對抗被拿下的整片衛星 –
工控場域之衛星網路防護準則

Yenting Lee, Sr. Threat Researcher
PSIRT and Threat Research, TXOne Networks Inc.
April 17, 2025 @CYBERSEC 2025

Keep the Operation Running

https://www.nasa.gov/

Outline

01 | 衛星網路的應用與架構

- Who is related to the space industry
- Architecture of the space industry

03 | 太空產業的安全策略

- From the U.S., Europe, and Japan
- Manufacturer, controller, and user

02 | 太空產業的攻擊案例

- To Space and Ground sides
- DoS and Hijack attacks

04 | 衛星網路使用者的緩解措施

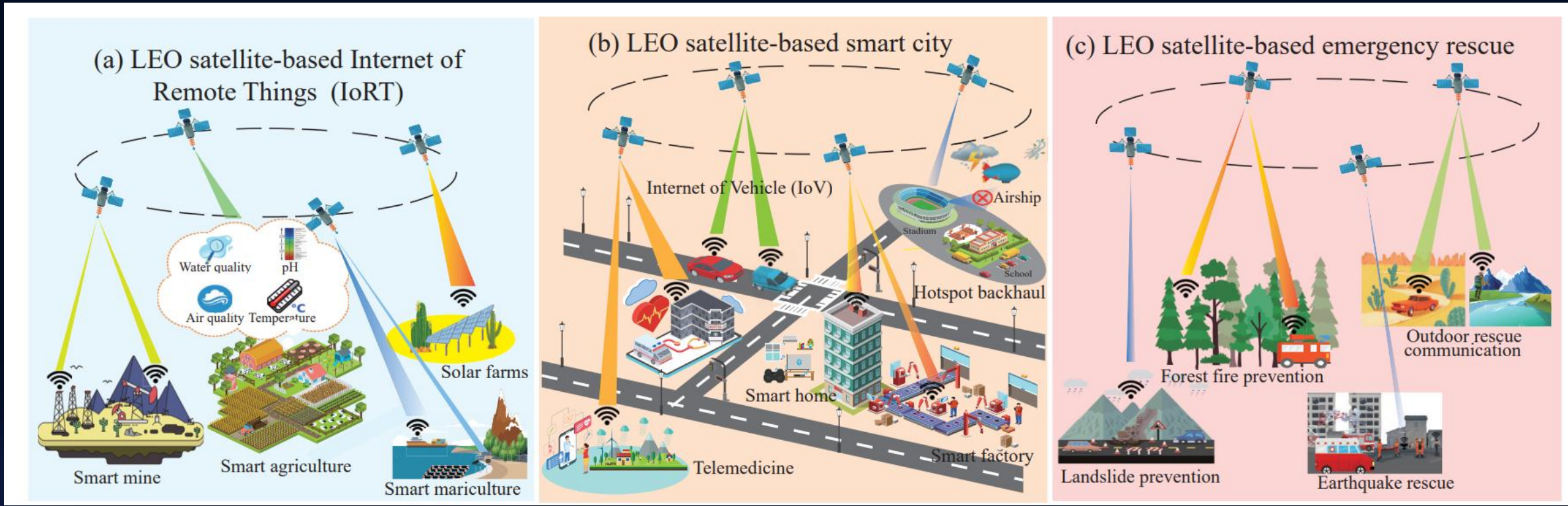
- Cybersecurity guidelines
- Takeaway

衛星網路應用

Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead

Pingyue Yue, *Student Member, IEEE*, Jianping An, *Senior Member, IEEE*, Jiankang Zhang, *Senior Member, IEEE*, Jia Ye, *Member, IEEE*, Gaofeng Pan, *Senior Member, IEEE*, Shuai Wang, *Member, IEEE*, Pei Xiao, *Senior Member, IEEE*, and Lajos Hanzo, *Life Fellow, IEEE*

2023



Keep the Operation Running

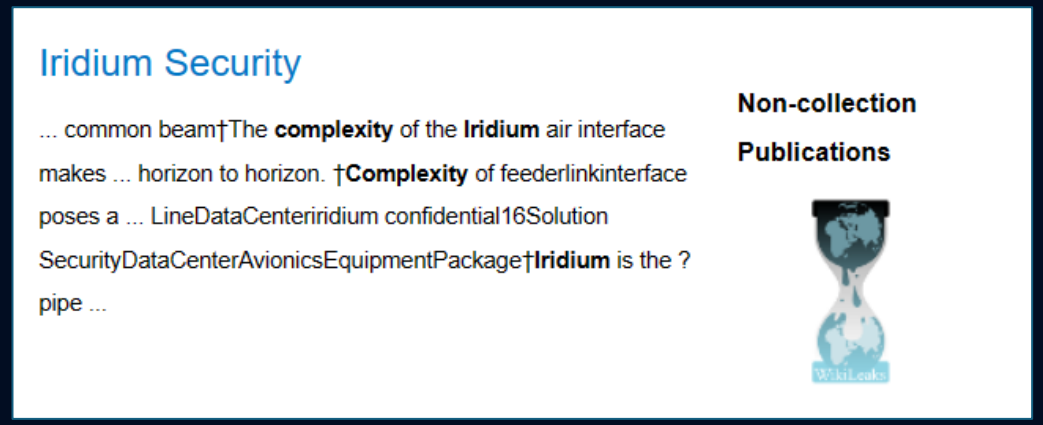
https://ieeexplore.ieee.org/document/10209551

https://www.birdnote.org/listen/shows/black-kites-do-birds-start-fires

衛星網路應用

- 美國與加拿大政府採用低軌衛星作為安全傳輸的解決方案

- (WikiLeaks, 2008) The complexity of the Iridium air interface
  - 硬體限制，攻擊者難以攔截到他們的波段



Keep the Operation Running
https://apps.dtic.mil/sti/pdfs/ADA371120.pdf
https://file.wikileaks.org/file/iridium-security.pdf

