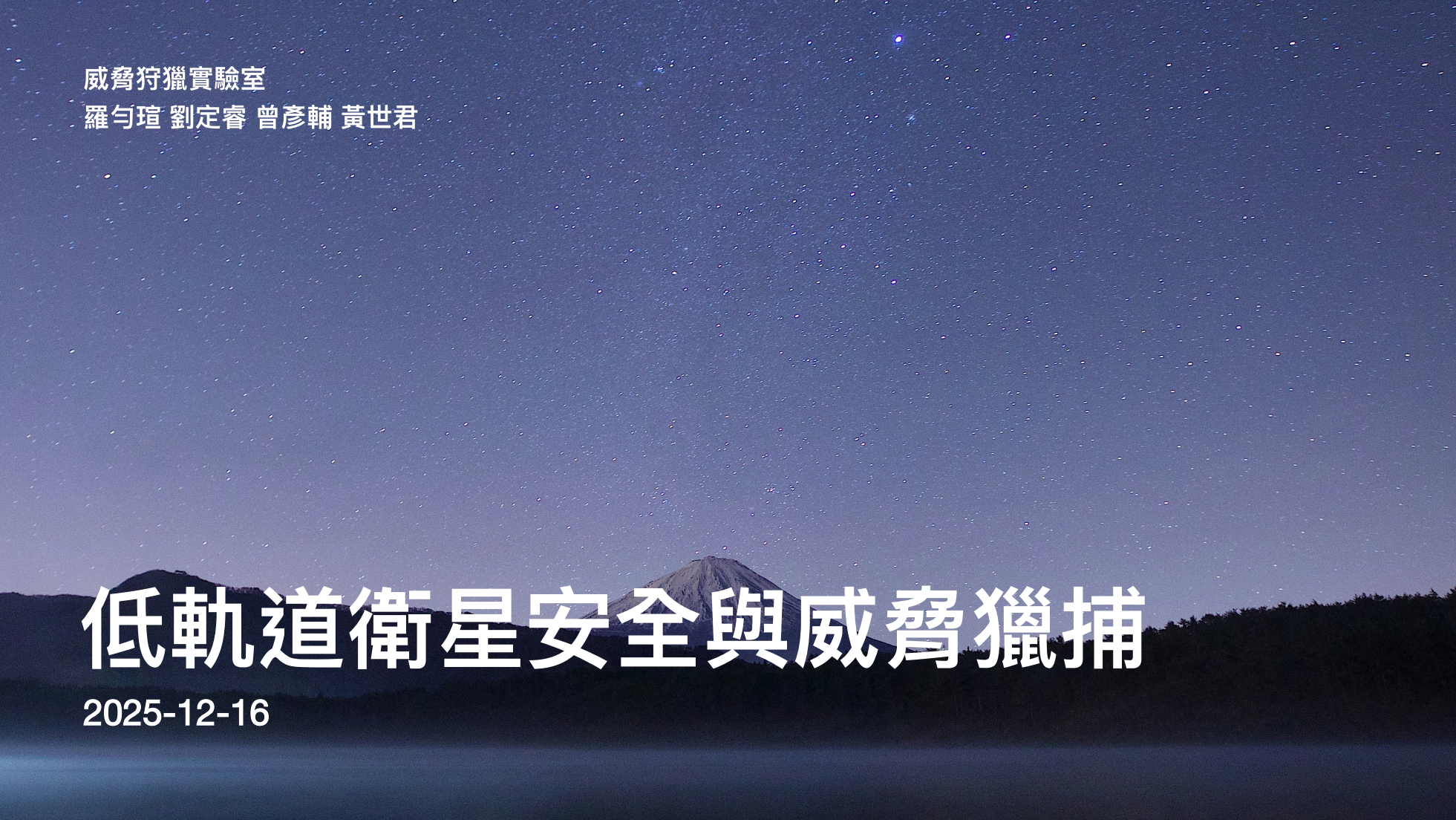
威脅狩獵實驗室
羅勻瑄 劉定睿 曾彥輔 黃世君



低軌道衛星安全與威脅獵捕

2025-12-16

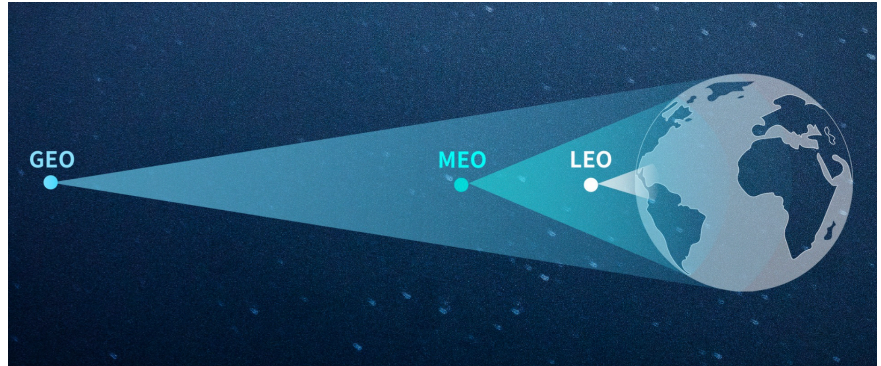
低軌道衛星簡介

為什麼選擇低軌衛星？

- 低軌衛星能補足偏遠地區、海上、空中及災害戰時通訊
- 形成新型通訊基礎設施，成為未來資安新戰場
- 高覆蓋率、低延遲特性引發全球關注

什麼是低軌衛星（LEO）？

- 高度 160-2000 公里，繞地球一圈 90-120 分鐘
- 一天繞行多圈，覆蓋多區域



	LEO（低軌道衛星）	MEO（中軌道衛星）	GEO（同步軌道衛星）
與地球距離	500~2000km	5000~12000km	35786 km
衛星覆蓋率	最小	次之	最大
所需衛星數	數百顆	6	4
單程傳輸延遲	3.3ms	66.7ms	119ms
衛星運行週期	100mins	12hrs	24hrs
天線追蹤速度	每10分鐘追蹤	每小時追蹤	穩定
軌道應用	低延遲應用	衛星導航系統	衛星電視/電話、氣象觀測

低軌衛星三大關鍵特性

- **延遲低**：20-40ms（vs. GEO 600ms+），適合視訊/遊戲
- **星座系統**：數千顆衛星組成，自動追蹤切換實現全球覆蓋
- **壽命短**：受大氣阻力影響，需持續補發新衛星

