Nation State Cyber Attacks Against Space Infrastructure: Toward a Techno-Political Future Risks Model

Space infrastructure, such as Global Navigation Satellite Systems (GNSS), provide vital positioning, navigation and time services on which many critical industries rely. These include the energy grid, stock market and GPS apps on our phones. This criticality makes it vulnerable to disruptive nation state level cyber attacks.

My research investigates why and how nation states attack space infrastructure, as well as how threats might evolve. I approach the issue with technical cyber attack analysis, political document analysis and interviews and futures thinking methods.

Jessie Hamill-Stewart
Supervised by Dr. Andre Barrinha (University of Bath) and Prof. Awais Rashid (University of Bristol)

Jessie.hamill-stewart@bristol.ac.uk
LinkedIn Jessie Hamill-Stewart
Twitter @jessie_hamills

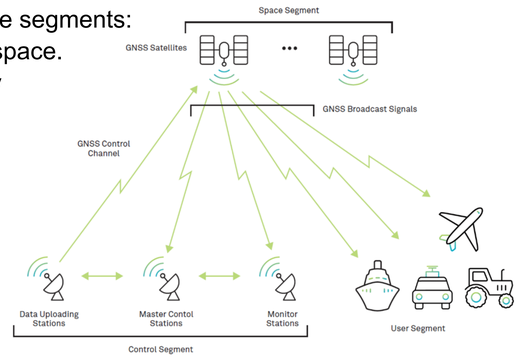
Background:

A sophisticated attack against space infrastructure would highly disrupt society.

In fact, the Centre for the Protection of National Infrastructure considers space to be Critical National Infrastructure.

Despite its criticality, space infrastructure, such as GNSS, is vulnerable to cyber attacks due to wide attack surface and multiple attack types.

1. GNSS have three segments: ground, user, and space. They provide many attack vectors.



2. This wide attack surface makes space systems vulnerable to a variety of attacks.

For instance, users are vulnerable to jamming and spoofing, amongst other threats.

Finland reports GPS disturbances in aircraft flying over Russia's Kaliningrad

The interference began soon after a mee Sauli Niinistö and Joe Biden

Reuters in Helsinki

Wed 9 Mar 2022 18.26 GMT

Seized UK tanker likely 'spoofed' by Iran

GPS spoofing involves ships' receivers being tricked with counterfeit satellite automatic identification signals generated to gain control of a navigation system. This can take the vessel off course or show it in a different location

16 Aug 2019 | NEWS

How Stena Impero veered off-course

Current Project:

1. Cyber Attack Analysis

Project: Analysing attacks and incidents within ground infrastructure of satellite systems in order to develop a theory to help understand this phenomenon.

Aims
- Develop a theory of cyber attacks against satellite system ground infrastructure.
- Assist with the placement of defensive measures.
- Increase technical knowledge on cyber attacks against space infrastructure.

Methodology
- Technical cyber attack analysis (ground infrastructure of satellite systems) and GTM.

Europe's version of GPS suffers major outage

By Bianca Britton, CNN Business
Updated 9:59 AM EDT, Mon July 15, 2019

US, UK and EU blame Russia for 'unacceptable' Viasat cyberattack

Carly Page @carlypage_ / 1:54 PM GMT+1 • May 10, 2022

Comment

Sources:
Russia suspected of jamming GPS signal in Finland - BBC News https://www.bbc.co.uk/news/world-europe-46178940
Seized UK tanker likely 'spoofed' by Iran :: Lloyd's List (informa.com) https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran
Above+Us+Only+Stars.pdf (squarespace.com) https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf
What are Global Navigation Satellite Systems? | NovAtel https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss
Galileo: Europe's version of GPS suffers major outage | CNN Business and US, UK and EU blame Russia for 'unacceptable' Viasat cyberattack | TechCrunch

Upcoming Projects:

2. Political Analysis

Project: Analysis of astropolitical, domestic and international political factors which increasingly motivate nation states to conduct disruptive cyber attacks against space infrastructure.

Aims
- Demonstrate the strategic gain of nation state cyber attacks.
- Provide new insights regarding astropolitics of the world order.

Methodology
- Qualitative thematic analysis of policy documents relating to state space policies.
- Interviews to highlight important cyber attack threats.

3. Evolution of Threats

Project: Development of a techno-political future risks model to help anticipate future threats against space infrastructure, drawing upon technical and political analysis.

Aims
- Develop a model to assist consideration of future threats against space infrastructure.
- Help space industry sector prepare for sophisticated cyber attacks.

Methodology
- Futures thinking methodologies, such as horizon scanning and writing scenarios.

HM Government – National Space Strategy September 2021 (publishing.service.gov.uk)
france_-_space_defence_strategy_2019.pdf (gouvernement.fr)
https://bandiasi.almaviva.it/sites/default/files/attach/dettaglio/dvs-ing_web.pdf