衛星網路安全議題

- (2021) PhD Research at Oxford University
  - 攔截真實環境的衛星網路的封包內容

- 效能限制
  - HTTP, FTP, POP3, SMTP, TCP, …
  - TCP hijacking

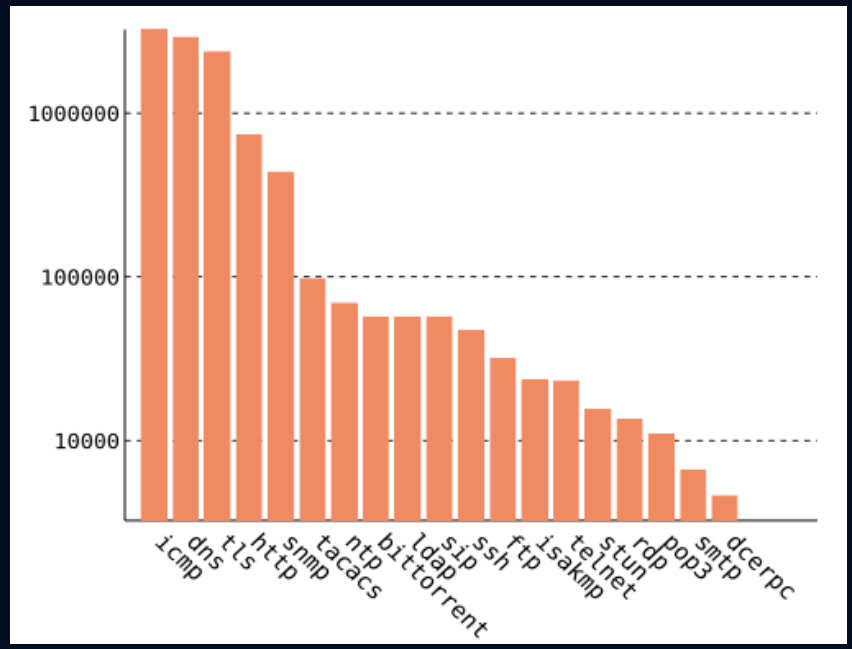
Securing New Space: On Satellite Cyber-Security

James Pavur

Wolfson College
University of Oxford

A thesis submitted for the degree of Doctor of Philosophy

Hilary 2021



https://ora.ox.ac.uk/objects/uuid:11e1b32a-8117-46b1-a0ce-9c485221d112/files/d02870w18z

太空產業資安事件

2008

US

NASA's Terra Earth Observation Satellite: Security Breach

2014

US

Meteorological Satellite System Attack

2015

US EU

Russian Hacker Group Turla exploited commercial satellite systems

US

Iridium Communication Satellite Signals Hacking

2020

US

SolarWinds Supply Chain Attack Impacts NASA and FAA

2022

EU

ViaSat's Satellite Ground Segment Faces Cyber Assault

US

Russia's Fancy Bear Penetrates U.S. Satellite Networks

2023

UKR

Starlink Service Endures Russian Cyberattack and Interference

US

SpaceX Supplier Faces Ransomware Attack

JP

Japan's space agency hit by series of cyberattacks

2024

UKR

War zone GPS jamming sees more ships show up at airports

Satellite

Station

Supply Chain

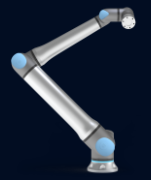
Keep the Operation Running

txOne networks

太空產業架構

Telemetry, Tracking, Command

Supply Chain



Manufacture

Transport

Space Side

GEO 35,786 km

MEO 2,000 - 30,000 km

LEO 300 - 1,500 km

Satellite

connect

TT&C

Uplink

Downlink

Ground Side

Station

Network

Terminals

Controller

Users

txOne networks

多面向的攻擊手法

1. Reconnaissance (BH'20)
2. Privacy: Info Leak by Ku/Ka-band overflow wave (BH'20)
3. TCP Hijack for data manipulation (BH'20)
4. Get O365 (MSFT) OTP to Control ICS and RCE(S&P'20)
5. Space Jam: Use RF attack your VSAT LEO connection (DC'30)

Space Side

1. WebUI password can be leak with physical access (or LEO network) to control the SATCOM system (BH'14)
2. CSP exploits allowed hackers to get RCE with only 10k$ devices (S&P 44th)

```
> Transmission Control Protocol, Src Port: 21, Dst Port: 41573, S
v File Transfer Protocol (FTP)
  v 257 "/Inbox/chartdelivery" is current directory.\r\n
      Response code: PATHNAME created (257)
      Response arg: "/Inbox/chartdelivery" is current directory.
```

TT&C

Uplink

Downlink

$3/min

$30K

SATCOM Provider Ground Side

1. Reconnaissance (BH'20)
2. Privacy: Info Leak by Ku/Ka-band overflow wave (BH'20)
3. TCP Hijack for data manipulation (BH'20)
4. Use only 100$ devices to Hijack Vessel ECDIS / Airline EFB (S&P'20)
5. Space Jam: Use RF attack your VSAT connection (DC'30)

```
<p class=3D"MsoNormal"><span
style=3D"font-family:&quot;Courier
New&quot;;t=
ext-transform:uppercase">THE CARGO MAY
POSSIBLY CONTAIN H2S. THE MASTER AND=
CREW SHOULD THEREFORE ENSURE THAT ALL
PERSONNEL HANDLING CARGO SHOULD BE M=
ADE FULLY AWARE OF THE HAZARDS AND
ADVICE RELATED TO H2S AS OUTLINED IN
THE LATEST EDITION OF ISGOTT. ALL
RELEVANT PRECAUTIO= NS, AS RECOMMENDED
BY THE LATEST EDITION OF ISGOTT, MUST
```

