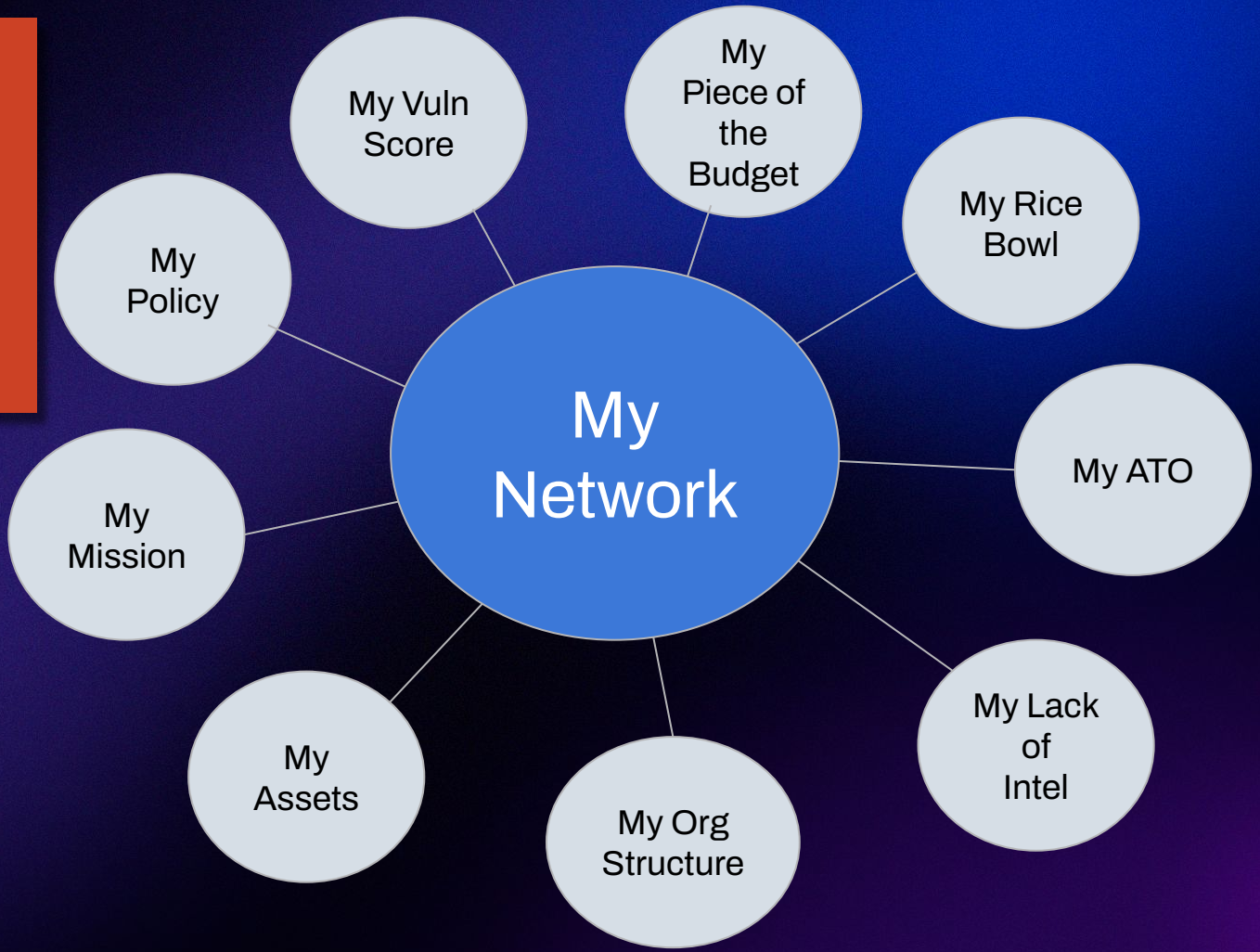
