



THE FIRST SHOTS FIRED IN
FUTURE CONFLICTS WILL BE IN
CYBERSPACE AND SPACE

WILLIE SHELTON

The background features a gradient from deep purple on the left to bright blue on the right. Overlaid on this are several concentric circles and arcs. A prominent white arc is visible in the upper right, while other thinner, semi-transparent arcs are scattered throughout. Small white dots are also present, adding to the abstract, digital aesthetic.

CYBERSPACE

China

“The PRC remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks.”

“If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.”

Russia

“Russia’s advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat.”

“Moscow’s unique strength is the practical experience it has gained integrating cyber attacks and operations with wartime military action, almost certainly amplifying its potential to focus combined impact on U.S. targets in time of conflict.”

Annual Threat Assessment of
The U.S. Intelligence Community
2025

SUCCESSFUL CYBER ACTIVITY

-
- 2007, Russia attacks Estonia government, banking and media
 - 2009, Lockheed Martin targeted by China for F-16 data
 - 2010, Stuxnet takedown of Iranian centrifuges
 - 2015, Russia attacks Ukraine power grid (also 2016 and 2022)
 - 2024, China cyber attacks increased 150% against Southeast Asia and Taiwan
 - Ongoing, Ransomware attacks

UNITED STATES CYBER COMMAND

Direct, Synchronize, and Coordinate Cyberspace Planning and Operations - to Defend and Advance National Interests - in Collaboration with Domestic and International Partners.

- Commander of USCYBERCOM & Director of the National Security Agency
- Title 50 vs. Title 10
- All Services have cyber forces
- Continuous cyber activity, warfighting readiness

The background features a gradient from deep purple on the left to bright blue on the right. Overlaid on this are several concentric circles and arcs. A thick white arc is visible in the upper right and lower left. Several thinner, light blue arcs and small circles are scattered throughout the composition, creating a sense of depth and movement.

SPACE

China

“China has eclipsed Russia as a space leader and is poised to compete with the United States as the world’s leader in space by deploying increasingly capable interconnected multi-sensor systems and working toward ambitious scientific and strategic goals.”

“Counterspace operations will be integral to PLA military campaigns, and China has counterspace-weapons capabilities intended to target U.S. and allied satellites. China already has fielded ground-based counterspace capabilities, including EW systems, directed energy weapons (DEWs), and antisatellite (ASAT) missiles intended to disrupt, damage, and destroy target satellites.”

Russia

- “Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities. It is expanding its arsenal of jamming systems, DEWs, on-orbit counterspace capabilities, and ASAT missiles designed to target U.S. and allied satellites. Despite its Soviet legacy, the war in Ukraine has revealed glaring deficiencies in Russia’s space-based architecture.”

○ “Moscow uses its and others’ civil and commercial remote-sensing satellites to supplement military-dedicated capabilities and has warned that other countries’ commercial infrastructure in outer space used for military purposes can become a legitimate target.”

Russia Part 2

- “Russia is developing a new satellite meant to carry a nuclear weapon as an antisatellite capability.”

“A nuclear detonation in outer space could cause devastating consequences for the United States, the global economy, and the world in general. It would harm all countries’ national security and commercial satellites and infrastructure, as well as impair U.S. use of space as a driver for economic development.”