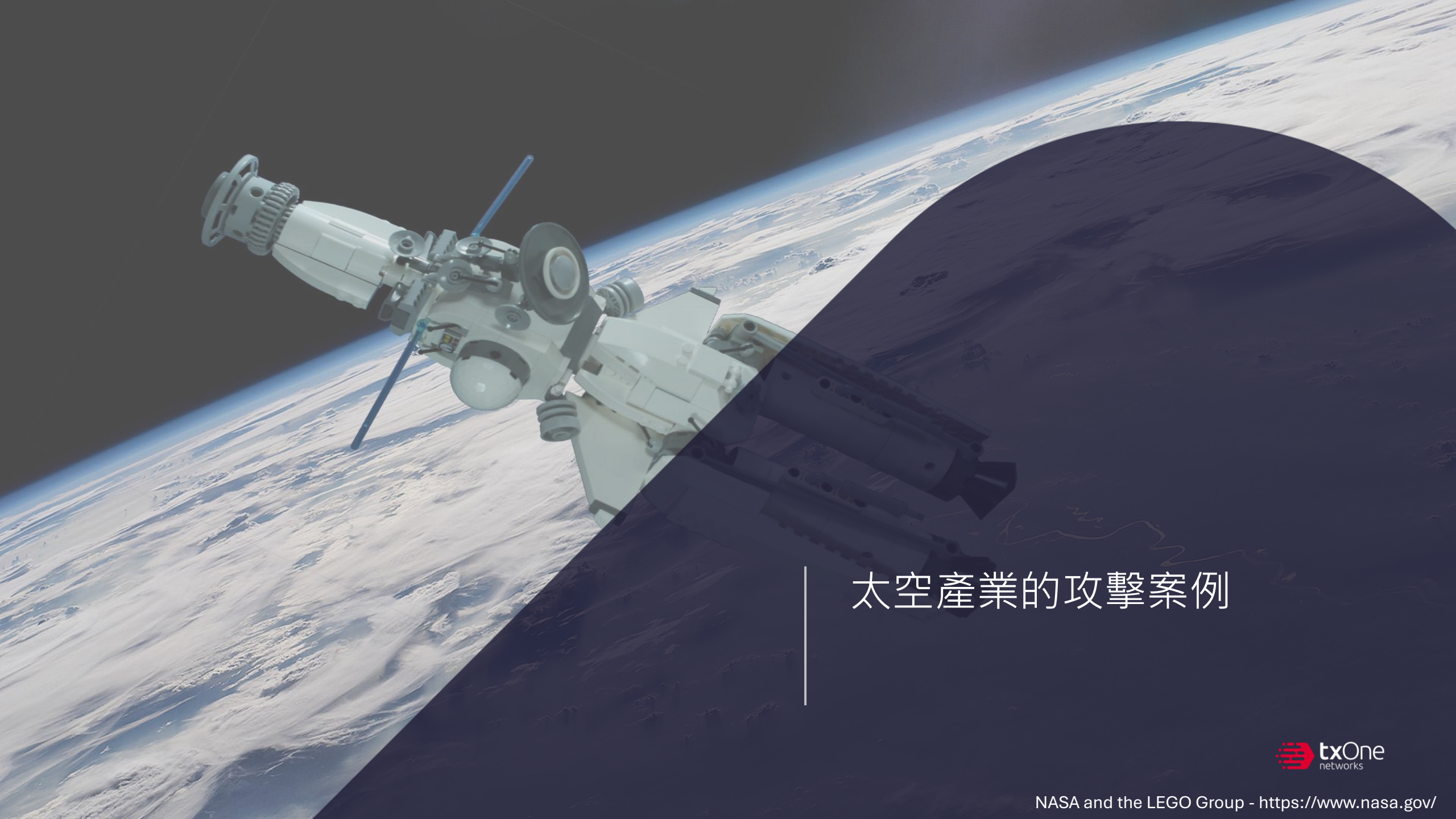
$100

User/ Manufacturing Ground Terminal Side

1. Fault Inject to get Root (BH'22)

Keep the Operation Running

txOne networks



太空產業的攻擊案例

NASA and the LEGO Group - https://www.nasa.gov/

Ground side: 相似於大多的 APT 攻擊

- 衛星網路需求量提升

- 商業考量，採用低成本的製造方式
  - 衛星訊號接收器、數據機

淘宝网
Taobao.com

Keep the Operation Running

https://www.nationalgeographic.com/science/article/space-junk

An APT War: 數據機擦除器阻斷衛星網路服務

- (2022) 俄羅斯 APT28 對美國通訊公司 Viasat 攻擊
  - 該公司提供歐洲衛星網路服務
  - VPN 配置錯誤
- 擦除烏克蘭數據機的韌體 (Modems Wiper)

This article is more than **1 year old**

Viasat spills on the Russian attack, warns of continued risks

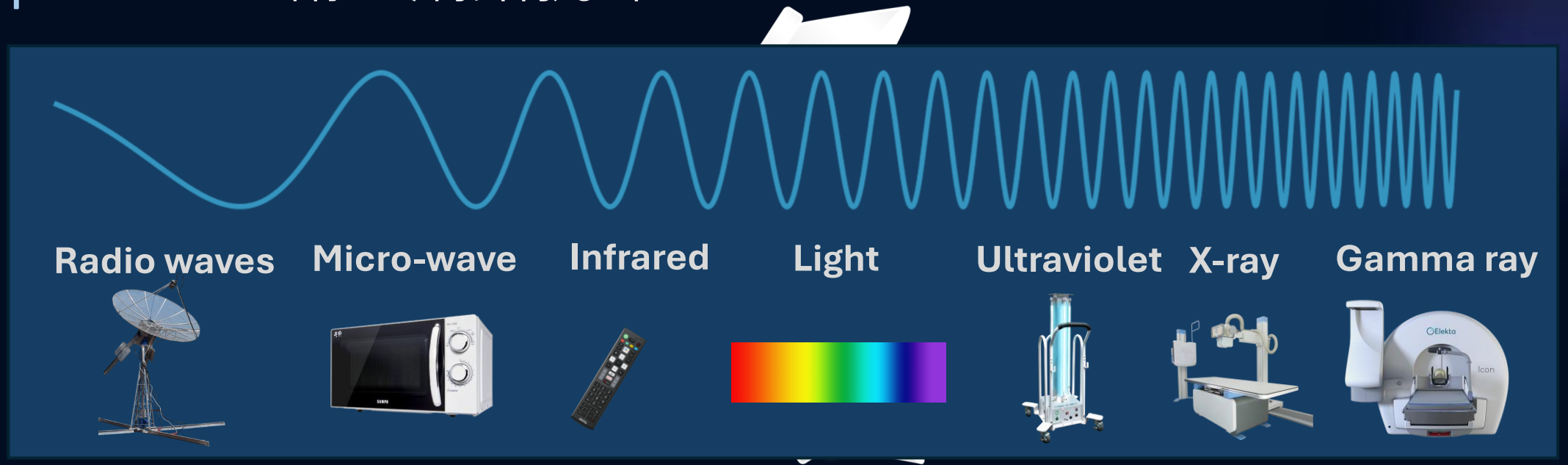
A misconfigured VPN appliance is to blame

Brandon Vigliarolo Wed 30 Mar 2022 // 16:45 UTC

Keep the Operation Running

https://www.theregister.com/2022/03/30/viasat_spills_on_russian_attack/

Space Side: 衛星網路抗噪



- Starlink 提供更快的網路速度
- (2023) Signal Structure of the Starlink Ku-Band Downlink

[Submitted on 20 Oct 2022 (v1), last revised 30 Aug 2023 (this version, v3)]

