Department of the Air Force

Mapping Mission Relevant Terrain in Cyberspace Supporting DAF Installation Control Infrastructure – event 210

Mr. Daryl Haegley, SL, GICSP, OCP

DAF Technical Director, DAF Control Systems Cyber Resiliency

29 August 2023, 1400-1450

Montgomery Performing Arts Center, Main Stage

Supply Chain Risk Management

DIB Cybersecurity

DoD missions

- **DoD weapon systems / platforms**

  FY16 NDAA Section 1647

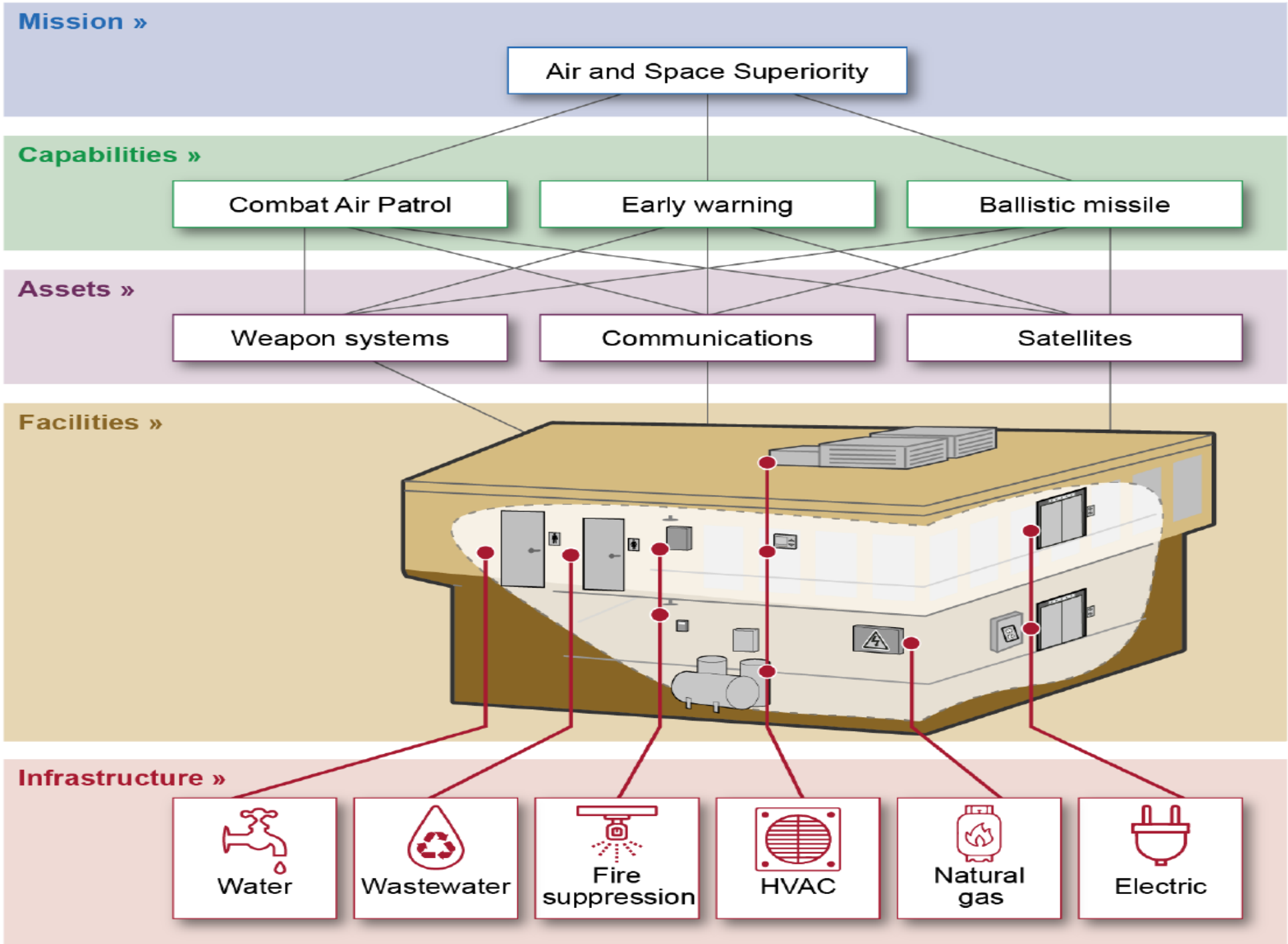
- **DoD critical infrastructure**

  FY17 NDAA Section 1650
  FY18 NDAA Section 1643

- **Commercial critical infrastructure**

Information Technology (IT)

Operational Technology (OT) / Control Systems


Mission »
Air and Space Superiority
Capabilities »
Combat Air Patrol
Early warning
Ballistic missile
Assets »
Weapon systems
Communications
Satellites
Facilities »
Infrastructure »
Water
Wastewater
Fire suppression
HVAC
Natural gas
Electric

Chinese Malware Detected on U.S. Military Systems *(reported July 2023)*

- China has hidden malicious code deep inside networks controlling power grids, communications systems and water supplies that feed military bases
- Investigations show Chinese effort appears more widespread — in US & at American facilities abroad — than initially realized
- Officials acknowledge that they do not know full extent of code's presence in networks around the world, partly because it is so well hidden
- Biden Administration: Discovery of malicious code in American infrastructure, "raises the question of, what exactly, China is preparing for?"

Chinese malware found in US military systems; a direct threat to Airmen and missions they support

FY22 NDAA Sec. 1505 DoD Responsibilities

Not later than Jan'25, SECDEF shall complete mapping of mission-relevant terrain in cyberspace [MRT-C] for Defense Critical Assets [DCA] and Task Critical Assets [TCA] at sufficient granularity to enable mission thread analysis & situational awareness, including required—

(1) decomposition of missions reliant on such Assets

(2) identification of access vectors

(3) internal and external dependencies

(4) topology of networks and network segments

(5) cybersecurity defenses across information & operational technology (OT)

(6) identification of associated or reliant weapon systems

Mapping Mission Relevant Terrain in Cyberspace - OT

Mr. Aaron Bishop
DAF Office of the CISO

Serves as DAF's Chief Information Security Officer (CISO). Responsible for advising CIO and senior officials on cybersecurity policy, programs, and cyber force development. Oversees risk management and cybersecurity accountability for IS, WS, and OT

Mr. Jayson Ilic
HAF Directorate for Mission Assurance

Strategic Advisor for Mission Assurance for the Air Force Operations Group. Holds a BS in Environmental Engineering from Rensselaer Polytechnic Institute and a MS in Engineering Management & Systems Engineering from The George Washington University

Mr. Michael McMahon
HAF Directorate for Intelligence, Partnerships, and Engagement

Intelligence Mission Manager for Information Warfare and Special Technologies. Produced authoritative assessments and advised Executive Branch on strategic cyber threats, threats to CI, and the national security implications to science and technology

Mr. Michael Dransfield
NSA Cybersecurity Directorate

Subject Matter Expert for Control System Cybersecurity. Senior technical executive at NSA with a career spanning 30+ years. Pioneered NSA's Control Systems Division over 14 years ago