

# Tech Brief:

## VULNERABILITY OF COMMERCIAL SATELLITE INTELLIGENCE NETWORKS TO HOSTILE ATTACK

Paul Struhsaker  
Arrasar Partners

[www.struhsaker.com/arrasar-partners](http://www.struhsaker.com/arrasar-partners)

# Introduction

2

“Through the first two weeks of the invasion, the Ukrainian government received data covering more than 15 million square miles of the war zone<sup>1</sup>”

[Astronomy - War in the Ukraine highlights Importance of private satellite companies](#)

The conflict has thus been dubbed the first “commercial imagery space war,” highlighting the value of commercial satellite imagery to augment national security – as well as the power of transparency and collaboration between allies’ space capabilities

[SpaceNews - On National Security | Drawing lessons from the first ‘commercial space war’](#)

# The Small Sat Revolution ushered in commercial EO/SAR The War in Ukraine Forged them into an Intelligence Network

- On February 20<sup>th</sup> 2022 Russia invaded Ukraine
  - The U.S. and our allies provided Ukraine not only Military Assistance, they also provided Intelligence Assistance
  - However, Security concerns limited Ukrainian access to the U.S.'s most Secret Satellite Intelligence Assets
  - Alternate Sources of real-time intelligence were required ASAP
- Enter DARPA, the NRO, Ukrainian ingenuity, and others to cobble together a commercial version of military C4I system:
  - Synthetic Aperture Radar (SAR) Satellites (All Weather) - strategic surveillance
  - Imaging Satellites including infrared imaging- strategic surveillance
  - SpaceX StarLink satellite network - real-time communications
  - Local UAV imaging drones for tactical surveillance (w/ "Delta" battlefield intel)
  - Home grown Ukrainian "GIS Art for Artillery" command and control APP
  - Ukrainian rebuild of NATO battlefield-awareness platform
  - US and NATO Alliance precision weapons (& Air Defense Systems, e.g. Patriot )



Starlink SatCom Terminal



ICEeye SAR LEO satellite

# From Commercial Stopgap to Military Backup

4

- The Effectiveness of LEO commercial satellites in Ukraine accelerated US military/intelligence community planning to use these systems as backup Mil/Intel satellite networks
- Three types of satellite constellations have proven their value:
  - Earth Observation (EO) in the visible and Infrared spectrum
    - Hyperspectral EO is also emerging
  - Synthetic Aperture Radar - SAR for all weather capability
  - Communications - Starlink is a game changer
    - Russia destroyed much of Ukraine's wired/fiber and cellular infrastructure at the start of the war
    - Despite significant Electronic Warfare efforts by Russia - Starlink is the backbone of Ukrainian military communications
- The hybrid commercial<> military is now embraced by military for communications is now expanding into Optical EO & SAR
  - NRO, DARPA, & USSF have an array of contracts awarded or in process to be awarded



# With dual use, the threat to commercial systems begins: Starlink under constant Cyber and Jamming Countermeasures

5

“On 15 October 2022, amidst Ukrainian counteroffensives in the Battle of Donbas, Russian forces reportedly disrupted a Ukrainian Starlink system in the Soledar-Bakhmut area after they destroyed a shortwave repeater”

The Institute for the Study of War. October 15, 2022

“Cyberattacks against Starlink appear to have been ineffective, in part because SpaceX quickly updates the system’s software”

“How Elon Musk's satellites have saved Ukraine and changed warfare”. The Economist

Tech Brief: Vulnerability of Commercial Satellite Intelligence Networks to Hostile Attack- P Struhsaker, Arrasar Partners