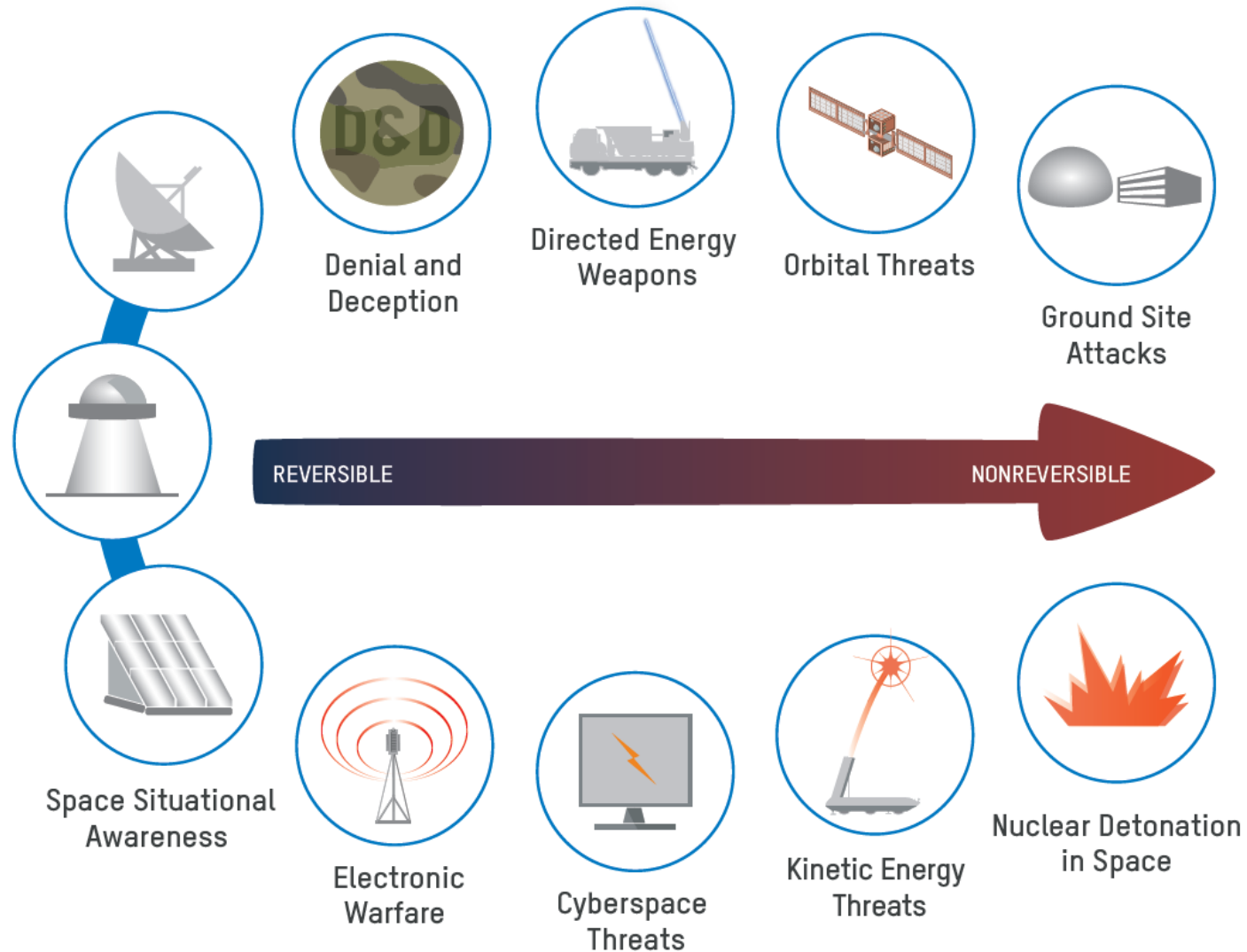
Annual Threat Assessment of
The U.S. Intelligence Community
2025

And then there were others...

“It is a wise thing to also have your own resources in case of contingencies or in case of complications in geopolitical spheres.”

