The Cyber Lifecycle

Jacqueline Janning-Lask
AFLCMC/WNE
6 June 2017

Cyber – Why is it so darn hard?

- *Human* generated domain – few "natural laws"
  - Filled with "oops", special cases, and surprises
- Properties:
  - Non-linear – what's a dB of cyber?
    - Vulnerable today – patched tomorrow?
  - Disruptive – which is the whole point of adding it
    - Awesome capabilities…with a potential dark side
  - Inconsistent – not always what you expect
    - Who is attempting what?
  - Often unpredictable – complexity drives this
    - Insert unexpected value X – weird thing Y happens
  - Easily "democratized" – non-nation-states can become near "national" capable cyber powers w/ little effort
    - Big capabilities leave only a tiny –INT footprint - no large infrastructure!
  - Cyber is a team sport – new area for weapon system acquisitions -- new problem for new people, skillsets, processes, and organizations that have never played together before -- but MUST!

*Comments provided by Rich Kutter, AFRL/RYW

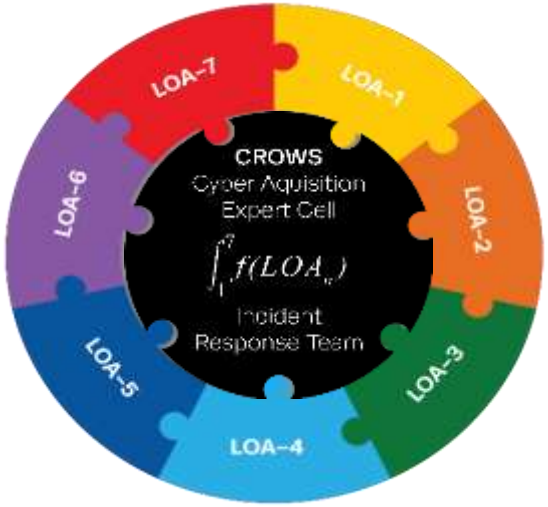
Food for Thought: RAND

- **Current policies are better suited to simple, stable, and predictable environments than to the complex, rapidly changing, and unpredictable reality of today's cybersecurity environment.**
- **Implementation of cybersecurity is not continuously vigilant throughout the life cycle of a military system.**
- **Control of and accountability for military system cybersecurity is spread over numerous organizations and is poorly integrated.**
- **Monitoring and feedback for cybersecurity is incomplete, uncoordinated, and insufficient for effective decision-making or accountability.**

-"Cybersecurity of Air Force Weapon Systems", RAND Research Brief, 2016.

AF Cyber Campaign Plan: Weapon System Focus

- **Goal:**
  - #1 “Bake-In” cyber resiliency into new weapon systems
  - #2 Mitigate “Critical” vulnerabilities in fielded weapon systems
- **7 Lines of Action (LOAs)**
  - LOA 1: Perform Cyber Mission Thread Analysis
  - LOA 2: “Bake-In” Cyber Resiliency
  - LOA 3: Recruit, Hire & Train Cyber Workforce
  - LOA 4: Improve Weapon System Agility & Adaptability
  - LOA 5: Develop Common Security Environment
  - LOA 6: Assess & Protect Fielded Fleet
  - LOA 7: Provide Cyber Intel Support



People, Processes, & Products

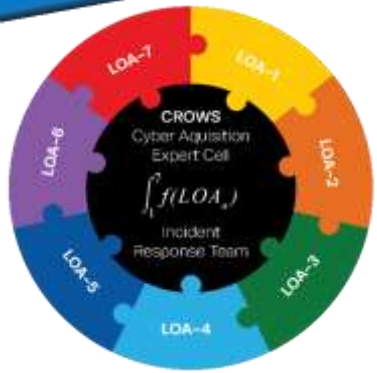
- **Test & Evaluation (infrastructure/capability growth): Part of LOA 2**
- **Cyber Squadron Initiative (CS-I)**
- **Industrial Control Systems/SCADA cyber protection measures**