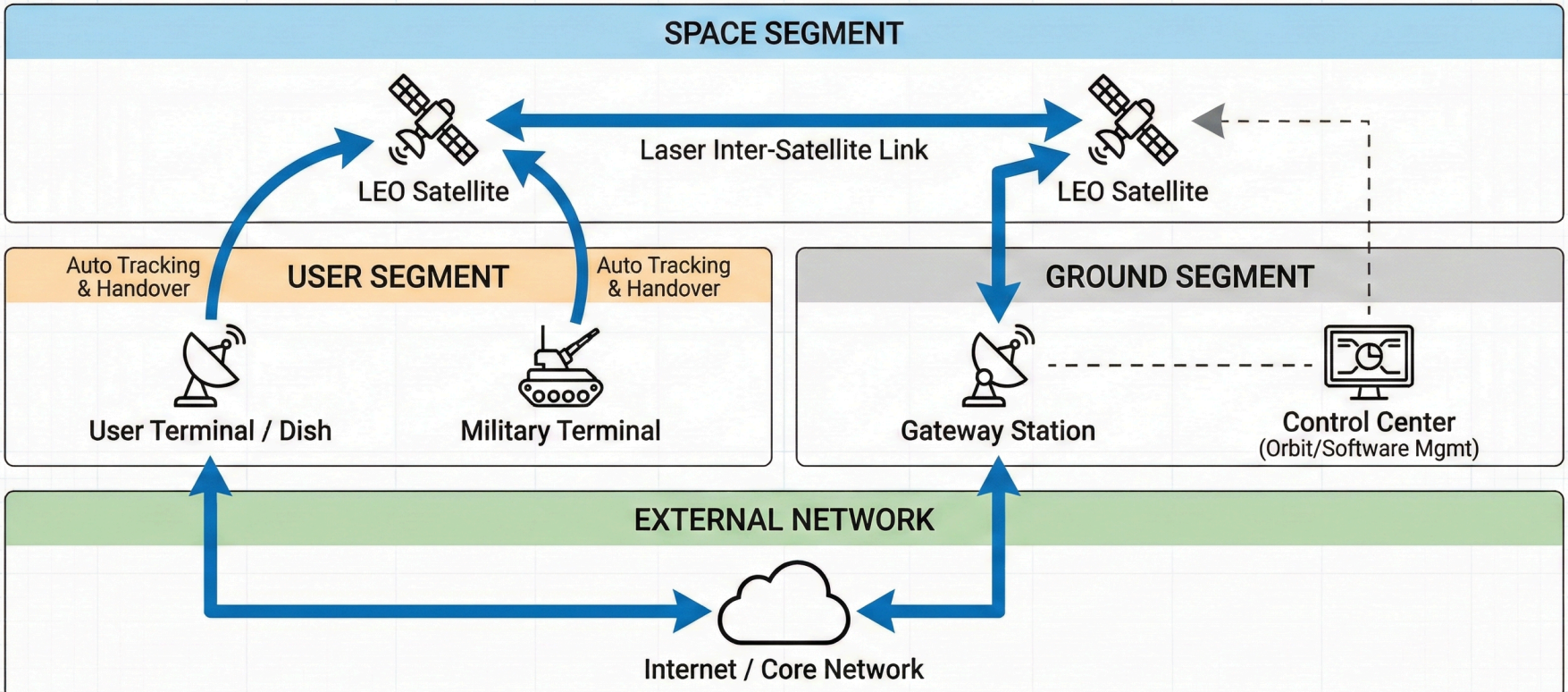
主要應用

- **寬頻上網**：Starlink/OneWeb 提供偏遠/海上高速網路
- **地球觀測**：高解析遙測、災害監測
- **物聯網**：感測器資料回傳（如船隻/環境）
- 案例：Starlink 戰爭/災害緊急通訊

系統架構三大部分

- **太空段**：LEO 衛星 + 雷射星間鏈路
- **地面段**：閘道站 + 控制中心（軌道 / 軟體管理）
- **用戶段**：碟形天線 / 軍用終端，自動追蹤切換

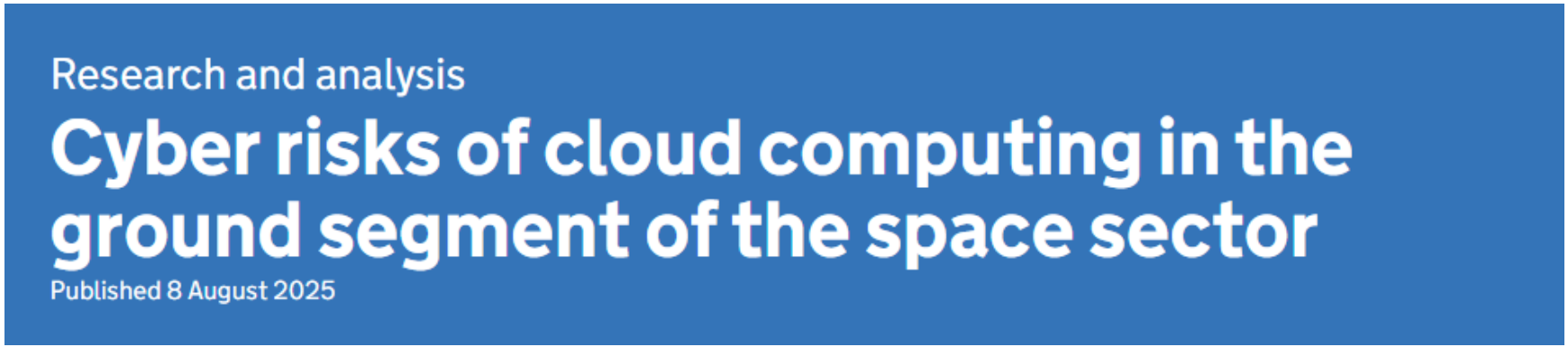
LEO SATELLITE SYSTEM ARCHITECTURE



DATA FLOW DIAGRAM: User ↔ LEO Satellite ↔ Gateway ↔ Internet

低軌道衛星攻擊

地面控制站攻擊（Ground/Control Segment）



https://www.gov.uk/government/publications/cyber-risks-of-cloud-computing-in-the-ground-segment-of-the-space-sector