Signal Structure of the Starlink Ku-Band Downlink

Todd E. Humphreys, Peter A. Iannucci, Zacharias Komodromos, Andrew M. Graff

https://ieeexplore.ieee.org/document/10107477

俄羅斯 Tobol-1

- 烏克蘭採用 Starlink 操作無人機
- Tobol-1 發出 counter-signal 進行干擾

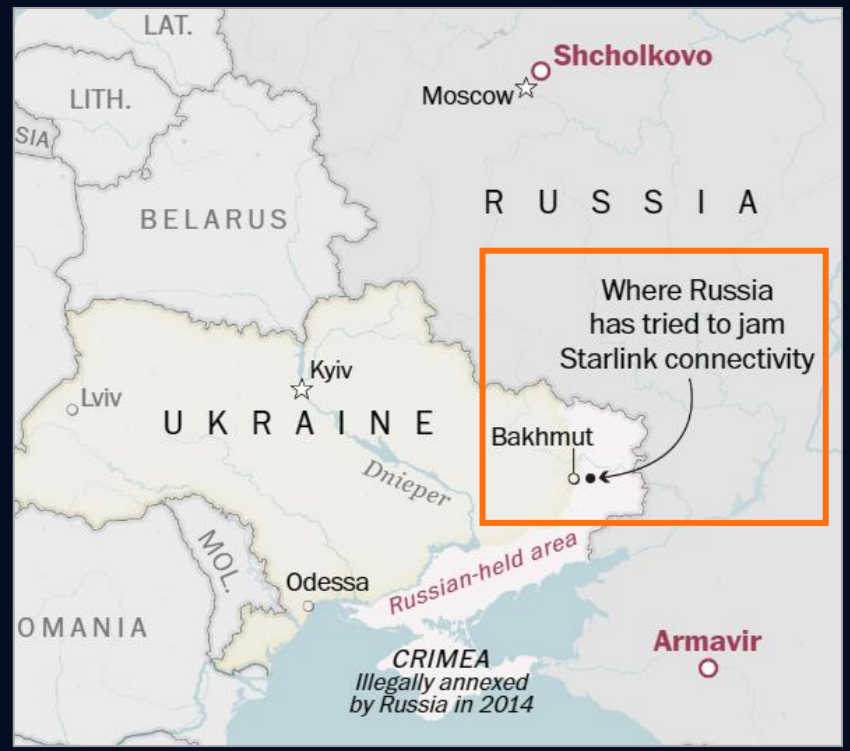
World / Europe

Ukraine relies on Starlink for its drone war. Russia appears to be bypassing sanctions to use the devices too

THE DISCORD LEAKS

Russia tests secretive weapon to target SpaceX's Starlink in Ukraine

THE DISCORD LEAKS | Moscow's bid to sever Ukrainian forces' internet access is more sophisticated than previously known, leaked document shows



A defense?

Keep the Operation Running

https://www.washingtonpost.com/national-security/2023/04/18/discord-leaks-starlink-ukraine/

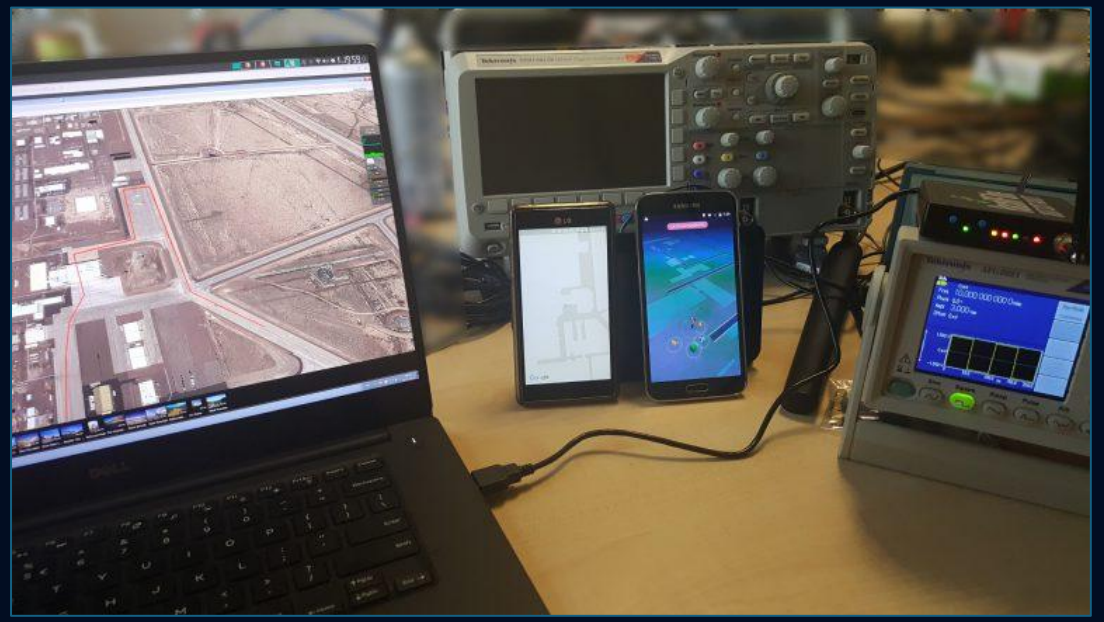
txOne networks

防禦的生活應用

- Pokémon GO
- HackRF tool
  - TWD 10,000

BREAKING July 15, 2016 by Stefan Kiese

Gotta Catch 'Em All! – WORLDWIDE! (or how to spoof GPS to cheat at Pokémon GO)



https://insinuator.net/2016/07/gotta-catch-em-all-worldwide-or-how-to-spoof-gps-to-cheat-at-pokemon-go/


HackRF View
Drone View
H:2.3 M
D:0.1 M
V.S:0.0
Edit View Search Terminal Help
Exiting...
hackrf_close() done
hackrf_exit() done
fclose(fd) done
exit
hackrf_info version: unknown
libhackrf version: unknown (0.5)
Found HackRF
Index: 0
Board ID Number: 2 (HackRF One)
Firmware Version: 2018.01.1 (API:1.02)
Part ID Number: 0xa000cb3c 0x00574762
call hackrf_set_sample_rate(2600000 Hz/2.600 MHz)
call hackrf_set_freq(1575420000 Hz/1575.420 MHz)
call hackrf_set_amp_enable(1)
Stop with Ctrl-C
HackRF One
GREAT SCOTT GADGETS
Spoof GPS
Drone Conetroller
Be forced to terminate
H:-0.2 M
D:N/A
V.S:0.2 M/S
H.S:0

衛星網路劫持

- 衛星網路效能限制

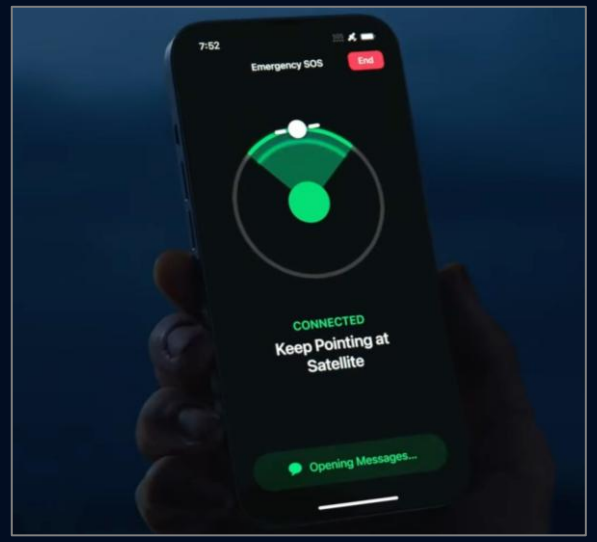
- **Iridium Network** of 66 LEO satellites
  - U.S. DoD & Pentagon: Tracking purposes in logistic
  - 2.4 Kbps, unencrypted and plaintext by default
  - Decrypt on RPi2: *github.com/muccc/iridium-toolkit*