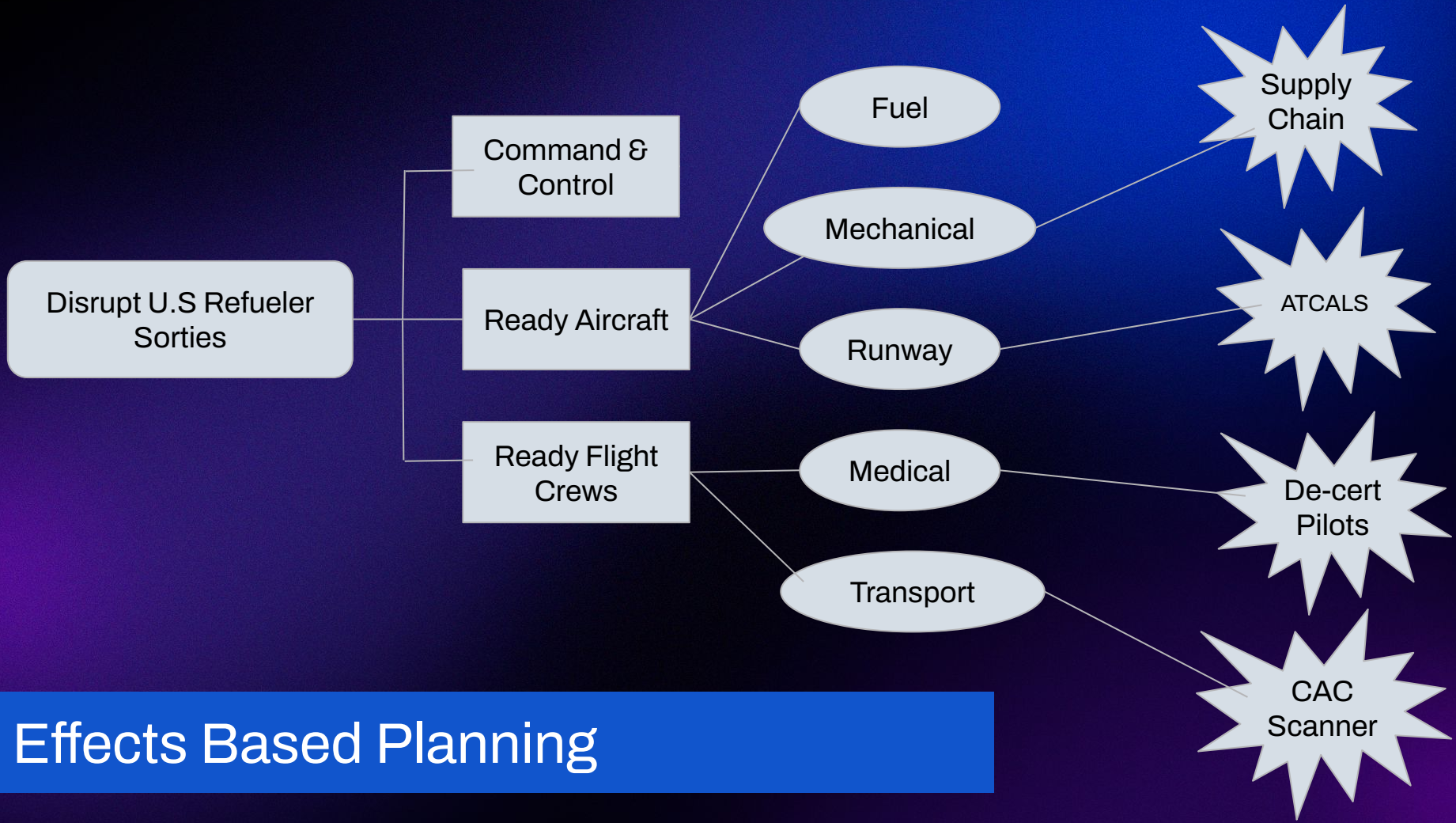
Building a Seamless Cyber Defense