Security Challenges in Satellite Ground Stations and their Risk Mitigation Techniques

Machacha Tafadzwa Langton
School of Cyberspace and Technology
Beijing Institute of Technology
Beijing, China
machachatafadzwa@outlook.com

Ziyi Yang*
School of Cyberspace and Technology
Beijing Institute of Technology
Beijing, China
yziyi@bit.edu.cn
*Corresponding author

Gaofeng Pan
School of Cyberspace and Technology
Beijing Institute of Technology
Beijing, China
gfpan@bit.edu.cn

Hao Zhang
NO.208 Research Institute of China Ordnance Industries
Beijing, China
13260186899@163.com

Guangwen Luo
NO.208 Research Institute of China Ordnance Industries
Beijing, China
lgw0627@163.com

Haomin Yang
NO.208 Research Institute of China Ordnance Industries
Beijing, China
15321776871@163.com

地面控制站威脅/攻擊手法

- 進階持續性滲透攻擊（APT）
  - 傳統滲透獲得地面站控制
- 物理攻擊
  - 實體破壞
- 通訊攻擊
  - 竊聽與攔截（Eavesdropping and Interception）
  - 干擾（Jamming）

Threats Against Satellite Ground Infrastructure: A retrospective analysis of sophisticated attacks

Jessie Hamill-Stewart
University of Bristol, University of Bath
jessie.hamill-stewart@bristol.ac.uk

Awais Rashid
University of Bristol
awais.rashid@bristol.ac.uk

Hamill-Stewart, J., & Rashid, A. (2024, March). Threats against satellite ground infrastructure: A retrospective analysis of sophisticated attacks. In Proceedings of the 2024 Workshop on Security of Space and Satellite Systems (Vol. 1).

Space Odyssey: An Experimental Software Security Analysis of Satellites

Johannes Willbold*, Moritz Schloegel*‡, Manuel Vögele*, Maximilian Gerhardt*,
Thorsten Holz‡, Ali Abbasi‡

*Ruhr University Bochum, firstname.lastname@rub.de
‡CISPA Helmholtz Center for Information Security, lastname@cispa.de

Willbold, J., Schloegel, M., Vögele, M., Gerhardt, M., Holz, T., & Abbasi, A. (2023, May). Space odyssey: An experimental software security analysis of satellites. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 1-19). IEEE.

通訊鏈路攻擊（Link Segment）

- 衛星與衛星之間的通訊鏈路 (Inter-Satellite Link)
- 攻擊者控制一顆衛星 → 透過 ISL 向衛星群中其他衛星發送惡意遙測指令 (Telecommand, TC)

太空段/衛星平台攻擊（Space/Onboard Segment）

- 未加密通訊協議/弱驗證
  - 遠端地面站或自製天線發送任意構造的遙測指令 (Telecommand, TC) 至衛星通訊模組 (COM)
  - 衛星完全不使用加密，攻擊者可用商用無線電設備（如 HackRF）攔截與偽造指令

太空段/衛星平台攻擊（Space/Onboard Segment）

- 未加密通訊協議/弱驗證
  - 遠端地面站或自製天線發送任意構造的遙測指令 (Telecommand, TC) 至衛星通訊模組 (COM)
  - 衛星完全不使用加密，攻擊者可用商用無線電設備（如 HackRF）攔截與偽造指令
- 緩衝區溢位與任意程式碼執行
  - 危險遙測指令 (Dangerous TC)
  - 堆疊緩衝區溢位 (String Overflow)

太空段/衛星平台攻擊（Space/Onboard Segment）

- 未加密通訊協議/弱驗證
  - 遠端地面站或自製天線發送任意構造的遙測指令 (Telecommand, TC) 至衛星通訊模組 (COM)
  - 衛星完全不使用加密，攻擊者可用商用無線電設備（如 HackRF）攔截與偽造指令
- 緩衝區溢位與任意程式碼執行
  - 危險遙測指令 (Dangerous TC)
  - 堆疊緩衝區溢位 (String Overflow)
- 韌體更新指令缺乏加密完整性驗證或簽章驗證