- **GlobalStar Network**
  - Lockheed Martin Flight Service
  - Black Hat USA'15: *"Attacking The Globalstar Simplex Data Service"*
  - iPhone SOS Message

I could spoof Globalstar satellite messages, boasts infosec bod

'We've never been hacked so everything's fine' says hacked firm

John Leyden Wed 5 Aug 2015 // 11:04 UTC



Keep the Operation Running

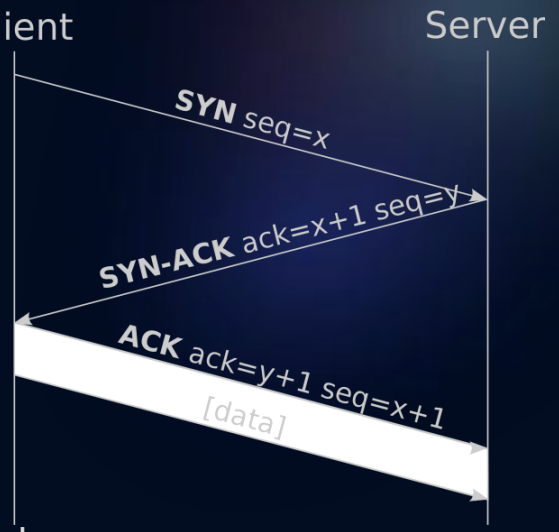
https://www.theregister.com/2015/08/05/globalstar_satellite_comms_hacking/

txOne networks

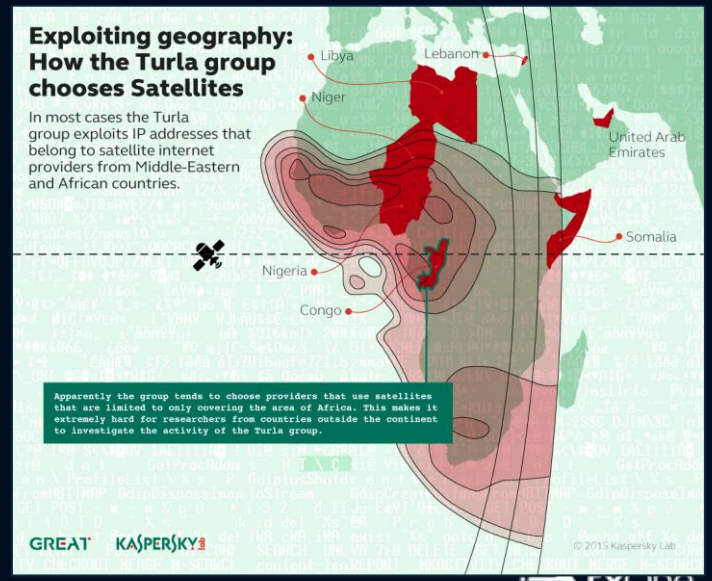
衛星網路劫持

- Black Hat'10 - Hijacking satellite DVB links by S21Sec
  - A satellite dish ~ TWD 10,000
  - A dedicated DVB-S tuner (PCIe card) ~ TWD 3,000

TBS-6922SE PCIe card



- (2015~2020) 俄羅斯 Turla 劫持衛星網路 downstream links
  - 偽造 SYN-ACK 封包給受害者



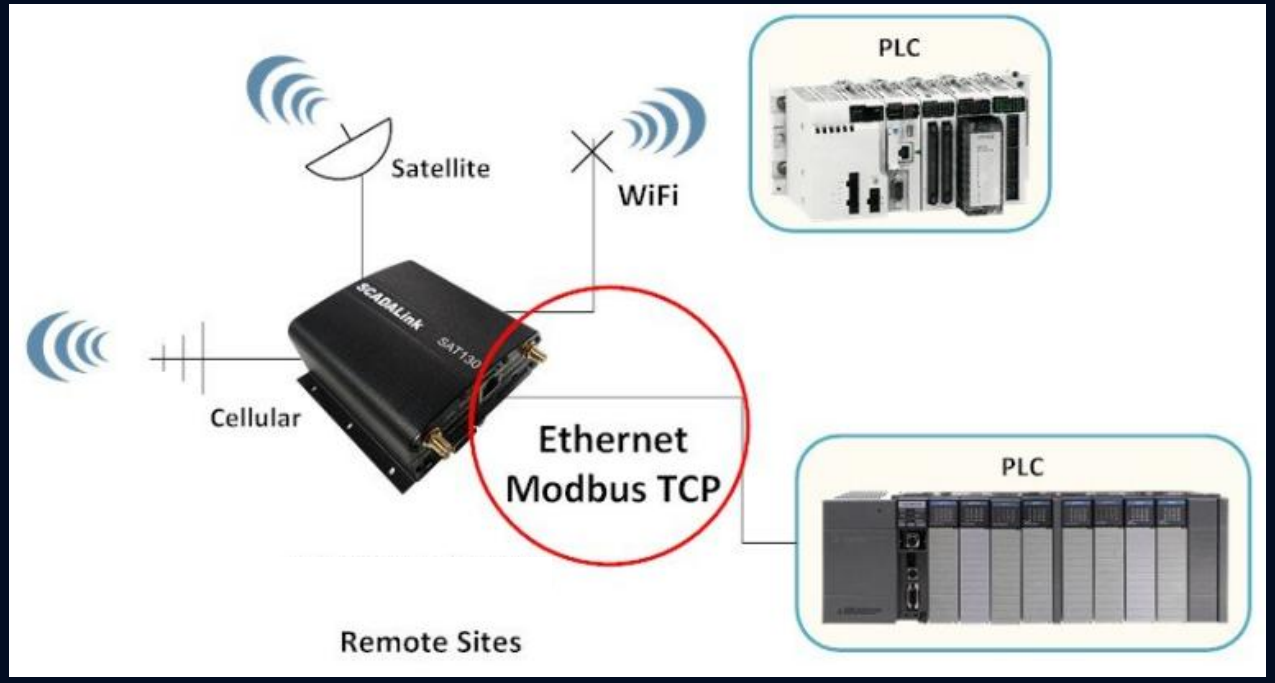
Keep the Operation Running

https://www.spacesecurity.info/en/back-to-turla-or-how-a-russian-speaking-cyber-espionage-group-exploits-satellites/

