

Inside the Cyber Battlefield: How China Threats Target U.S. Critical Infrastructure & Defense



What is CISA?

- The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against cybersecurity threats
- Threat Hunting's Mission is to hunt cyber threats targeting U.S. infrastructure to mitigate national risk
- Forensic Investigations and Incident Response support for Federal Civilian Government (.gov) and critical infrastructure



How does CISA do its Mission?

- Voluntary Incident Response Deployments
- Voluntary Technical Services
- Baseline of Visibility and Security across the “.gov”
- Close Partnership with IC, Industry, and International Partners



PRC Threats

- PRC shift to pre-positioning for possible disruptive cyberattacks
- Persistent, Sophisticated, and well-resourced
- Continuous cyber espionage campaigns
- Volt Typhoon and Salt Typhoon



China 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 the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces.



THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE'S
2024 ANNUAL THREAT ASSESSMENT



R. Connor Gauvin, Threat Hunting
April 25, 2025

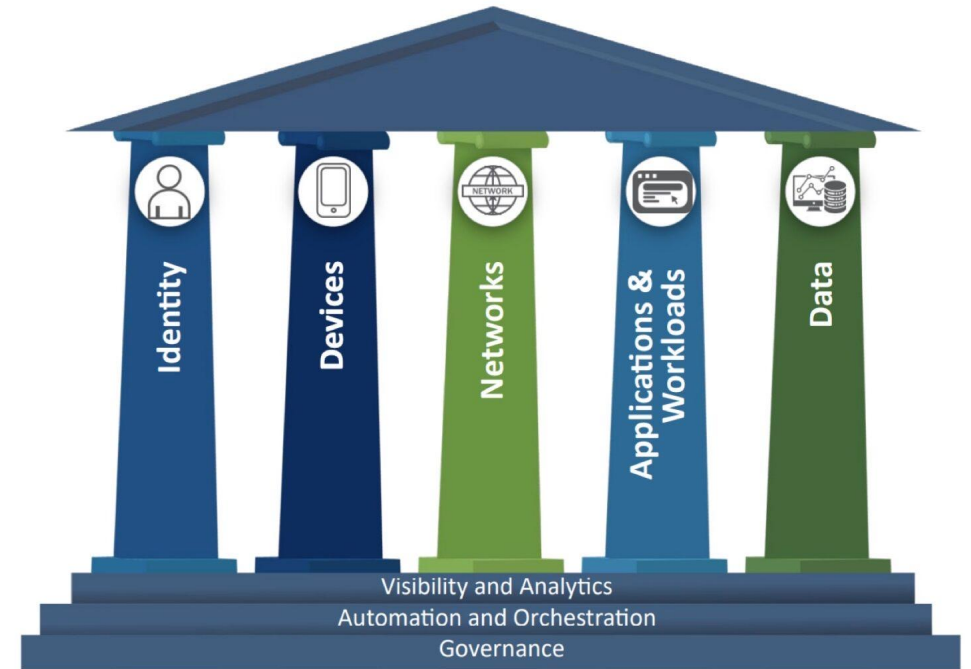
What to Defend

- What HVAs could disrupt US Intelligence Community/DoD?
- What could lead to access elsewhere?
- What would provide intelligence value?



How to Defend

- Do the Basics
- Patch Top Routinely Exploited Vulnerabilities
- Defense-in-Depth/ZeroTrust
- Breaches will happen



Additional Resources

- CISA
- DC3



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE



A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)



R. Connor Gauvin, Threat Hunting
April 25, 2025



For more information:
www.cisa.gov

Incident?
Email: report@cisa.gov
Phone: 1-844-Say-CISA

Questions?
Email: Ronald.Gauvin@cisa.gov