  1. 攻擊者發送惡意韌體映像 (透過破壞的指令處理器)
  2. 衛星接受並燒寫至快閃記憶體
  3. 下次重開機時執行攻擊者的韌體 → 永久性控制

其他風險與弱點

- 定時與位置同步破壞
  - 依賴 GNSS 的衛星導航與授時系統
    - 信號欺騙 (Spoofing)：發送虛假 GNSS 訊號，微調衛星時鐘偏差
    - 漸進式破壞：不觸發即時警報，而是逐步誤導定位計算

Stojnic, T., Kayes, A. S. M., Rahayu, W., & Chowdhury, M. J. M. (2025). A comprehensive literature review of cyber threats and vulnerabilities in IoT-driven satellite networks: Research challenges and future directions. Computer Networks, 111678.

其他風險與弱點

- 認證協議缺陷 (前向安全性)
  - 傳統衛星認證協議缺乏前向安全性 (Perfect Forward Secrecy, PFS)
  - 如果攻擊者未來獲得衛星的長期私鑰，可解密過去所有截獲的通訊紀錄

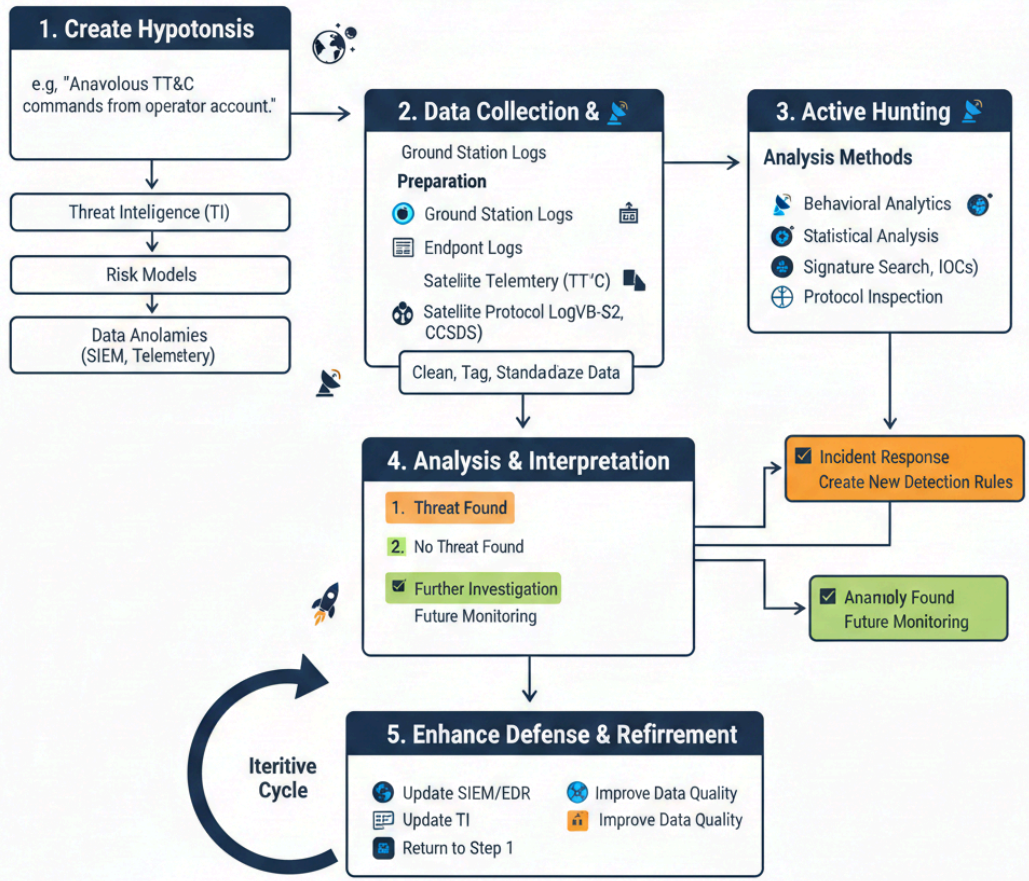
Xu, S., Liu, X., Ma, M., & Chen, J. (2020). An improved mutual authentication protocol based on perfect forward secrecy for satellite communications. International Journal of Satellite Communications and Networking, 38(1), 62-73.