User Side: OT 解決方案趨勢

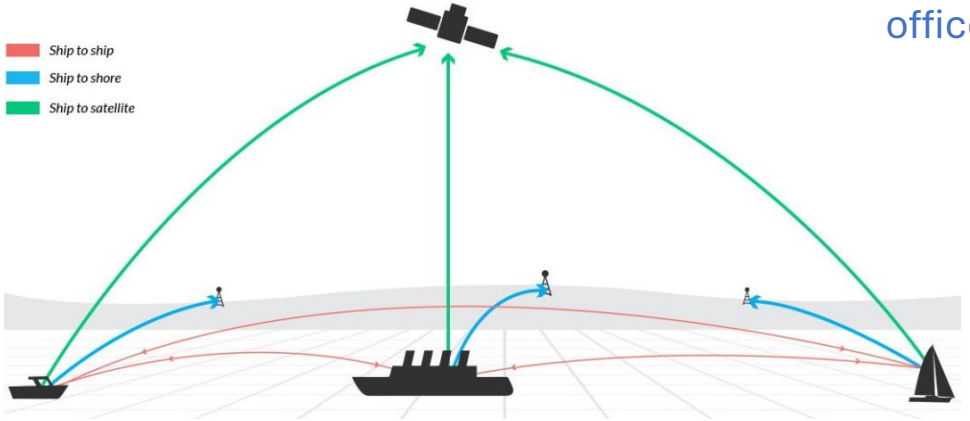
- 與 Modbus TCP 連接，包括 PLC、RTU、…

- 透過 LAN, WiFi, Cellular, and 衛星網路傳遞資料



Communication System

- Use satellite networks to keep in touch with onshore offices and assure safety and operational coordination



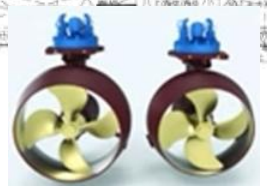
	Inmarsat	Iridium	Globalstar
Speed	2.4-20 Kbps	2.4-20 Kbps	9.6-20 Kbps
GPS	YES	YES	NO

Drone

- Deliver cargo to the vessel
- Quick overview and evaluation of hard-to-reach areas

Automatic Identification System (AIS)

- To receive and provide identification and position information with other vessels/rigs and onshore stations
- Take your position via the vessels' GPS or internal sensors



Dynamic Position System (DPS)

- Receive satellite signal to maintain a constant position above the drilling site

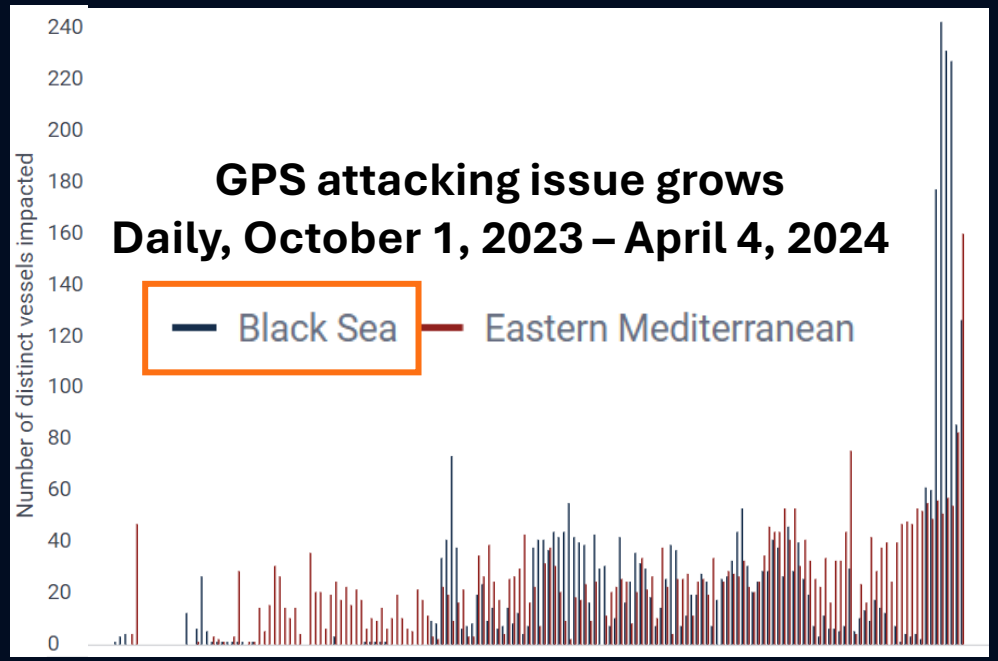
Keep the Operation Running

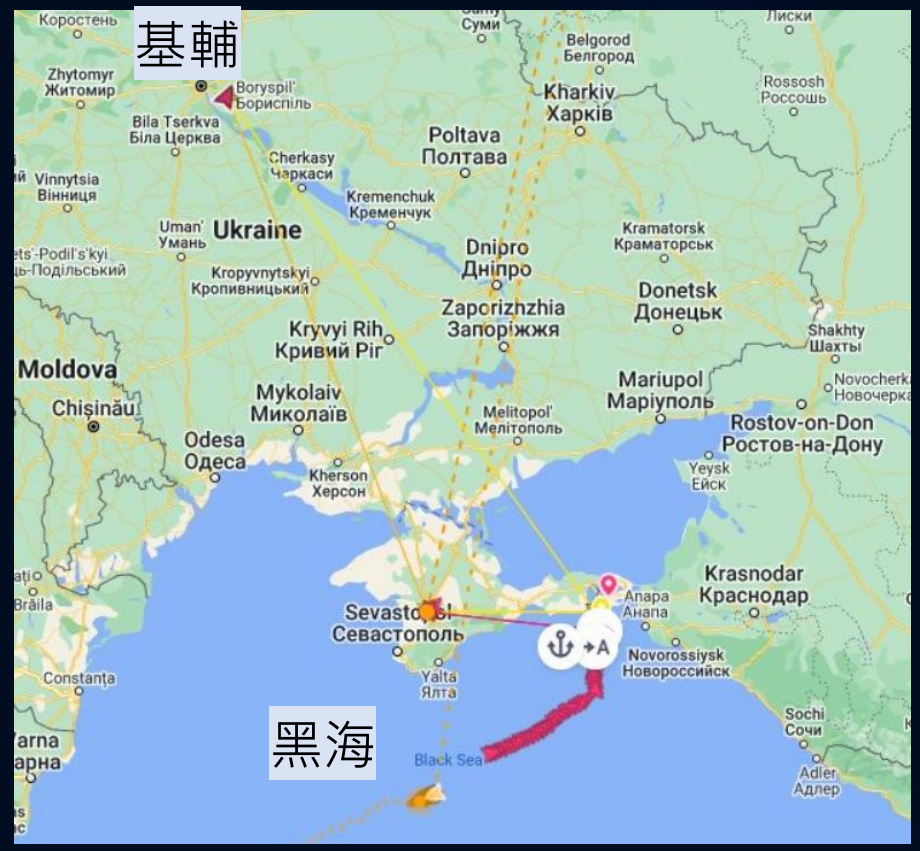
https://www.deepwater.com/documents/RigSpecs/Deepwater%20Champion.pdf