Starlink - Artist Concept



Russian  
Krashuka-4  
Jammer

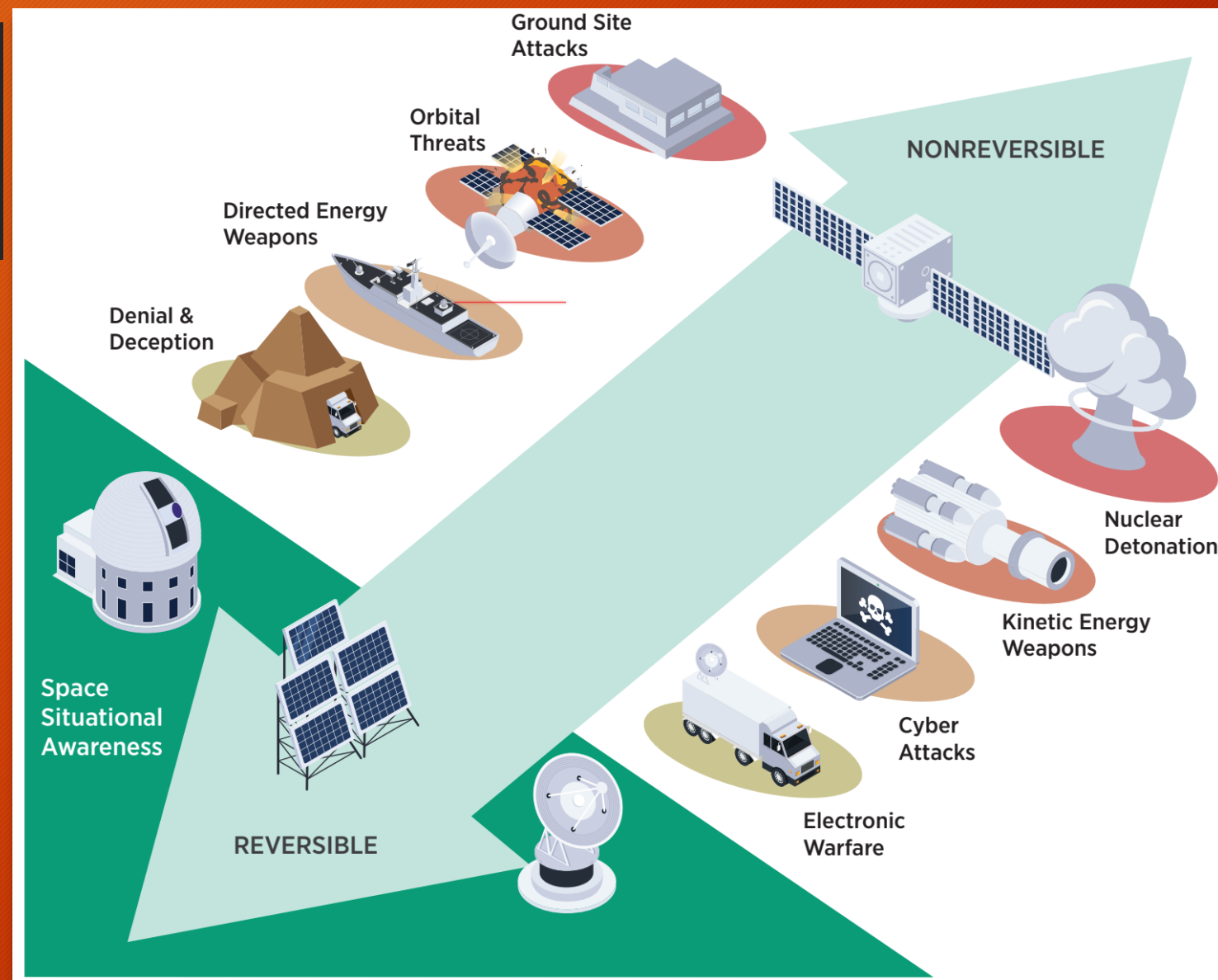


# Threats to Commercial Intelligence Satellites

6

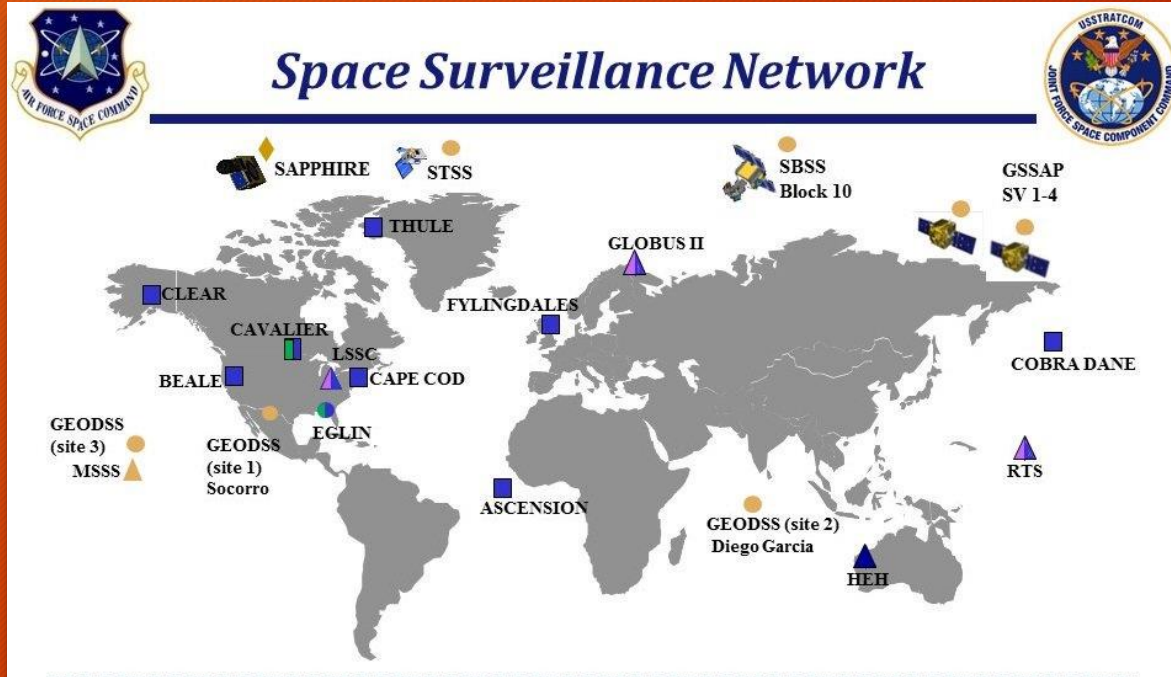
# The Counterspace Threat Continuum

- Current satellite threats
  - Kinetic Energy Weapons
  - Cyber Attacks
  - Electronic Warfare
  - Ground site attacks
  - Denial and Deception
- Commercial and Military “Space Situational Awareness systems”
  - Threat Assessment
- Future satellite threats
  - Orbital threats
  - Direct energy weapons