衛星網路中的威脅獵捕

威脅狩獵核心機制

- 定義： 主動搜尋現有防禦機制（如防火牆）漏掉的潛在威脅。
- 標準流程：
  - 建立假設： 基於對攻擊者手法 (TTPs) 的了解，推測攻擊可能發生的位置。
  - 調查與驗證： 透過日誌 (Logs) 與數據確認假設是否成立。
  - 偵測與回應： 發現威脅並阻斷。
- 關鍵依賴： 需具備「攻擊情資」來建立假設，以及「可視化數據」來進行驗證。

Satellite Network Threat Hunting Process



衛星網路實施威脅狩獵之困境

- 困境一：無法建立假設
  - 傳統衛星領域依賴隱匿式安全，缺乏公開的攻擊案例。
  - 後果： 研究人員不知道衛星會遭受何種具體攻擊，導致無法提出有效的狩獵假設。

衛星網路實施威脅狩獵之困境

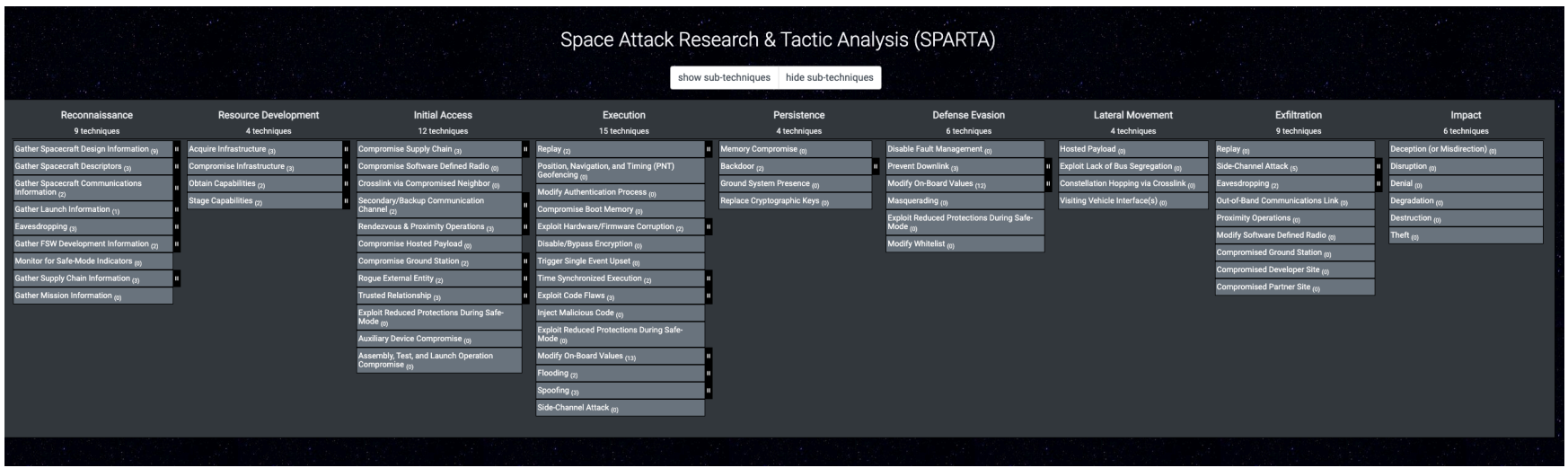
- 困境一：無法建立假設
  - 傳統衛星領域依賴隱匿式安全，缺乏公開的攻擊案例。
  - 後果： 研究人員不知道衛星會遭受何種具體攻擊，導致無法提出有效的狩獵假設。
- 困境二：缺乏資安可視性
  - 衛星受限於 SWaP (尺寸、重量、電力)，無法安裝傳統 EDR 或資安監控軟體。
  - 後果： 缺乏標準化資安日誌，導致無 Log 可查。

衛星網路實施威脅狩獵之困境

- 困境一：無法建立假設
  - 傳統衛星領域依賴隱匿式安全，缺乏公開的攻擊案例。
  - 後果： 研究人員不知道衛星會遭受何種具體攻擊，導致無法提出有效的狩獵假設。
- 困境二：缺乏資安可視性
  - 衛星受限於 SWaP (尺寸、重量、電力)，無法安裝傳統 EDR 或資安監控軟體。
  - 後果： 缺乏標準化資安日誌，導致無 Log 可查。
- 困境三：數據性質不匹配
  - 衛星僅產出**遙測數據 (Telemetry)**（如電壓、溫度、姿態）。
  - 後果： 遙測數據設計用於「健康監控」而非「資安偵測」，雜訊多且難以直接對應惡意行為。