AIS 資料遭受干擾

- APT 組織發射強訊號，導致 AIS 資料受到干擾
- (2023-2024) 俄羅斯試圖在黑海擾亂烏克蘭

受影響船隻數量

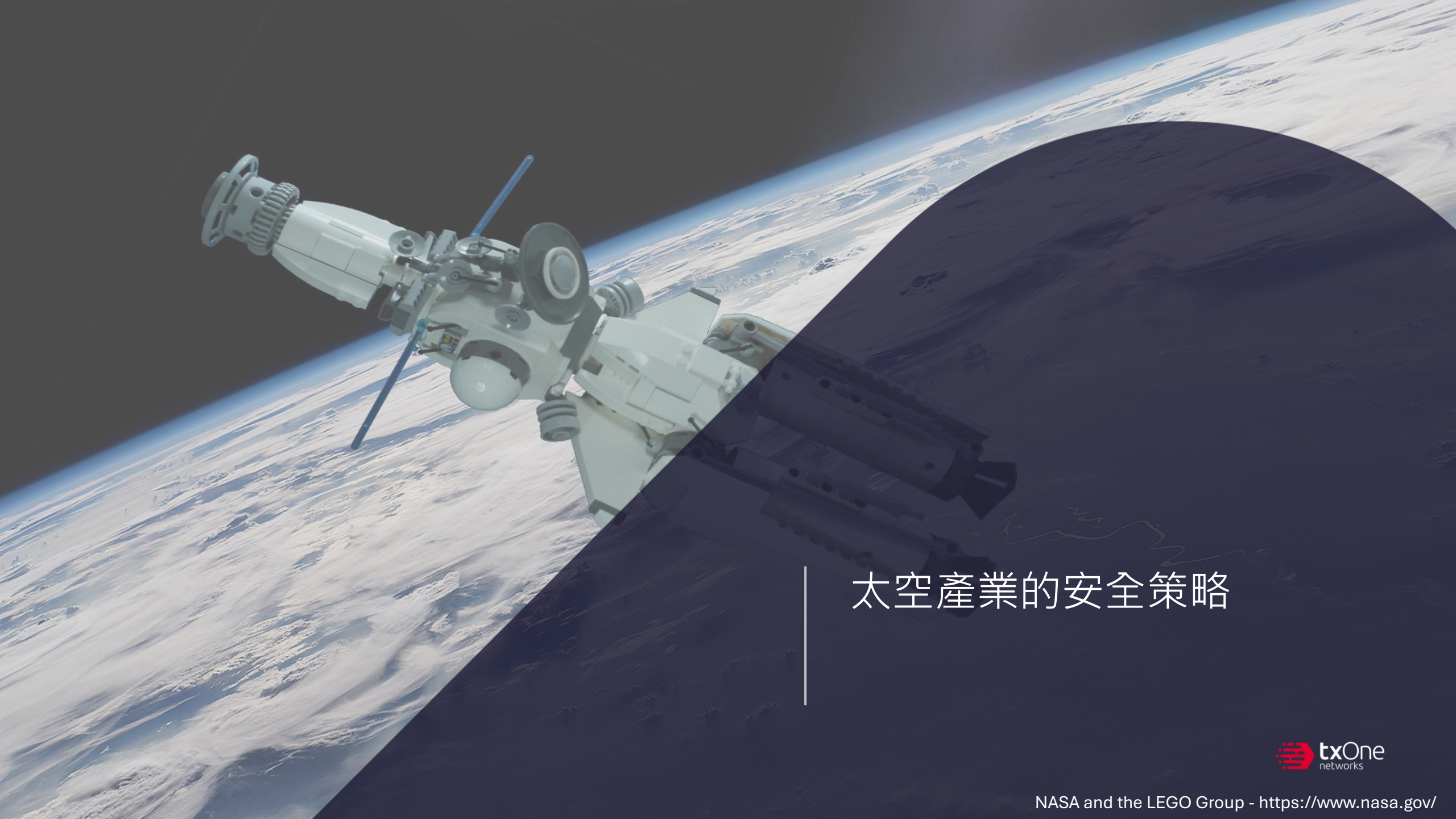




Keep the Operation Running

https://www.lloydslist.com/LL1148748/War-zone-GPS-jamming-sees-more-ships-show-up-at-airports

txOne networks



太空產業的安全策略

txOne networks

NASA and the LEGO Group - https://www.nasa.gov/

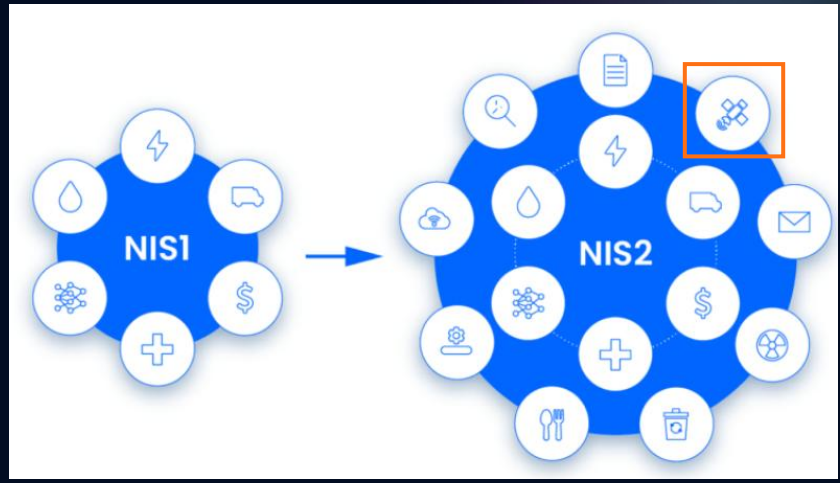
Principles in the U.S.