# Situational Awareness/ Space Surveillance

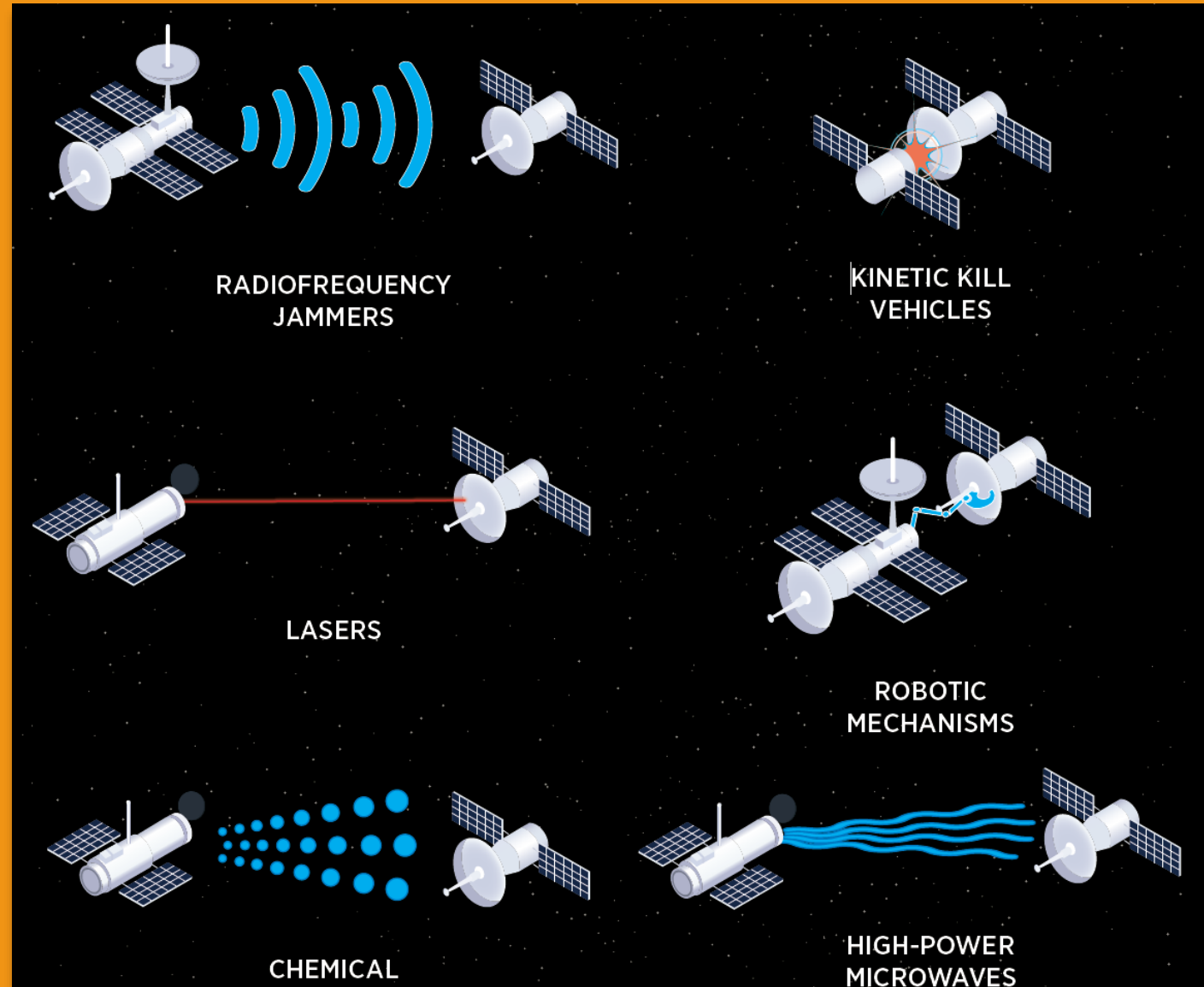
- **Space Awareness Goal:**
  - Tracking of any and all launches & deployed objects
  - Detect intentional or unintentional collisions or near pass events in time to take evasive maneuvers
- **Military and Commercial Systems**
  - US Space Surveillance Network
    - Ground and space based assets
  - LEO Labs
    - Developing a network of 20 S-Band and UHF Phased Array Radars
    - Track objects as small as 2 cm
- **Critical is detecting threats and confirming source of harmful anti-satellite activity**





# Emerging Orbital Threats

- Evolving capabilities for satellite-on-satellite destructive or reversible threats
  - Reversible RF Jamming / Optical Dazzler
  - Destructive high power Laser / High-power microwaves (EMP)
  - Destructive chemical/paint spray - highly degrade solar cells - energy starvation
  - Mechanical Capture - tow out of orbit or capture and return (“Skyhook”)
- Orbital anti-satellite can be effective against large expensive military satellite networks with small constellation
- Limitations of Orbital threats:
  - Economics: Launch and vehicle cost on par with target Space Awareness allows defensive
  - Space Awareness allows for Defensive maneuvering as a countermeasure



# Current and Expanding Threats

10

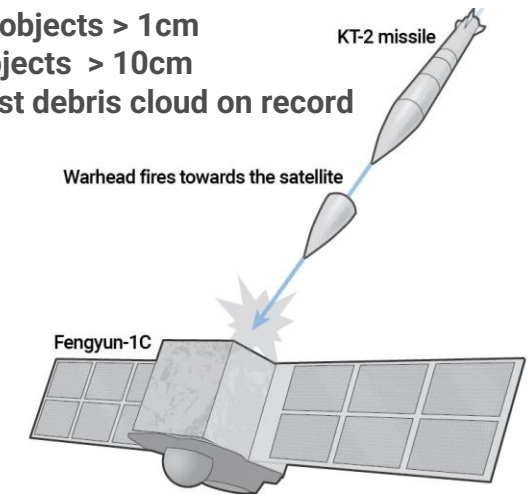
# Anti-Satellite Kinetic Energy Weapons

- China, Russia, and US have fielded Kinetic Anti-satellite weapons
  - Ground based ASAT missile
  - Space based Kinetic Kill Vehicle
- A few examples:
  - Intentional anti-satellite weapons tests (ASAT missile)
    - Example KT-2 missile & Fengyun-1C weather satellite
  - Kinetic Kill Vehicle - accidental Collision between satellites
    - Example Iridium 33 and Cosmos 251