「無法建立假設」的解決方案：SPARTA 框架介紹

- 簡介： Space Attack Research and Tactic Analysis，由 The Aerospace Corporation 發布。
- 定位： 太空領域的 MITRE ATT&CK，提供標準化的戰術與技術矩陣。
- 適用範圍： 涵蓋**太空段**、**地面段**與**鏈路段**，適用於完整衛星網路架構。



攻擊戰術與技術分析

戰術階段	相關技術範例
偵察	收集航天器設計資訊、收集航天器描述符、竊聽、收集供應鏈資訊和任務資訊等
資源開發	獲取和危害基礎設施、獲得網路能力、獲得非網路能力、分級 (火箭級) 能力等
初始存取	危害供應鏈、透過被危害的鄰近衛星交叉連結、利用安全模式下保護減少的漏洞、危害地面系統等
執行	重播攻擊 (Replay)、PNT 地理圍欄、引發單粒子翻轉 (Trigger single event upset)、惡意代碼、干擾 (Jamming)、欺騙 (Spoofing) 等

攻擊戰術與技術分析

戰術階段	相關技術範例
持續控制	記憶體危害、後門、地面系統存在、加密金鑰替換、有效憑證等
防禦規避	停用故障管理、防止下行連結、偽裝、根套件 (Rootkit)、溢出審計日誌等
橫向移動	託管有效載荷、透過交叉連結進行星座跳躍、虛擬化逃逸、有效憑證等
資料外洩	重播攻擊、側信道攻擊、帶外通信連結、修改通信配置、受損的地面系統等
影響	欺騙（或誤導）、中斷、拒絕、降級、破壞、盜竊

「針對 SWaP 限制」的解決方案：輕量級 AI/ML 偵測與獵捕模型

- 簡介: 集中在使用 AI/ML 來規避 SWaP 限制，並建立威脅模型來指導獵捕。
- 核心: 它的設計理念是利用自主性 (Autonomous) 和輕量化的 AI 解決方案，以適應衛星系統的限制，在軌道上即可實施近乎實時的網路安全態勢感知和威脅響應。它強調通過縮短入侵到識別的時間來保護空間通信的完整性。
- 功能與技術
  - 人工智慧與機器學習 (AI/ML)
  - 用戶與實體行為分析 (UEBA)
  - 自動化假設檢測與回應
  - 安全報告

76th International Astronautical Congress (IAC 2025), Sydney, Australia, 29 Sep-3 Oct 2025.

IAC-25,E9,2,13,x96563

PROACTIVE CELESTIAL HUNTER FOR ARTIFICIAL INTELLIGENCE-DRIVEN CYBER THREAT HUNTING IN SPACE (A.I.C.T.H.S)

Teymur Novruzov*

Teymur Novruzov* *SABAH Groups, Azerbaijan State Oil and Industry University, Baku, Azerbaijan, teymurn50615@sabah.edu.az*
* Corresponding Author

PROACTIVE CELESTIAL HUNTER FOR ARTIFICIAL INTELLIGENCE-DRIVEN CYBER THREAT HUNTING IN SPACE (A.I.C.T.H.S)

針對「遙測數據與資安不匹配」困境所提出的解決方案

- AI可解釋性
- 基於深度學習的時序數據異常偵測
- 利用合成數據集進行模型訓練

部署地點	角色與功能	克服 SWaP 的方式
衛星端/邊緣模組 (Lightweight Agent)	執行**初步**、**實時**的異常偵測（Anomaly Detection）。模型專注於極少數的**關鍵遙測數據**和**行為指標**。	**最小化運算資源：** 模組只在衛星上運行**輕量化**的 AI/ML 推論模型，不運行資源密集型的**深度學習訓練**或複雜的數位鑑識。這將大部分的計算負載留在地面。
地面雲端中心 (Cloud-Centric)	執行**集中審核**、**深度鑑識**、**模型訓練**，以及運行**自動化回應**的決策樹。	**最大化電力效率：** 將高度耗能的運算（如模型訓練、數據庫存儲和複雜的行為關聯分析）全部放在地面機房或雲端，衛星只負責最基本的數據前置處理和偵測。