Ensure mission success in a cyber contested environment

Roadmap to Resiliency

Present

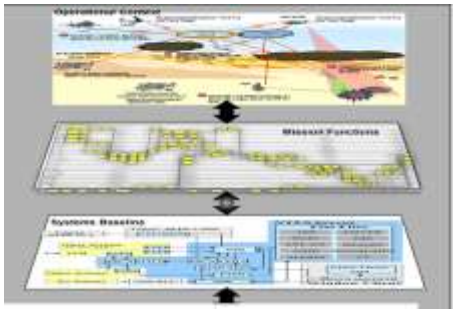
Future



Mission Assurance

- Mission Thread Analysis

- Develop assessment methodology framework
- Develop cyber acquisition workforce



System Assurance

- Assess and Fix

- Assess cyber posture of fielded systems
- Enable weapon system adaptability

Mx and Aircrew Trainers

Off Board Support

Institutionalize

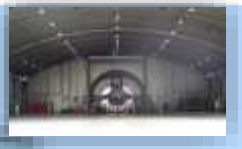
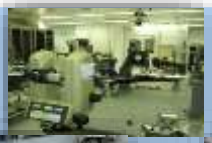
- "Baked" in resiliency

- Institutionalized methodology, tools, T&E infrastructure
- Skilled workforce
- Integrated cyber tools, policy, etc.

