Homeland Security

Economic Security Mission Center

Space: Conflict and Consequences

Updated: 14MAY22

Agenda

- **Geopolitics: Russia-Ukraine Conflict**
  - **Cyber Attacks**
  - **Electronic Attacks**
  - **Implications**
- **Other Geopolitical Actors**
- **Enduring Threats**
  - **Cybersecurity**
  - **Insider Threats**
  - **Physical Security**
  - **Supply Chain**
- **Mitigation: Cybersecurity Best Practices and Resources**

Russia/Ukraine

Not Deployed:

- Kinetic Antisatellite (ASAT) Weapons
- Cyber attack on Space Segment

Deployed:

- Cyberattacks
- Electronic attacks
- Sanctions/Countersanctions

This Photo by Unknown Author is licensed under CC BY

Space System Attack Vectors

Segments Vulnerable to Cyberattack

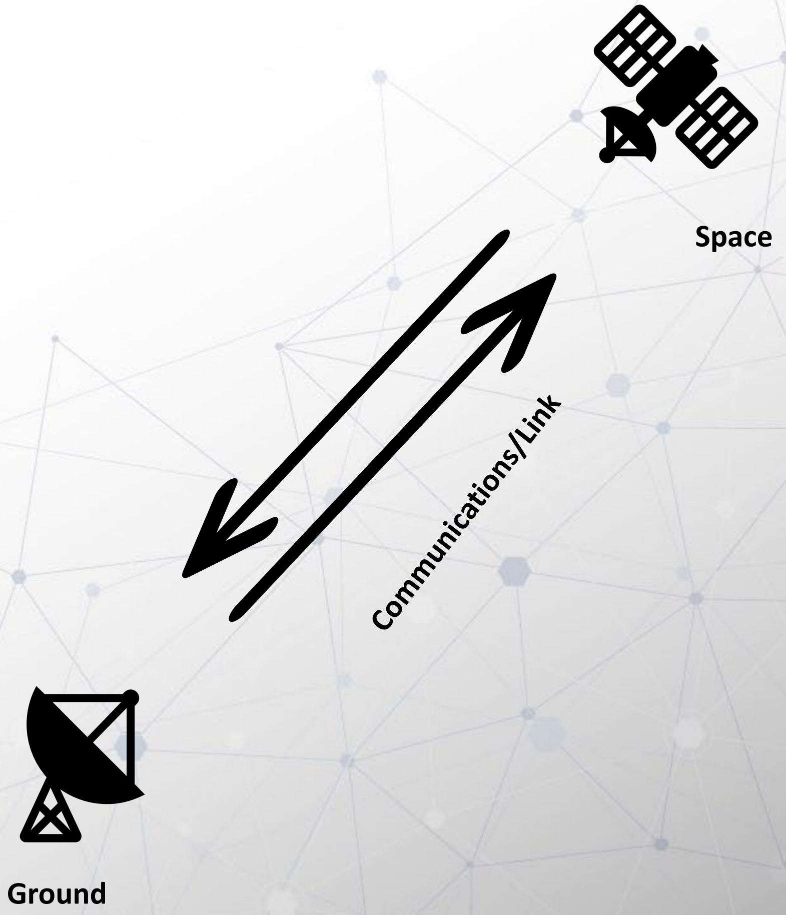
- Ground
- Space
- Link

Vulnerable Owners/Operators:

- Government
- Military
- Commercial

Russia/Ukraine Conflict:

- Ground
- Link



Russia/Ukraine: What We Have Seen

- Cyber Attacks
  - Targeted Ground Segment
  - Space-based assets not targeted
  - Damaging Spillover Effects outside of conflict zone
- Electronic Attacks
  - Targeted Link Segment
  - Signal Spoofing
  - Signal Jamming
  - Damaging Spillover Effects outside of conflict zone

Cyber Attack

Cyberattack in Conflict Zone:

- Spillover effects reaching as far as Morocco
    - 27,000 customers Impacted
- Energy infrastructure sector impacted
    - Long-lasting
    - Open to follow-on attack by different malicious cyber actors
- Potential Damage:
    - Reputational (company and sector)
    - Financial (company)
    - Economic (sector)

Electronic Attack

Electronic Attack In Conflict Zone:

- Signal Spoofing
- Signal Jamming

Spillover effects in Europe and Israel

- Transportation Sector (aviation)
- Communications Sector (provider)

Aviation industry impacted

- Planes grounded up to a week
- Planes diverted mid-air

Communication sector impacted

- Company redirected resources
- Potential delays to other business projects

Sanctions/Countersanctions

Space enterprise is interconnected

- March 2021: Russia Launched 38 spacecraft from 18 different countries on a single Soyuz rocket
- March 2022: Russia is isolated, due to sanctions and its reaction to them.

Impacts:

- ExoMars Rover Research Mission Postponed
- OneWeb launch canceled; forced to find alternate launch provider
- Rocket engine delivery to US Defense Contractors and others canceled
- Delayed launches of the following:
  - One reconnaissance satellite
  - Four Galileo PNT satellites
  - Multiple scientific research satellites

Future Conflict

Current conflict does not guarantee similar outcomes in future conflict.

Different actors have different calculus.

Different actors have different counterspace/cyberspace capabilities:

- **China: Kinetic + Cyber**
- **North Korea: Jamming/Spoofing + Cyber**
- **Iran: Cyber**

Enduring Threats

- Not exclusive to space industry
- Not limited to nation-states
  - Cyber criminal groups
  - Insider Threats
  - Lone wolves
- Can take the following forms:
  - Weak cybersecurity practices
  - Insider threats
  - Lax Physical Security
  - Supply Chain Vulnerabilities

Cybersecurity

- Imperative to have strong cybersecurity at every stage of space system/space asset development and deployment.

- Malware, ransomware, denial of service: some common types that have affected aerospace/defense sector.

- Reversible and irreversible cyberattacks.

- Insider threats and lax physical security can have a compounding effect on cyberattacks.

- Jurisdictional issues impact cybersecurity and can create additional cybersecurity vulnerability.

Supply Chain

- Many organizations involved in development and deployment of space system/asset.
- Shared components/vendors
- Increases cyber vulnerability

This Photo by Unknown Author is licensed under CC BY

Resources for Mitigation

CISA.GOV

QUESTIONS?