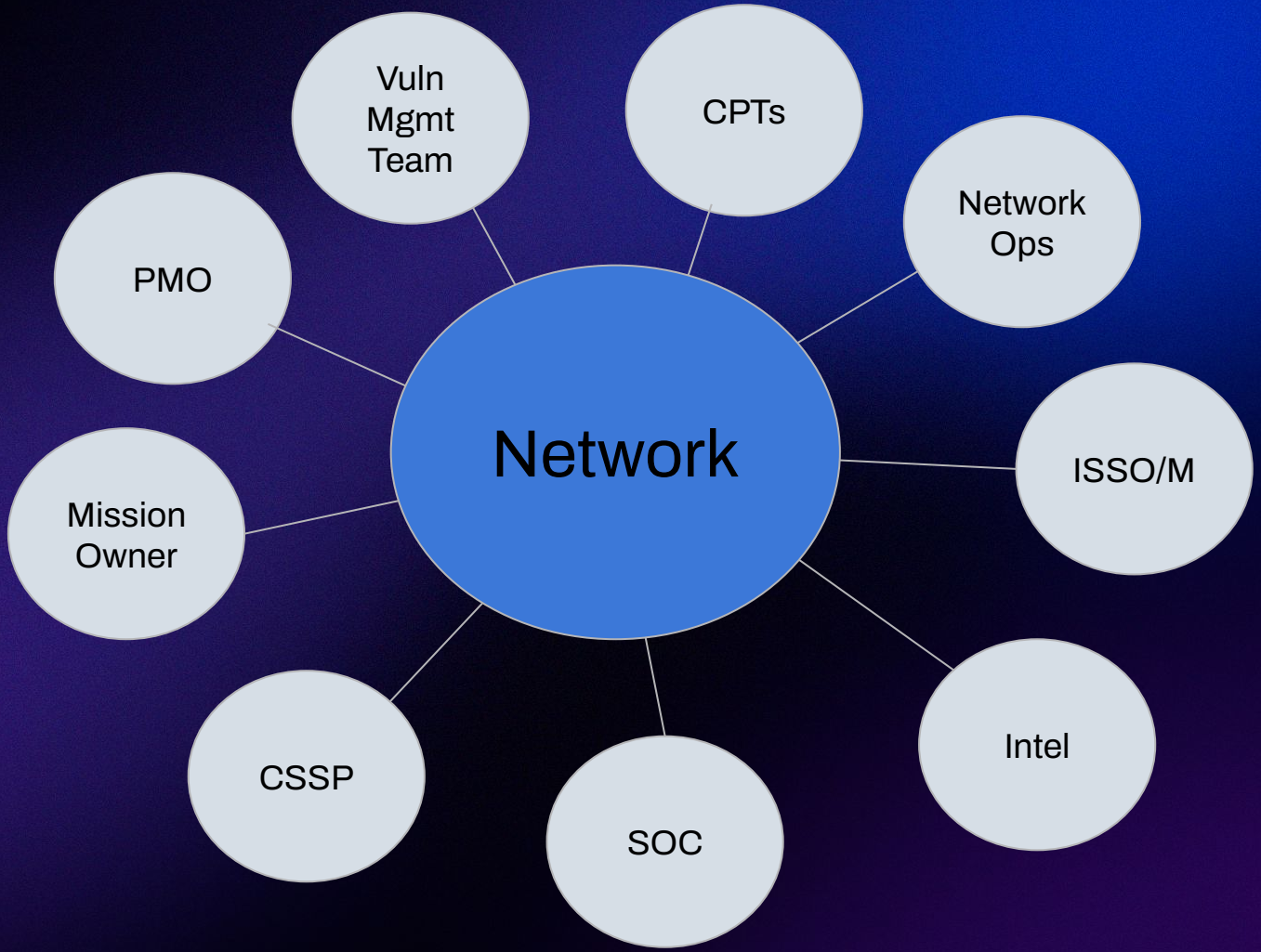
Colonel (Ret) Joseph Wingo
Director of Strategy, Armis Federal

