APPLICATION OF GEOSPATIAL INTELLIGENCE IN SECURING CRITICAL INFRASTRUCTURE

By. Joshua Gollapudi

WHAT IS GEOSPATIAL INTELLIGENCE?

- Also known as GEOINT
- Analyzing and using imagery and geospatial information to describe, assess, and visualize the Earth's physical features and activities
- Includes geographic information such as maps, satellite data, and GPS
- Applications in national security and military, surveillance, environmental monitoring, emergency response, and intelligent vehicle navigation
- National Geospatial-Intelligence Agency (NGA): a US agency that provides geospatial intelligence (GEOINT) to support national security

WHAT IS CRITICAL INFRASTRUCTURE?

- Systems, assets, and networks that are vital to the function of society
  - Utilities: electricity, clean water, waste management
  - Transportation: airports, roads, bridges, railways, tunnels, shipping ports
  - Communication: networks, telephone lines, broadcasting systems
  - Healthcare: hospitals, clinics, emergency services
  - Financial Services: banks, stock exchange
  - Emergency Services: police, fire stations, emergency response (911)
  - Food Supply: Agriculture production and food distribution

WHY IS CRITICAL INFRASTRUCTURE IMPORTANT?

- Public Safety and Health
  - Ensures access to essential services (e.g., emergency response, healthcare)
  - Protects citizens from disruptions in basic need
- National Security
  - Protects against threats (e.g., cyberattacks, terrorism)
  - Critical for defense and military operations
- Economic Stability
  - Supports the economy by maintaining operations of key industries
  - Facilitates trade and commerce, ensuring the flow of goods and services

GEOSPATIAL DATA APPLICATIONS IN SECURING CRITICAL INFRASTRUCTURE

- Threat Mapping
  - Analyze geographic areas prone to specific threats (e.g., natural disasters, attacks, criminal activity)
  - Identify patterns and trends that inform risk assessments and resource allocation
- Risk/Vulnerability Assessment
  - Pinpoint critical assets and their geographic vulnerabilities
  - Assess potential impacts of various threat scenarios on infrastructure components
- Incident Response Planning
  - Utilize real-time geospatial data to improve situational awareness during incident
  - Coordinate emergency response efforts by mapping the locations of resources and identifying affected areas

CASE STUDY: RUSSIAN-UKRAINE WAR

- Russia has targeted Ukraine's civilian critical infrastructure in order create instability, cripple the economy, and demoralize the Ukrainian public
- Targeted: Energy Infrastructure, Water Supply Systems, Transportation Networks, Telecommunications, Healthcare Facilities, Industrial sites
- Carried out missile and drone strikes, artillery shelling, cyberattacks, ground assaults, and naval blockades
- Effects of these attacks
  - **Humanitarian Crisis**
  - **Crippled Economy**
  - **Military Strain**

INTERNATIONAL AID TO UKRAINE FOR CRITICAL INFRASTRUCTURE

- Humanitarian Assistance: $15 billion
  - **Food, Shelter, Healthcare, Water, Energy**
- Economic Support: $30 billion
  - **Public Administration, Economic Stabilization, Public Services**
- Reconstruction and Recovery: $50 billion
  - **Energy, Transportation, Housing, Public Institutions**

CASE STUDY: GEOINT UTILIZATION IN THE WAR

- Platforms and Sensors
  - HawkEye 360: satellites that monitor RF signals and sensors that capture GPS interference over Ukraine
  - Spire: nanosatellites that track aviation traffic
  - ICEYE: synthetic aperture radar (SAR) satellites that provide imagery
- Precision
  - High Mobility Artillery Rocket System (HIMARS): rapid and precise mobile artillery system
  - Observe-Orient-Decide-Act (OODA) Loop: AI used to process data, analyze live battlefield situations, select targets, and plan strikes