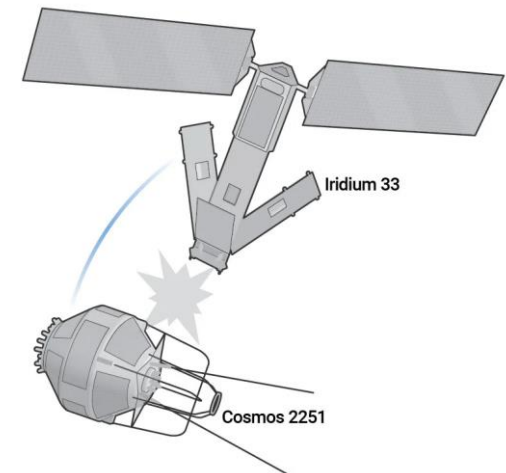
## Major Drawback to Kinetic Weapons:

Debris fields generated cause unintended harm to friendly and enemy satellites

2007, China tests an anti-satellite missile  
300K objects > 1cm  
3K Objects > 10cm  
Largest debris cloud on record

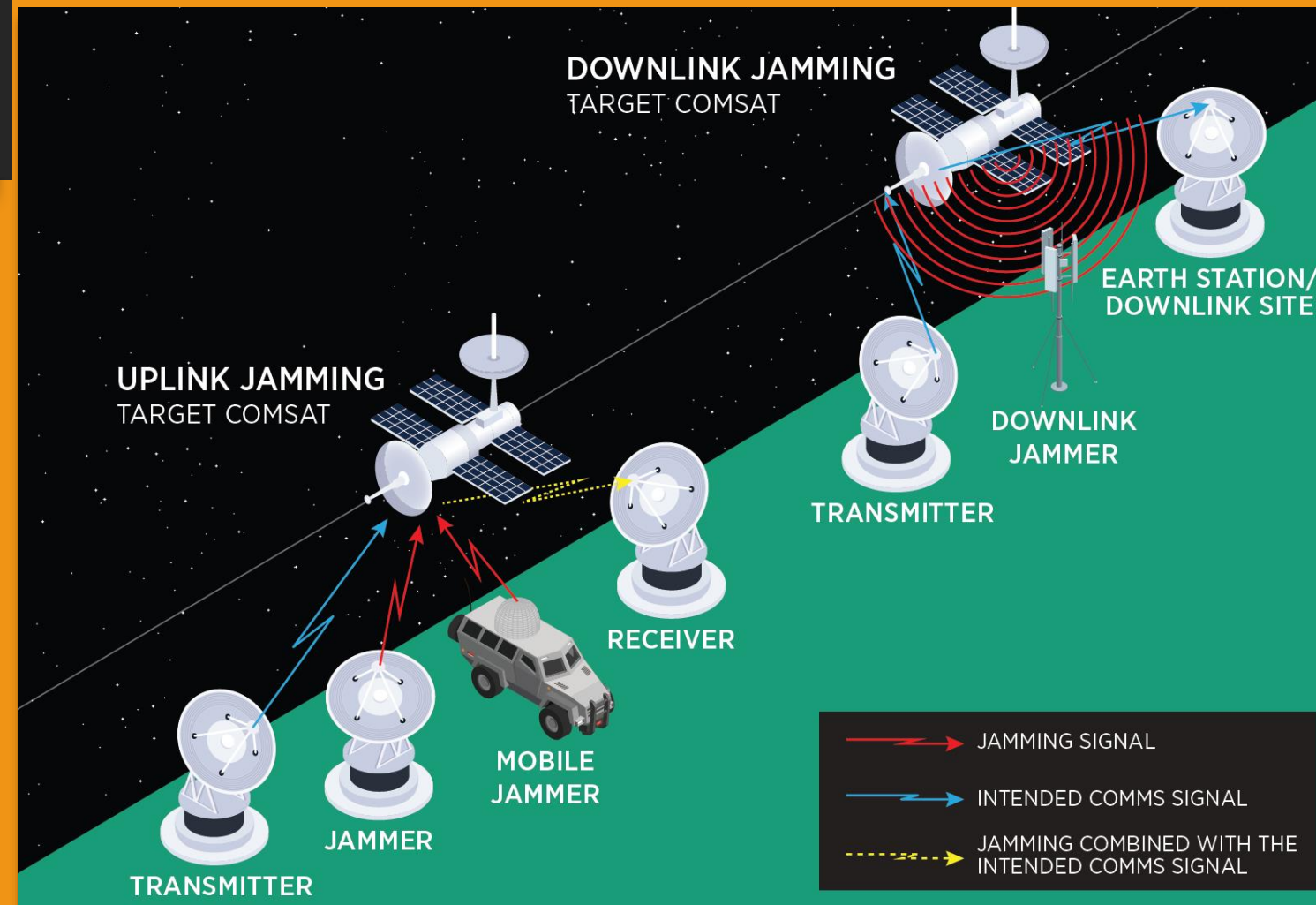


February 10, 2009 first Satellite Collision  
~2k Objects > 10cm created



# Satellite System Jamming

- Ground Based Jamming is effective against:
  - Communications satellite Up and Down Links
  - Earth Observation data down links
- Ground Based Uplink Jamming
  - Pure Jamming fixed and mobile