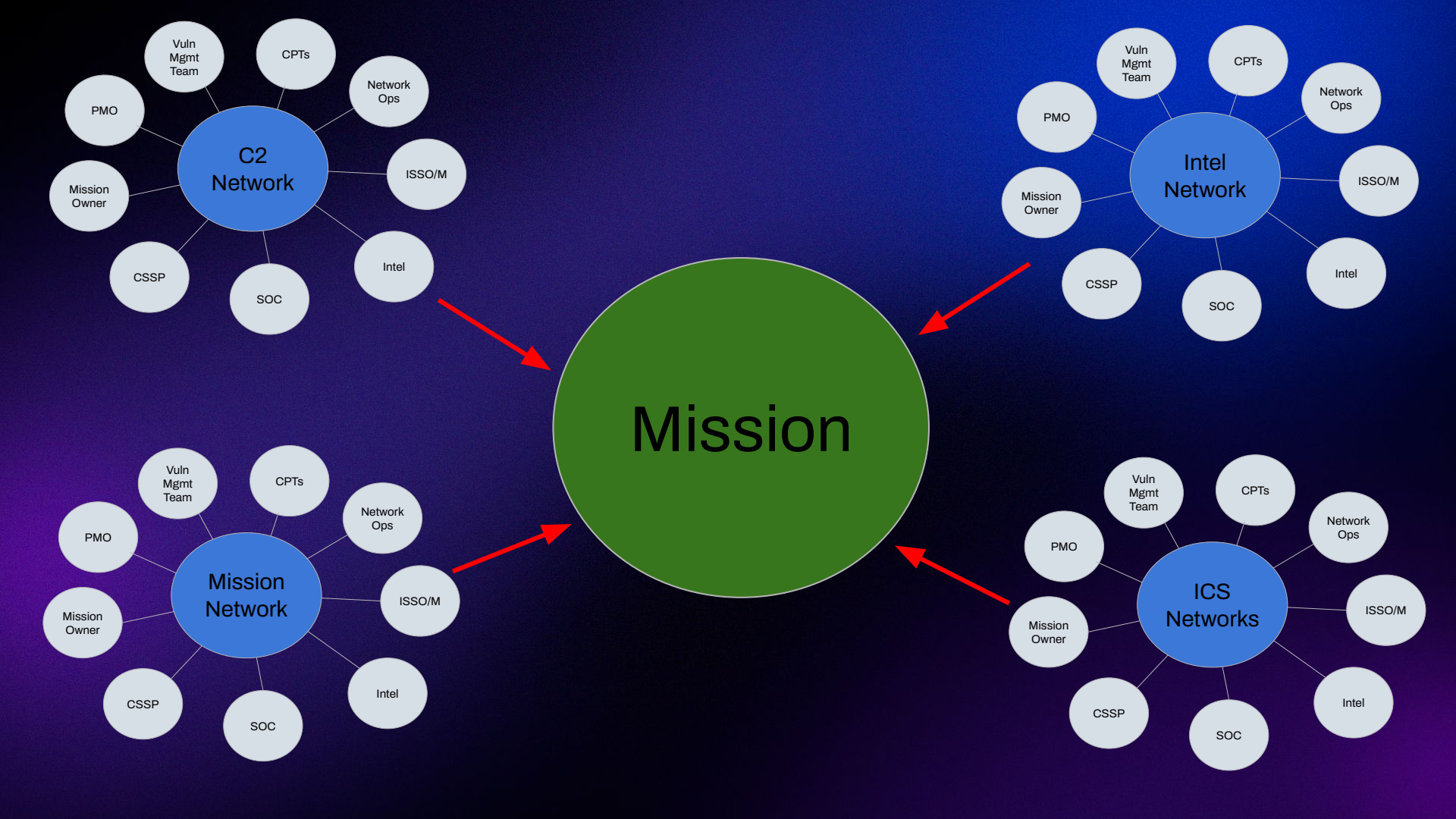
Traditional View of Network Security

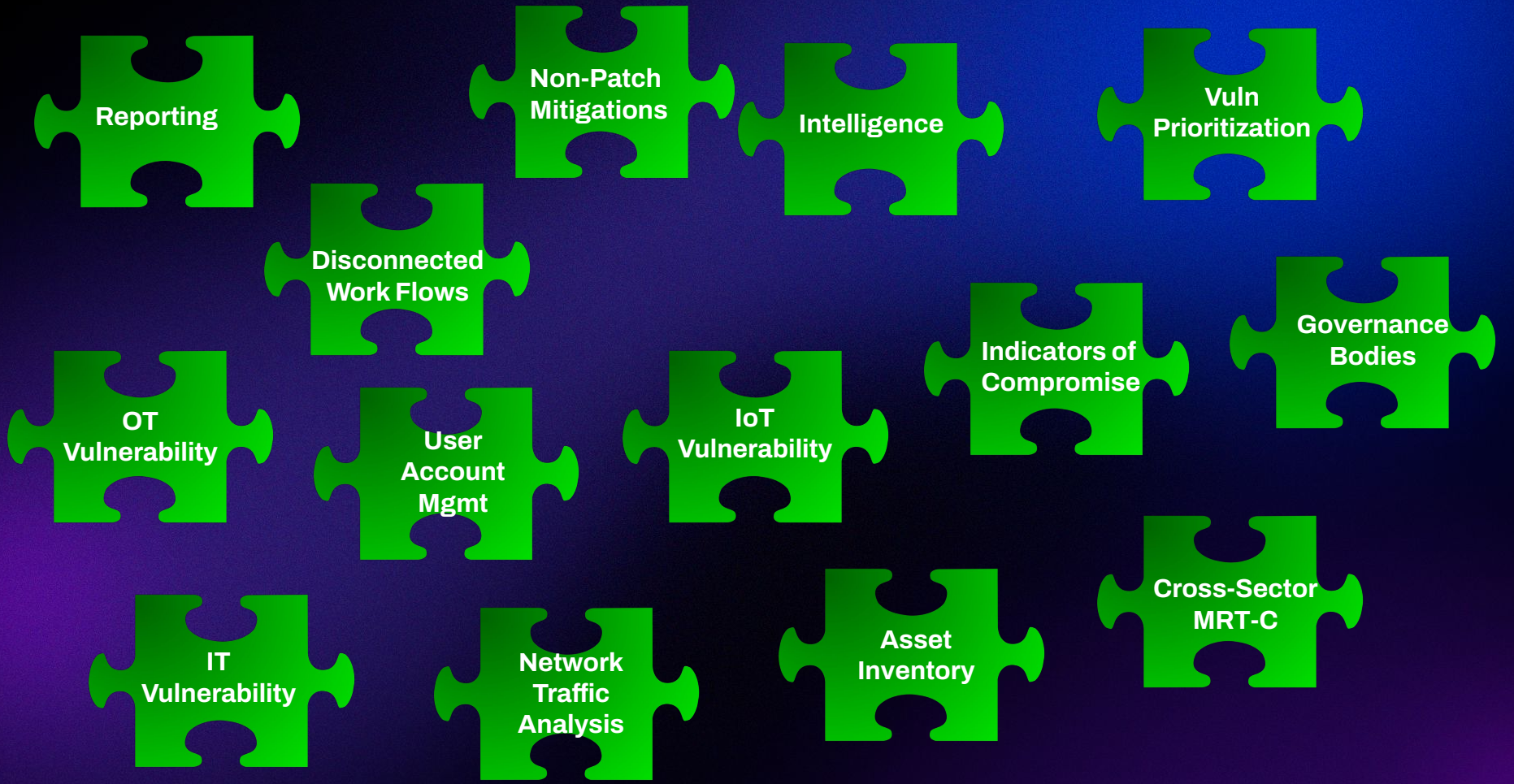


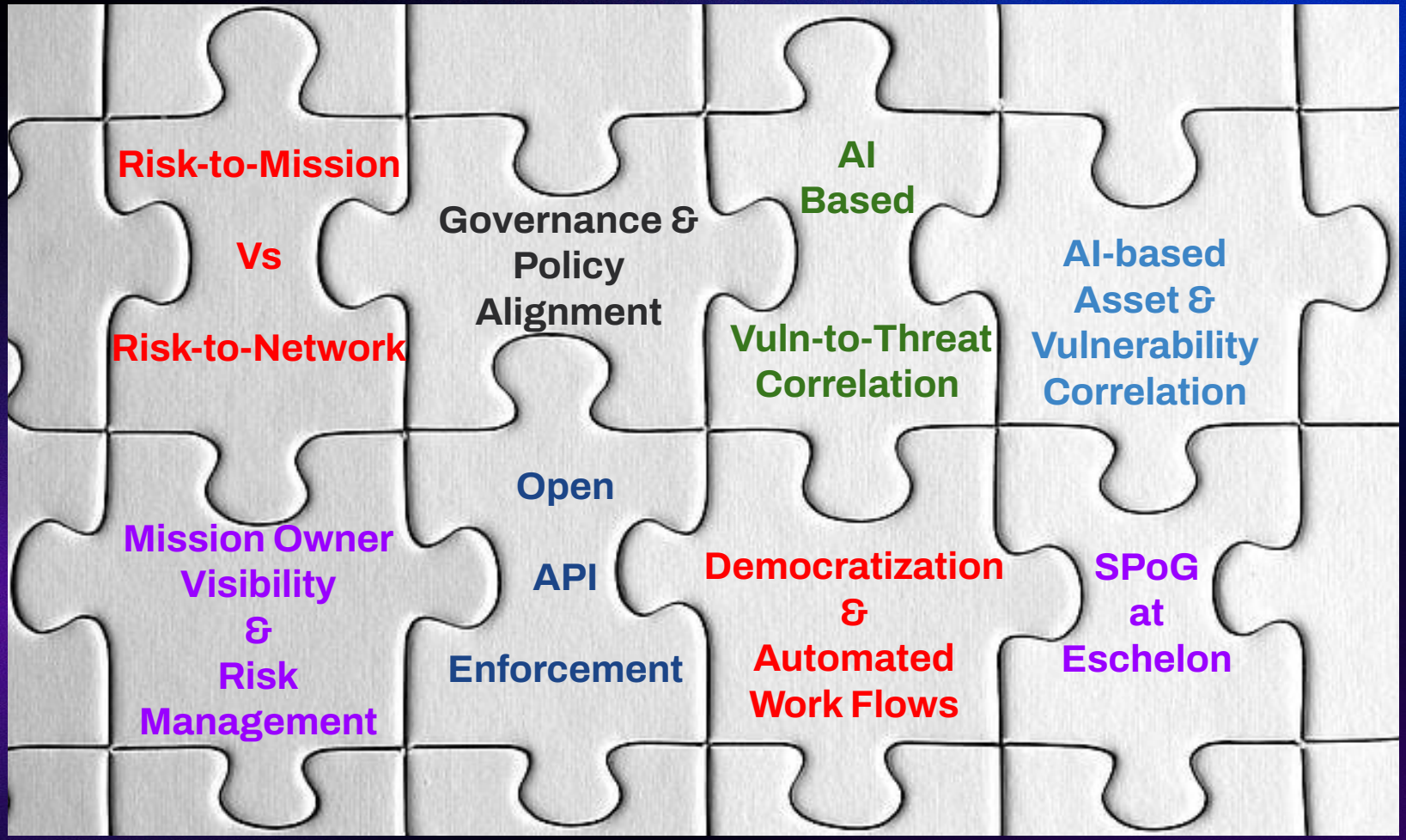


Effects Based Planning


Vuln Mgmt Team
CPTs
Network Ops
PMO
Network
ISSO/M
Mission Owner
CSSP
SOC
Intel


Mission
C2 Network
Vuln Mgmt Team
CPTs
Network Ops
ISSO/M
Intel
SOC
CSSP
Mission Owner
PMO
Intel Network
Vuln Mgmt Team
CPTs
Network Ops
ISSO/M
Intel
SOC
CSSP
Mission Owner
PMO
Mission Network
Vuln Mgmt Team
CPTs
Network Ops
ISSO/M
Intel
SOC
CSSP
Mission Owner
PMO
ICS Networks
Vuln Mgmt Team
CPTs
Network Ops
ISSO/M
Intel
SOC
CSSP
Mission Owner
PMO


Reporting
