information in satellite networks. By integrating blockchain technology into their networks, satellite operators can enhance the security and integrity of their data transmissions. Blockchain technology can also be used to create secure communication channels between satellites and ground stations, further enhancing the security of satellite networks (Aggarwal, Kumar & Tanwar, 2020, Kumar, et. al., 2021, Yue, et. al., 2022).

With the advent of quantum computing, there is a growing need for quantum-safe cryptography to protect satellite networks from quantum-enabled cyber attacks. Quantum computing has the potential to break traditional cryptographic algorithms, making them vulnerable to cyber attacks (Chawla & Mehra, 2023, Lindsay, 2020, Rozenman, et. al., 2023). To address this challenge, satellite operators are exploring the adoption of quantum-safe cryptography, which uses quantum-resistant algorithms to secure data transmissions. By adopting quantum-safe cryptography, satellite operators can ensure the security of their networks against future quantum-enabled cyber threats.

The future of cybersecurity analytics for satellite networks also includes enhanced regulatory frameworks to ensure the security and resilience of satellite networks. Regulatory bodies are increasingly recognizing the importance of cybersecurity in satellite telecommunications and are implementing regulations to enhance cybersecurity practices in the industry. Satellite operators must comply with these regulations and standards to ensure the security of their networks. This may involve implementing robust cybersecurity measures, such as encryption, authentication, and access control, to protect satellite systems from cyber threats (McCarthy, et. al., 2023, Turner & Jahankhani, 2021, Verco, 2021).

In conclusion, the future of cybersecurity analytics for satellite networks is shaped by emerging technologies and evolving cyber threats. By staying ahead of these trends and adopting advanced cybersecurity measures, satellite operators can enhance the security and resilience of their networks and ensure the continued reliability of satellite telecommunications services.

CONCLUSION

Cybersecurity analytics plays a crucial role in protecting satellite telecommunications networks from cyber threats. This article has explored the conceptual development of current trends, challenges, and strategic responses in cybersecurity analytics for satellite networks.

We discussed the increasing sophistication of cyber threats targeting satellite networks, the adoption of machine learning and artificial intelligence in cybersecurity analytics, the integration of cloud-based security solutions, and the emphasis on threat intelligence sharing and collaboration. Challenges such as the complexity of satellite systems, limited visibility into network traffic, regulatory and compliance challenges, and insider threats and human error were also highlighted. Strategic responses including the use of advanced analytics techniques for anomaly detection, implementation of secure-by-design principles, development of incident response plans, and investment in employee training and awareness programs were identified.

To enhance cybersecurity in satellite telecommunications networks, satellite operators should consider the following recommendations: Implement advanced cybersecurity analytics tools and techniques, such as machine learning and artificial intelligence, to detect and mitigate cyber threats in real-time. Integrate secure-by-design principles into satellite system design to minimize vulnerabilities and enhance network security. Develop and regularly test incident response plans and cyber resilience strategies to ensure the continuity of operations in the event of a cyber attack. Invest in employee training and awareness programs to educate staff about cybersecurity best practices and reduce the risk of human error leading to cyber incidents. It is crucial for satellite operators to adopt proactive cybersecurity measures to protect their networks from evolving threats. By staying ahead of the curve and implementing robust cybersecurity measures, satellite

operators can ensure the security and reliability of their networks and protect sensitive information from cyber attacks.

In conclusion, cybersecurity analytics is essential for protecting satellite telecommunications networks from cyber threats. By understanding current trends, challenges, and strategic responses in cybersecurity analytics, satellite operators can enhance their cybersecurity capabilities and ensure the continued security and reliability of satellite telecommunications services.

Reference

Abbasi, M., Shahraki, A., & Taherkordi, A. (2021). Deep learning for network traffic monitoring and analysis (NTMA): A survey. *Computer Communications, 170*, 19-41.

Aggarwal, S., Kumar, N., & Tanwar, S. (2020). Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions. *IEEE Internet of Things Journal, 8*(7), 5416-5441.