  - Intelligent Jamming - Spoofing/Corrupt mimic of Uplink Signal
- Downlink Jamming
  - Saturate Earth Station receiver
  - Jam through the side lobes of the receiver antenna



Defense Intelligence Agency- Jamming Scenarios

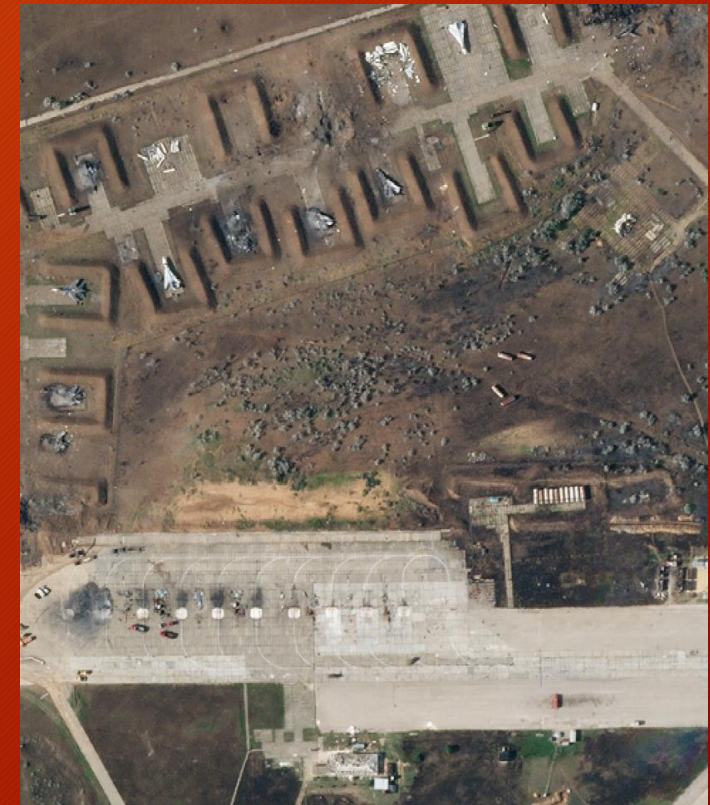
# LEO Earth Observation (EO) Example: Saki Air Base Crimea

13

- Open Source/Commercial satellite intelligence
  - Multiple Constellations of EO satellites
  - Providing real-time and near real-time monitoring
  - Resolution approaching 0.15M
- Intelligence provided:
  - Troup/asset movement
  - Targeting
  - Post attack BDA (Bomb Damage Assessment)