結論

- 衛星網路資安不僅是資訊安全議題更是國家通訊安全與數位韌性議題。
- 借鏡烏俄戰爭，使臺灣發展衛星安全更為重要。
- 威脅無所不在，透過已知攻擊的情資無法補足的，可以透過威脅狩獵獵捕未知攻擊。

Reference

- SSH.com, "Satellite Cybersecurity: Threats and Impacts," SSH Academy, Helsinki, Finland. Online. Available: https://www.ssh.com/academy/satellite-cybersecurity-threats-impacts. Accessed: Dec. 12, 2025.

- BQPSim, "Satellite Hacking & Cyber Warfare," BQPSim Blog. Online. Available: https://www.bqpsim.com/blogs/satellite-hacking-cyber-warfare. Accessed: Dec. 12, 2025.

- "Threats Against Satellite Ground Infrastructure: A retrospective analysis of sophisticated attacks," in Proc. Network and Distributed System Security Symposium (NDSS) SpaceSec Workshop, San Diego, CA, USA, 2024.

- C. Swope, K. A. Bingen, M. Young, and K. LaFave, "Space Threat Assessment 2025," Center for Strategic and International Studies (CSIS), Washington, D.C., USA, Rep., Apr. 2025.

- Rohde & Schwarz, "An Overview of Space Electronic Warfare," Munich, Germany, White Paper, 2025. Online. Available: https://www.rohde-schwarz.com.

- M. Ciccaglione, L. Bracciale, P. Loreti, and A. M. Zanon, "Cyber Range for Space Systems: Training Scenarios for Satellite Cybersecurity Preparedness," in Proc. 10th Intl. Symp. on End-User Development (IS-EUD), CEUR Workshop Proceedings, vol. 3978, Munich, Germany, Jun. 2025.
- S. K. Khan et al., "Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions," Int. J. Crit. Infrastruct. Prot., vol. 2025, Art. no. S1874548224000659, 2025.
- M. Donchev and D. Smyth, "Evaluating an Effective Ransomware Infection Vector in Low Earth Orbit Satellites," arXiv:2412.04601 cs.CR, Dec. 2024.
- Malva.re, "Ransomware Attack Vector in LEO Satellites," Malva.re Blog. Online. Available: https://malva.re/ransomware-attack-vector-leo-satellites/.
- LSE IDEAS, "Cyberattacks on Satellites," London School of Economics and Political Science, London, UK, Project Rep., 2025.
- J. Vanlyssel, E. Sobrados, et al., "SpyChain: Multi-Vector Supply Chain Attacks on Small Satellite Systems," arXiv:2510.06535 cs.CR, Oct. 2025.

- "Security Analysis of Low Earth Orbit Satellites Based on Different Software-Defined Networking Structure," in Proc. 2023 IEEE 6th Int. Conf. on Knowledge Innovation and Invention (ICKII), 2023, pp. 1-6, doi: 10.1109/ICKII59356.2023.10332769.

- S. Yoon, M. Kang, and J. Y. Choi, "Security Attacks Against the Availability of Low Earth Orbit Satellite Networks," in Proc. 12th Int. Conf. on Networks, Communication and Computing (ICNCC), 2023, pp. 64-69, doi: 10.1145/3638837.3638847.

- European Union Agency for Cybersecurity (ENISA), "LEO Satcom Cybersecurity Assessment," Athens, Greece, Rep., Feb. 2024.

- "Satellite Network Attack and Defense Simulation and Visualization Platform," in Proc. ACM Conference, 2025, doi: 10.1145/3759179.3760360.

- "A Survey of Satellite Internet Network Attack and Defense Techniques," in Proc. 2023 Cross Strait Radio Science and Wireless Technology Conf. (CSRSWTC), 2023, doi: 10.1109/CSRSWTC59637.2023.10426896.

- "The Growing Risk of a Major Satellite Cyber Attack," Via Satellite (SatelliteToday). Online. Available: https://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/.