Hermann Ludwig Moeller, Director, European Space Policy Institute
2025

THREATS TO SPACE SYSTEMS





Monjes del Sur

Aruba

Curaçao

Amuay and Cardon Refineries

Punto Fijo

Coro

Cerro el Avila

Fort Tiuna

Caracas

Maracay

Puerto La Cruz

MUSCAR gas complex

Maturin

Maracaibo

Valledupar

Merida

Barinas

Cúcuta

Bucaramanga

Venezuela

Guri Dam/hydroelectric plant

Ciudad Bolívar

Guayana City

St Vincent and the Grenadines

Grenada

Trinidad and Tobago

GPSJAM

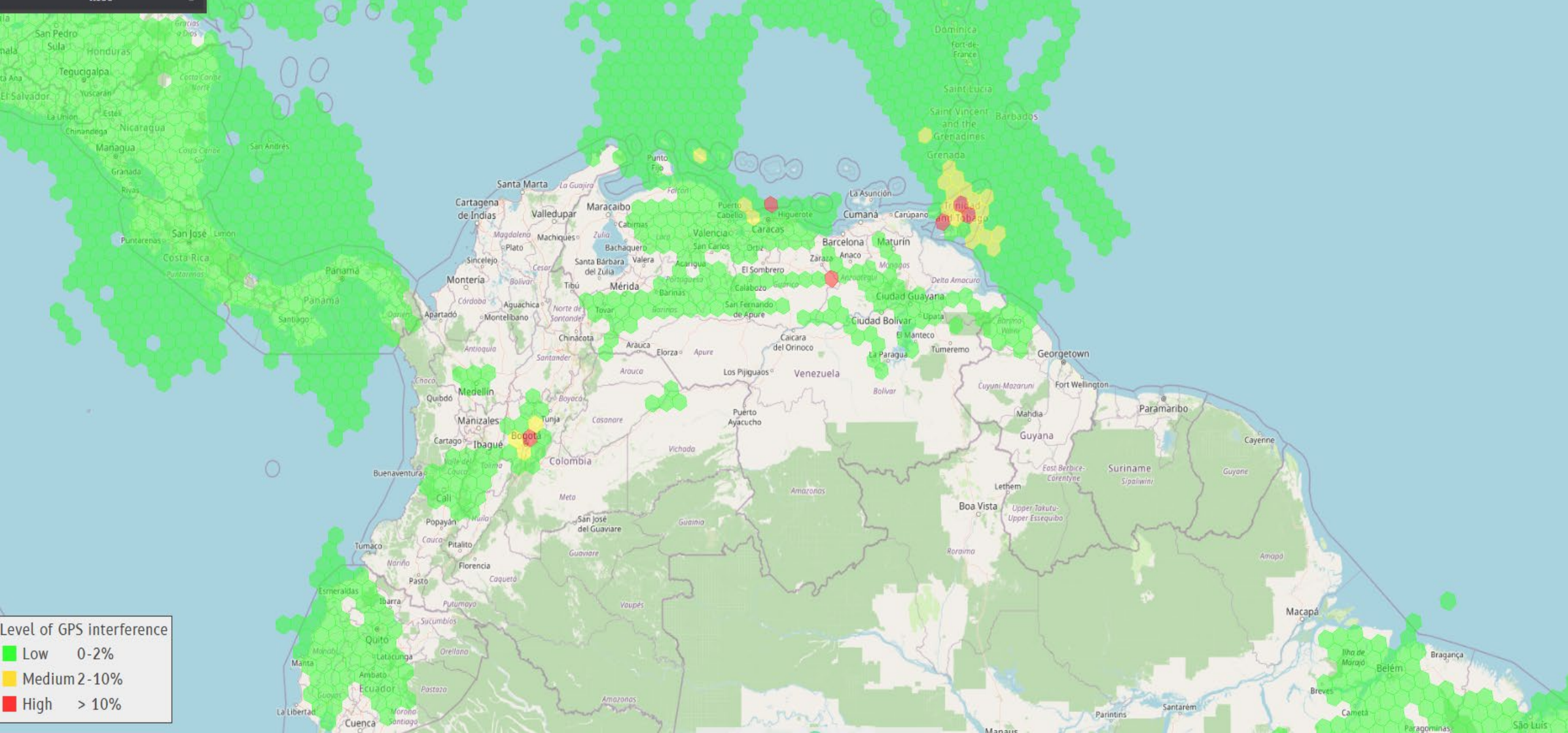
Daily maps of GPS interference

[About](#) | [FAQ](#)