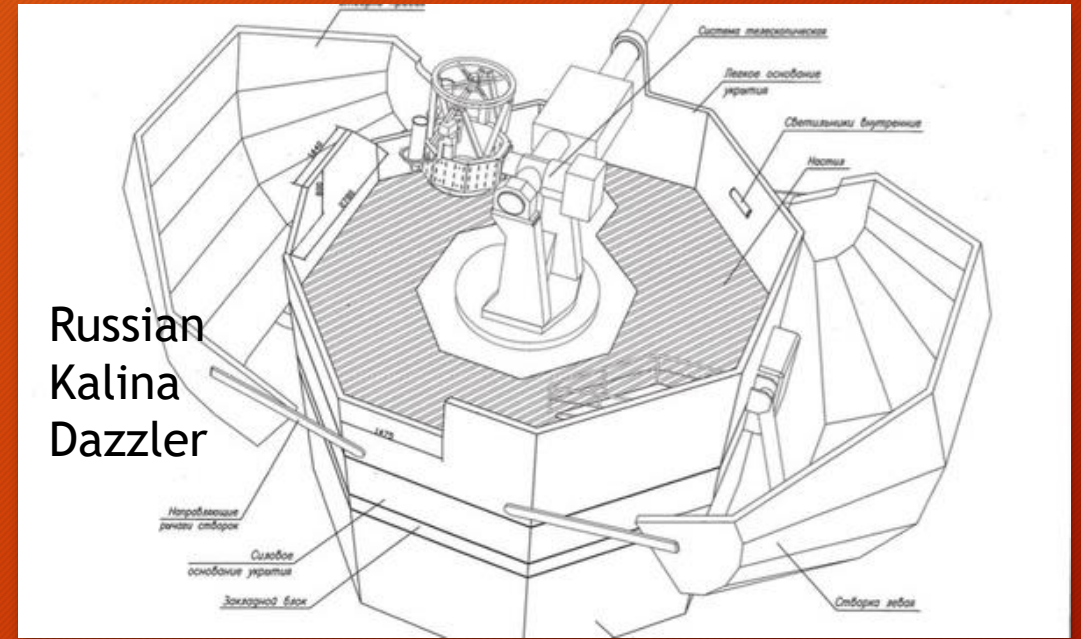
August 9 2022 (prior to Attack)



August 10 2022 (Post Attack)

# Countering EO satellite intelligence: Ground based Laser for Dazzling or Blinding

- Laser operations can be broadly classified into 3 categories, ranging, dazzling, and blinding.
  - Ranging is used for Satellite Situational Awareness - Tracking (LIDAR)
  - “Dazzlers,” are lasers designed to temporarily blinding optics systems or EO satellites
  - Blinding is the act of permanently damaging or destroying a satellite’s sensor with a laser
- Russia developing several facilities
  - Bohu Laser Facility (Dazzling and Blinding)
  - Krona space surveillance complex - Kalina Dazzler
- US has its own facilities and capabilities
  - Starfire Optical Range - Kirkland AFB



## “Quantity has a quality all its own” - Joseph Stalin

- The sheer volume of LEO EO/SAR/COMM constellations create Tactical and Strategic reserve for Intelligence gathering
  - It is not physically or economically viable to suppress with space based weapons
  - A ground based antisatellite arms race is underway for this very reason
- MEO/GEO government strategic satellite platforms
  - In the near term distances exceed ground based weapon effective range
  - Space Based Weapons are both a physically and economically viable against these satellite platforms
- Kinetic Anti-satellite weapons should be avoided
  - Create long term extended collateral dangers for Friend and Foe

# Thank You

Questions/Comments Contact: [paul@struhsaker.com](mailto:paul@struhsaker.com)

Visit the Arrasar Web Page: [www.struhsaker.com/arrasar-partners](http://www.struhsaker.com/arrasar-partners)

PDF download available at: [www.struhsaker.com/dystopic-science-stories](http://www.struhsaker.com/dystopic-science-stories)