Applying Cyber Across All Domains



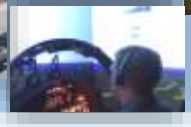


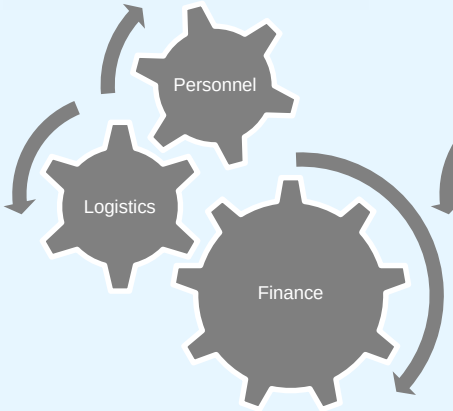




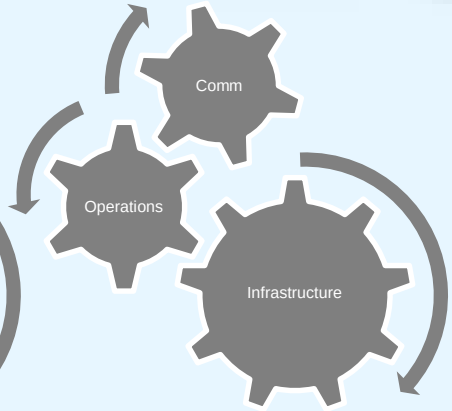


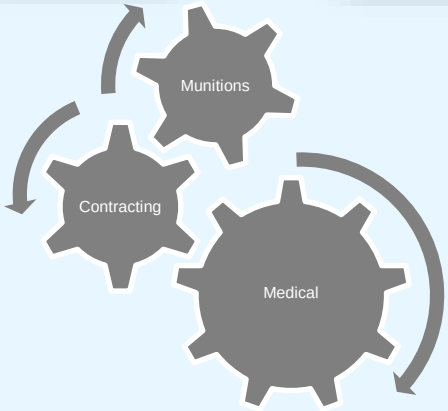


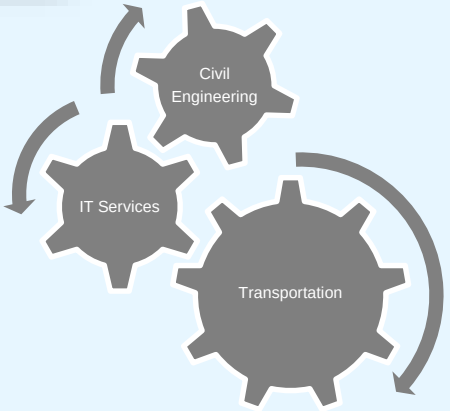


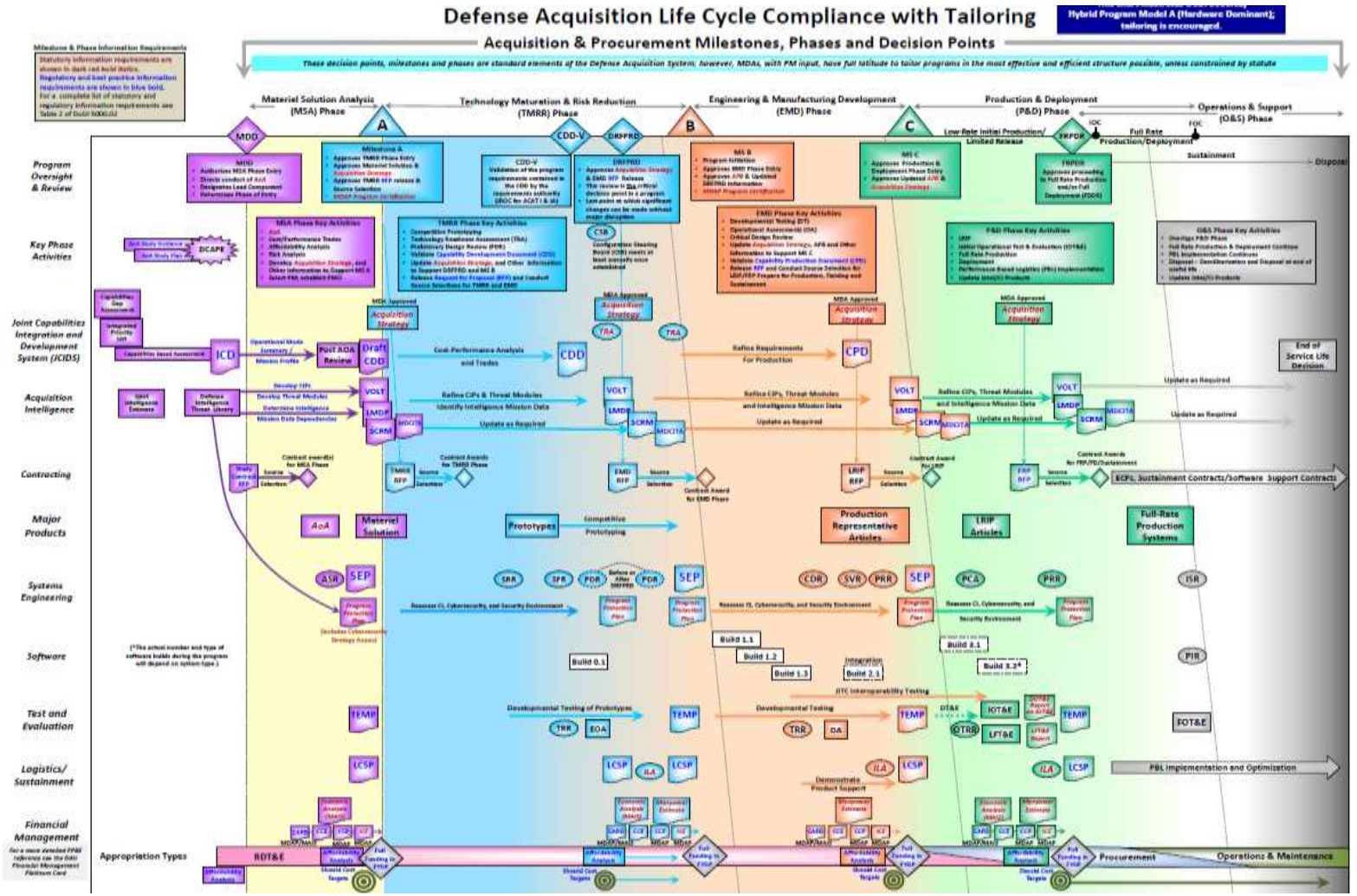








Applying Cyber Across the Lifecycle



Assuring Resiliency

- **Ability of weapon systems to maintain mission effective capability under adversary offensive cyber operations**
- **Manage the risk of adversary cyber intelligence exploitation**
- **Resiliency is the ability to morph, change in the face of adversity**
- **”Cyber resiliency is the ability of cyber systems and cyber-dependent missions to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats” ---”Cyber Resiliency Engineering Aid, MITRE, Defense Innovation Marketplace, May 2015**

Resiliency is key to cyber success and mission assurance
Between, Among, Within and Across the Lifecycle

Questions?

?