Non-Patch Mitigations
Intelligence
Vuln Prioritization
Disconnected Work Flows
Governance Bodies
Indicators of Compromise
OT Vulnerability
User Account Mgmt
IoT Vulnerability
Cross-Sector MRT-C
IT Vulnerability
Network Traffic Analysis
Asset Inventory


Risk-to-Mission
Vs
Risk-to-Network
Governance &
Policy
Alignment
AI
Based
Vuln-to-Threat
Correlation
AI-based
Asset &
Vulnerability
Correlation
Open
API
Enforcement
Mission Owner
Visibility
&
Risk
Management
Democratization
&
Automated
Work Flows
SPoG
at
Eschelon

Bottom Line

China & Russia Don’t Care About….

- Your Network
- Your PoAM
- Your Cyber Risk Score Card
- Your Zero Trust Fan Chart

China & Russia Are Obsessed With…

- Effects
- Creating a stutter-step in our order-of-battle
- Increasing Fog-of-War
- Slipping in through gaps and seams

IMHO….

- Think multiple echelons above & outside our position/lane
- Who needs this information & how can I share it effectively…& vis versa
- Rationalize tools & focus on interoperability/integration
- BOLDLY implement AI/ML capabilities to
  - Generate data
  - Correlate data in realtime
  - Automate risk analysis
  - Automate vulnerability prioritization
  - Generate workflows
- Automate operationalization of information for Decision Makers

Questions?