- (2020) Space Policy Directive-5 (SPD-5)
  - 早已意識到網路安全對太空產業的重要性
  - 白宮發布 SPD-5，重點關注太空系統的網路韌性
  - 定義一個太空系統包含太空飛行器、地面控制網路、使用者
- (2022) CISA's Strengthening Cybersecurity of SATCOM Network Providers and Customers
  - CISA 發布了旨在商業衛星網路的安全指南
  - 提供衛星網路供應商和使用者安全緩解措施
- (2023) NIST-IR-8401 for the space sector's ground systems
  - NIST and MITRE Corp 發布太空部門**地面系統**框架
  - 提供管理網路安全風險的指引

- 涉及範圍是相對廣泛，包含衛星使用者端的網路威脅

Principles in Europe

- (2023) NIS 2 Directive for the space sector
  - 歐盟範圍內的網路安全立法
  - 規範關鍵基礎設施的網路安全要求
    - 通報資安事件、供應鏈管理
  - 具有強制力，違規將面對鉅額罰款
- (2023) BSI TR-03184 for Aerospace Applications
  - 關注衛星網路生命週期的網路安全指南
  - 提供多達 60 項安全措施
- 強制力與細緻程度



ESSENTIAL ENTITIES (EE)

- Includes public and private companies in sectors such as transport, finance energy, water, space, health, public administration, and digital infrastructure
- Fine level: €10MM or 2% of global annual revenue.

Keep the Operation Running

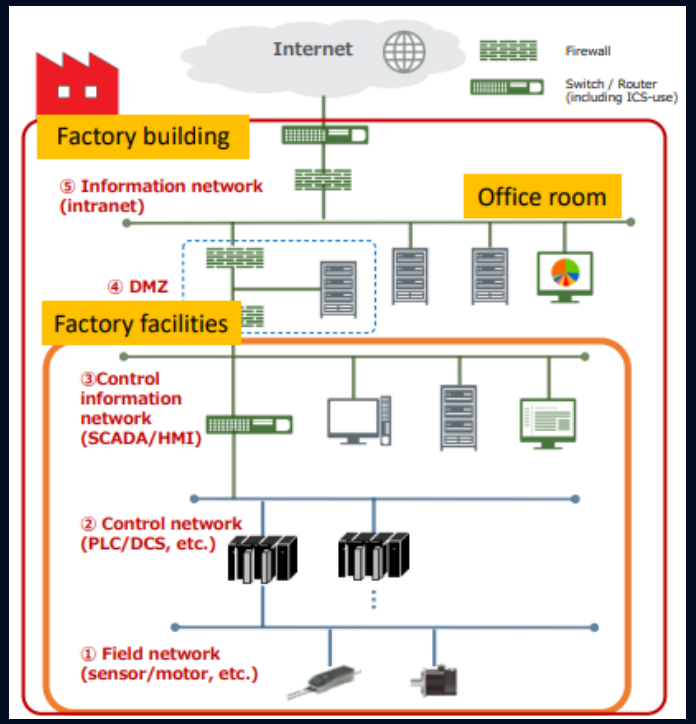
https://nis2directive.eu/nis2-fines/

Principles in Japan

- (2023) JP METI- Cybersecurity Guidelines for Commercial Space Systems Ver. 1.1
  - 經濟部發布商業衛星網路指南
  - 涵蓋衛星系統的設計、開發、製造、運作、維護和處置階段

Commercial space system		Phase to be covered in the lifecycle			
		Design, development and manufacturing	Launch	Operations and maintenance	Disposal
Satellite	Remote sensing satellite	✓	-	✓	✓
Satellite operation facility	Tracking and control station, receiving station and mission control system, etc.	-	-	✓	✓
Satellite data utilization facility	Data processing systems, observation reception and data distribution processing, etc.	-	-	✓	✓
Launch facility	Launch site, launch control facility, etc.	-	-	-	-
Development and manufacturing facility	OT system (FA system, etc.)	✓	-	✓	✓
	IT system (OA system, etc.)	✓	-	✓	✓

- 針對衛星製造工廠，提供 OT 網路安全概念



Country	Principle	Manufacturer	Controller	User
	(2020) Space Policy Directive-5	V	V	V
	(2022) CISA's Strengthening Cybersecurity of SATCOM Network Providers and Customers	X	V	O (1 content)
	(2023) NIST-IR-8401 for the space sector's ground systems	X	V	X
	(2023) NIS 2 Directive for the space sector	V	V	X
	(2023) BSI TR-03184 for Aerospace Applications	V	V	V
	(2023) JP METI- Cybersecurity Guidelines for Commercial Space Systems Ver. 1.1	V	V	X

OT 使用者端網路安全參考指南

Principle
(2020) Space Policy Directive-5
(2022) CISA's Strengthening Cybersecurity of SATCOM Network Providers and Customers
(2023) NIST-IR-8401 for the space sector's ground systems
(2023) NIS 2 Directive for the space sector
(2023) BSI TR-03184 for Aerospace Applications
(2023) JP METI- Cybersecurity Guidelines for Commercial Space Systems Ver. 1.1

OT 使用者端

資安管理

- Integrity check
- Malware scan
- Support logging
- … (6)

端點防護

- Vulnerability protection
- Protect against changes
- … (7)

網路防護

- Roles and rights
- Use of IDS/IPS systems
- … (7)

資安管理

- Integrity check of the supply chain
- Conduct malware/vulnerability scan before asset is introduced
- Documentation of assets and its components
- Support logging and auditing functions
- Determination and implementation of an applicable cybersecurity standard at the supplier
- Use Cyber Threat Intelligence to prevent known threats

產品的完整性檢查、盤點、安全日誌、威脅情資

端點防護

- Measures to protect against tampering in the system
- Conduct malware/vulnerability scan regularly
- Use virus protection programs/update regularly
- Implementation of a roles and rights principle in the system
- Implementation of logging and auditing principle in the system
- Guidelines for password security
- Change tracking/documentation for system

權限最小化原則、使用防毒、系統變更追蹤

NIS 2 Directive Reporting Obligations -
Essential and important entities must have processes in place for prompt reporting of security incidents with significant impact on their service provision or recipients

網路防護

- Use of IDS/IPS
- Use of separate, task-specific networks
- Implementation of a roles and rights principle between equipment
- Implementation of logging and auditing principle in the network
- Use encrypted communication if possible
- Documentation of Network configuration
- Communication with the satellite in several communication channels

使用多種通訊頻道的衛星通訊、
使用網路防護設備、系統變更追蹤

Takeaway

- 太空產業同時面對針對性的 APT 攻擊與隨機性的攻擊
  - 過去研究人員所發現多面向的攻擊手法，已實際應用在真實環境中
  - Space Side, Ground Side, Supply Chain

- 即使各國已越來越重視太空產業的網路安全，但仍側重於衛星製造商與衛星控制端

- OT 使用者端網路安全參考指南
  - 資安管理 (6)
  - 端點防護 (7)
  - 網路防護 (7)

- The Final Frontier: Fortifying Cyber Resilience for the Commercial Space Industry


txOne
networks