Ahmad, I., Suomalainen, J., Porambage, P., Gurtov, A., Huusko, J., & Höyhtyä, M. (2022). Security of satellite-terrestrial communications: Challenges and potential solutions. *IEEE Access, 10*, 96038-96052.

Al-Hawawreh, M., Moustafa, N., & Slay, J. (2024). A threat intelligence framework for protecting smart satellite-based healthcare networks. *Neural Computing and Applications, 36*(1), 15-35.

Ali, A., & Ditta, A. (2024). Securing Satellite Constellations: Challenges and Solutions for Next-Generation Space-Based Networks (No. 11831). EasyChair.

AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023). Cybersecurity Risk Analysis in the IoT: A Systematic Review. *Electronics, 12*(18), 3958.

Alturki, N., Aljrees, T., Umer, M., Ishaq, A., Alsubai, S., Saidani, O., ... & Ashraf, I. (2023). An intelligent framework for cyber–physical satellite system and IoT-Aided aerial vehicle security threat detection. *Sensors, 23*(16), 7154.

Andås, H. E. (2020). Emerging technology trends for defence and security.

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering, 149*, 106829.

Ashraf, I., Narra, M., Umer, M., Majeed, R., Sadiq, S., Javaid, F., & Rasool, N. (2022). A deep learning-based smart framework for cyber-physical and satellite system security threats detection. *Electronics, 11*(4), 667.

Baker, C., & Kholidy, H. A. (2020). Cyber Security Advantages of Optical Communications in SATCOM Networks (Doctoral dissertation, SUNY Polytechnic Institute).

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information, 13*(1), 22.

Bird, D. (2019). Cybersecurity considerations for Internet of things small satellite systems. *Current Analysis on Communications Engineering Journal, 2*, 69-79.

Bonnart, S., Capurso, A., Carlo, A., Dethlefsen, T. F., Kerolle, M., Lim, J., ... & Zarkan, L. C. (2023). Cybersecurity Threats to Space: From Conception to the Aftermaths. In Space Law in a Networked World (pp. 39-101). Brill Nijhoff.

Borowitz, M. (2019). Strategic implications of the proliferation of space situational awareness technology and information: lessons learned from the remote sensing sector. *Space Policy, 47*, 18-27.

Green, A. W., Woszczynski, A. B., Dodson, K., & Easton, P. (2020). Responding to cybersecurity challenges: Securing vulnerable US emergency alert systems. *Communications of the Association for Information Systems, 46*(1), 8.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks, 169*, 107094.

Housen-Couriel, D. (2023). IAC-21-E-9 (Paper ID: 67116) Information sharing for the mitigation of outer space–related cybersecurity threats. *Acta Astronautica, 203*, 546-550.

Islam, M. A. (2023). Application of artificial intelligence and machine learning in security operations center. *Issues in Information Systems, 24*(4).

Koroniotis, N., Moustafa, N., & Slay, J. (2022). A new Intelligent Satellite Deep Learning Network Forensic framework for smart satellite networks. *Computers and Electrical Engineering, 99*, 107745.

Kumar, R. L., Pham, Q. V., Khan, F., Piran, M. J., & Dev, K. (2021). Blockchain for securing aerial communications: Potentials, solutions, and research directions. *Physical Communication, 47*, 101390.

Lam, K. Y., Mitra, S., Gondesen, F., & Yi, X. (2021). ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities. *IEEE Internet of Things Journal, 9*(8), 5895-5908.

Lekota, F., & Coetzee, M. (2021, June). Aviation Sector Computer Security Incident Response Teams: Guidelines and Best Practice. In European Conference on Cyber Warfare and Security (pp. 507-XII). Academic Conferences International Limited.

Lindsay, J. R. (2020). Surviving the quantum cryptocalypse. *Strategic Studies Quarterly, 14*(2), 49-73.

Luo, Y., Xiao, Y., Cheng, L., Peng, G., & Yao, D. (2021). Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. *ACM Computing Surveys (CSUR), 54*(5), 1-36.

Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2021). Cyber security in new space: analysis of threats, key enabling technologies and challenges. *International Journal of Information Security, 20*, 287-311.

Matei, V. C. (2021). Cybersecurity Analysis for the Internet-Connected Satellites.

McCarthy, J., Mamula, D., Brule, J., Meldorf, K., Jennings, R., Wiltberger, J., ... & Sepassi, S. (2023). Cybersecurity framework profile for Hybrid Satellite Networks (HSN). National Institute of Standards and Technology, NIST Interagency or Internal Report (IR) NIST IR, 8441(2023), 28.

Meyer, B. L. (2022). Perilous paths: the cybersecurity issues of a space-based cloud imagery processing system. In ASCEND 2022 (p. 4327).

Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial intelligence for cyber security: Current trends and future challenges. *Automated Secure Computing for Next-Generation Systems*, 83-114.

Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management, 5*(1), 51-63.

Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). Machine learning for anomaly detection: A systematic review. *IEEE Access, 9*, 78658-78700.

Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment, 11*(4), 507-518.

Pavur, J. (2021). Securing new space: on satellite cyber-security (Doctoral dissertation, University of Oxford).

Pavur, J., & Martinovic, I. (2022). Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight. *Journal of Cybersecurity, 8*(1), tyac008.

Petrenko, S. (2022). Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation. CRC Press.

Popova, R. (2023). Space Technology and Cybersecurity: Challenges and Technical Approaches for the Regulation of Large Constellations. In Space Law in a Networked World (pp. 102-128). Brill Nijhoff.

Rozenman, G. G., Kundu, N. K., Liu, R., Zhang, L., Maslennikov, A., Reches, Y., & Youm, H. Y. (2023). The quantum internet: A synergy of quantum information technologies and 6G networks. *IET Quantum Communication, 4*(4), 147-166.

Saeed, M. M., Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. (2023). Anomaly detection in 6G networks using machine learning methods. *Electronics, 12*(15), 3300.

Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science, 10*(6), 1473-1498.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE Access, 8*, 222310-222354.

Singh, S., Karimipour, H., HaddadPajouh, H., & Dehghantanha, A. (2020). Artificial intelligence and security of industrial control systems. *Handbook of Big Data Privacy*, 121-164.

Tedeschi, P., Sciancalepore, S., & Di Pietro, R. (2022). Satellite-based communications security: A survey of threats, solutions, and research challenges. *Computer Networks, 216*, 109246.

Turner, L. A., & Jahankhani, H. (2021, May). An investigation into an approach to updating the governance of satellite communications to enhance cyber security. In Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London, January 2021 (pp. 23-33). Cham: Springer International Publishing.

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. *Information, 13*(3), 146.

Ullah, F., & Babar, M. A. (2019). Architectural tactics for big data cybersecurity analytics systems: a review. *Journal of Systems and Software, 151*, 81-118.

Unal, B. (2019). Cybersecurity of NATO's Space-based Strategic Assets. Chatham House. The Royal Institute of International Affairs.

Van Camp, C., & Peeters, W. (2022). A world without satellite data as a result of a global cyber-attack. *Space Policy*, *59*, 101458.

Varadharajan, V., & Suri, N. (2023). Security challenges when space merges with cyberspace. *Space Policy*, 101600.

Verco, E. (2021). Satellites are cyber insecure: We need regulation to avoid a disaster. *ANU Journal of Law and Technology*, *2*(2), 57-94.

Wu, X., Du, Y., Fan, T., Guo, J., Ren, J., Wu, R., & Zheng, T. (2023). Threat analysis for space information network based on network security attributes: a review. *Complex & Intelligent Systems*, *9*(3), 3429-3468.

Yue, P., An, J., Zhang, J., Pan, G., Wang, S., Xiao, P., & Hanzo, L. (2022). On the security of LEO satellite communication systems: Vulnerabilities, countermeasures, and future trends. *arXiv preprint arXiv:2201.03063.*