12/30/2025



More



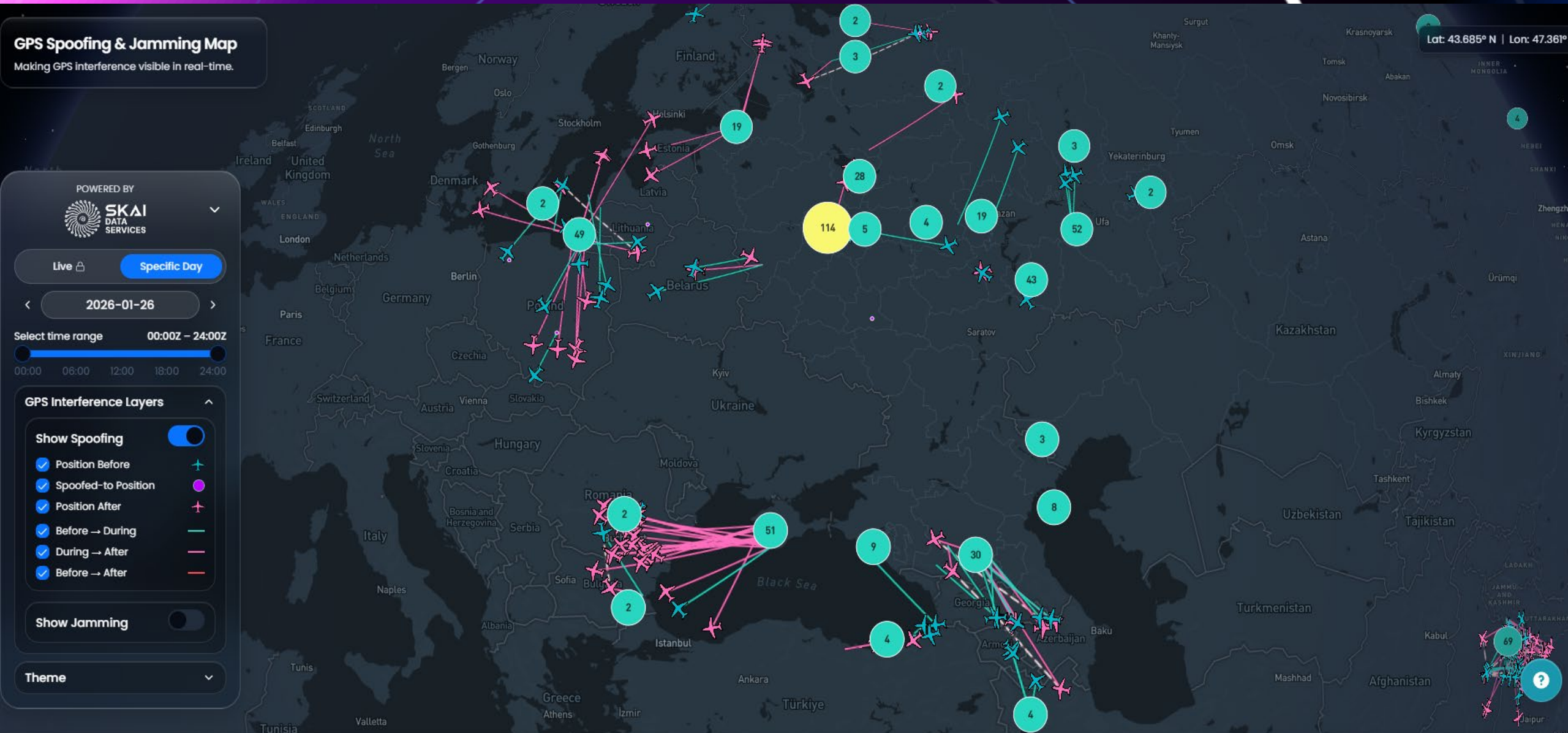
Level of GPS interference

Low 0-2%

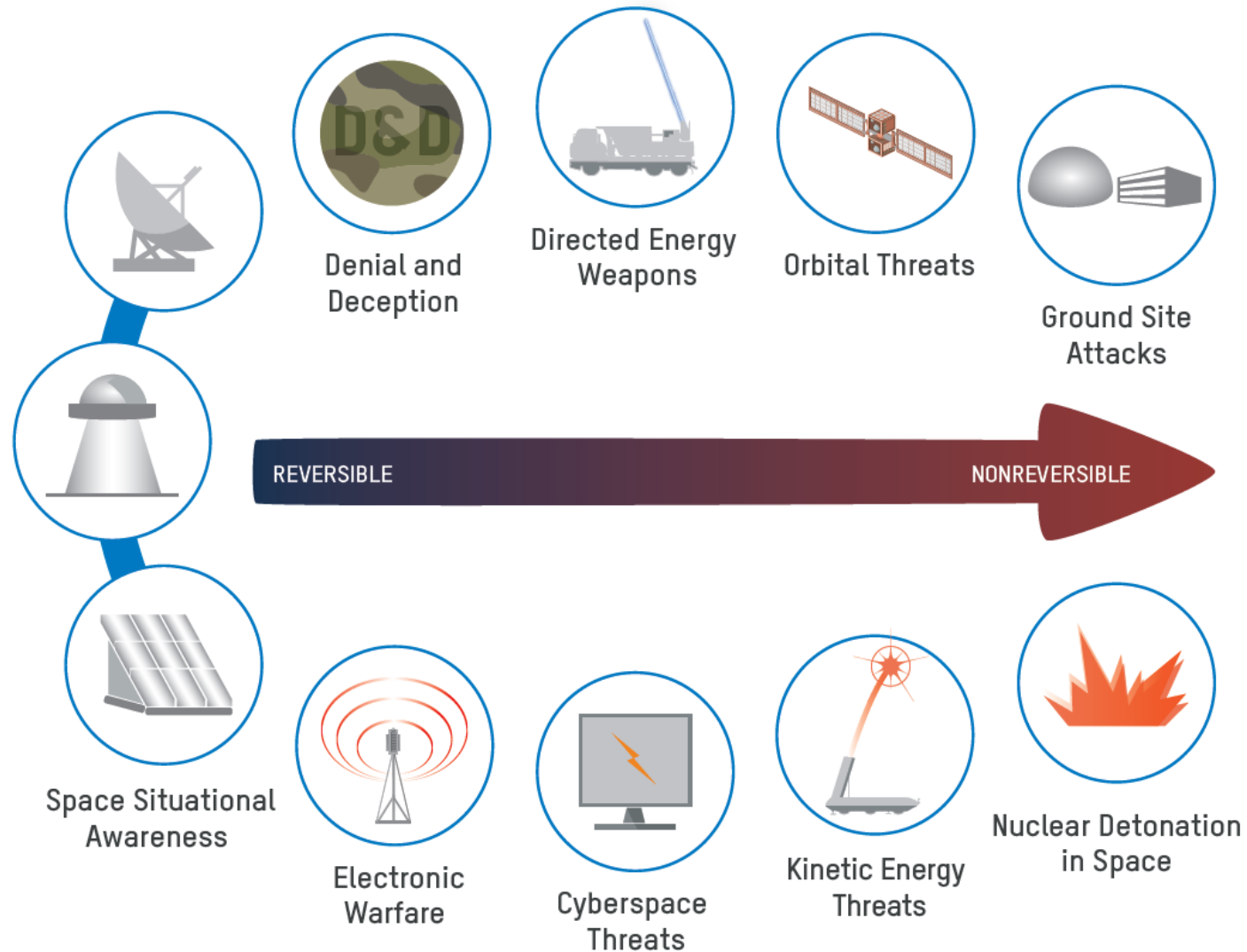
Medium 2-10%

High > 10%

GPS SPOOFING



THREATS TO SPACE SYSTEMS



RECENT SPACE ACTIVITY

- 2007, China conducts hit-to-kill anti-satellite (ASAT) test; India (2019) and Russia (2021) follow suit and continue to develop counterspace programs
- 2016, China tests first robotic arm on satellite
- 2018, Russia conducts tests on “stacking doll” satellite
- 2022-present, Russia continually jams and spoofs GPS

UNITED STATES SPACE COMMAND

USSPACECOM conducts operations in, from, and through the space domain (100 km+ altitude) to deter aggression, defend U.S. and allied interests, and deliver space combat power. As a unified combatant command, it integrates military spacepower into global, multi-domain operations, ensuring space superiority and protecting national security

- Forces principally from United States Space Force, Colorado connection
- Continuous space activity, warfighting readiness
- Traffic in space growing exponentially

HYBRID ATTACKS – CYBER AND SPACE

- 2010, Russian actors hacked Norwegian ground station. NASA/NOAA satellites, no commands
- 2022, Russia effectively attacks Viasat modems, targeting command and control
- 2023, China hacked the Japan Space Agency and downloaded its directory
- 2022-present, Russia “cat and mouse” game with Starlink user terminals

DETERRENCE IS THE KEY

“The most important priority for Western militaries is to prepare for a great power war with the intent to deter.”

The Character of Future War to 2030, 2024
Lt Gen (ret.) Hinote, USAF; Maj Gen (ret.) Ryan, Royal Aus. Army
Special Competitive Studies Project
(Funded by Eric Schmidt, fmr Google Chair, CEO)

BUT HOW TO DETER IN CYBER AND SPACE?

-
- Classic strategic deterrence theory:
 - Demonstrate the weaponry to impose unacceptable costs
 - Have the ability to deny benefits of the adversary's attack
 - Cyberspace and space highly classified
 - We don't reveal weaponry in either domain, so neither aspect works



THE FIRST SHOTS FIRED IN
FUTURE CONFLICTS WILL BE IN
CYBERSPACE AND SPACE

WILLIE SHELTON