



Systems Engineering in a Cyber World

Connecting Frameworks for Program Decisions

Ernest Hibbs
Chief Engineer, Cyber Development Directorate
15 May 2019



Agenda

- **Reasons SE is not done in Cyber**
 - Cultural Problems and Opinions
- **SE Rationale for Cyber**
 - Doctrine, Organization, Training, Leadership, Personnel, Facilities (DOTMLPF)
Decision-Based Example
- **Latest approaches to SE in Cyber**
 - DOD Cybersecurity Assessment Review (DODCAR), Connecting NSA's Threat Framework
- **Cyber SE benefits to Program**
 - Communication, Management, and Portfolio Planning



Reasons SE is not done in Cyber:

Cultural Problems and Opinions

- **Oversimplifying the complexity of the problem**
- **Spending excessive funds just discussing the problem**
- **Commissioning a burdensome documentation effort**
- **Forcing engineers outside their skills for urgent needs**
- **Meeting the changing decision needs of the PM**
- **Organizing SE is harder than building the systems**



SE Rationale for Cyber:

DOTMLPF Decision-Based Example

- **Need to organize engineering to beat organized crime**
- **Need to synchronize the expanding and compressing solution spaces**
- **Need to execute lean Systems of Systems (SoS) approach**
- **Need to provide high ROI engineering guidance to PM**
- **Need to quantify the extra dimensions of a decision**
- **Need to normalize priorities (with a DOTMLPF example)**



Normalizing Priorities with DOTMLPF – Criteria Scoring Approach

| DOTMLPF CATEGORY | DEFINITION (For Tools and DCO) | EVALUATION CRITERIA |
|---------------------|---|--|
| Doctrine | Technical Mission requirements (CND, Monitoring, CM, etc.), CONOPS, Tactics (TTPs, SOPs) and Network level (Application, Compute, Transport) | <ol style="list-style-type: none"> 1. Supports Existing Operational Procedures 2. Supports ITSM Automation 3. Part of Vital CND Monitoring |
| Organization | Number and type of structure and staff required to operate the technical capability with proper reporting (CCMDs, DECC, JSSC, Tier III, etc.) | <ol style="list-style-type: none"> 1. Does not require complex organization 2. Supports complex reporting/organization 3. DoD/DISA Enterprise organizational-level capability |
| Training | Over-the-shoulder, OJT, CBT, vendor classes, Gov't-specific classes, certifications | <ol style="list-style-type: none"> 1. Learning curve less than 1 month 2. Government specialized training available 3. Mobile training available |
| Materiel | Workstations, Servers, Storage, Operation Systems, and items required to operate the capability | <ol style="list-style-type: none"> 1. Virtualized 2. No special hardware 3. Simple Support Plan (less than 3 dependent licenses or required components) |



Normalizing Priorities with DOTMLPF – Criteria Scoring Approach

| DOTMLPF CATEGORY | DEFINITION (For Tools and DCO) | EVALUATION CRITERIA |
|--------------------------------|--|---|
| Leadership and Education | Ease of preparing management to strategically drive the portfolio to an enterprise level | <ol style="list-style-type: none"> 1. Leads to innovation and ability to integrate and interoperate 2. Potential enterprise scalability 3. Flexible/incremental contracting |
| Personnel | Availability of qualified people with key skill sets; ramp-up time | <ol style="list-style-type: none"> 1. Does not require high installation and implementation skills 2. Does not require unique operational and analysis skills 3. Does not require engineering change management skills |
| Facilities | Foot print, DECC resources, HVAC, power, physical security, access, and location | <ol style="list-style-type: none"> 1. Located at more than 1 prime location 2. Common hosting in place 3. COOP required or recommended |



Capability Database Planning with DOTMLPF – Historical Decision Weighting and Recording

| Item | Primary OV-5 Type | Feature | Tool | Description | Users | Totals Per Category | | | | | | | Action | Migrate Vital Features To | |
|------|-------------------------------|-----------------------|-------------------|--|-------------------------|---------------------|---|---|---|---|---|---|--------|---------------------------|----------------------|
| | | | | | | D | O | T | M | L | P | F | | | Avg |
| 1 | Infrastructure Mgmt. | Asset Mgmt | CM Extraordinaire | Does really cool stuff | Remote Office of 1 | 3 | 2 | 1 | 2 | 1 | 1 | 2 | 1.7 | Turn Off | Centralized Solution |
| 2 | Security Monitoring and Mgmt. | SA/COP Network Status | Logs and Frogs | Log aggregation, script generation, Track IP Hopping | Data Center Sys. Admin | 3 | 2 | 1 | 2 | 1 | 1 | 1 | 1.6 | Keep | |
| 3 | System Access | Unnecessary Step | NeverTell | Keep my brother in-law employed | COOP users | 2 | 2 | 2 | 3 | 1 | 3 | 0 | 1.9 | Turn Off | Nowhere |
| 4 | Decision Support | Dashboard | MyBigBrain | Has always been a pet project | At a great TDY location | 2 | 2 | 1 | 2 | 1 | 1 | 0 | 1.3 | Turn Off | Cloud |

After this, we get all the exceptions...the “But, but, but, you didn’t consider this.”
We will need a next step for scoring that will normalize biases.



Latest approaches to SE in Cyber:

DODCAR, Connecting NSA's Threat Framework

- **Use DoD Cybersecurity Assessment Review (DoDCAR) as the next dimension for normalizing priorities**
- **Use “Threat Capability Coverage Scoring” to support decisions**
- **Use DoDCAR engineering input to acquisition decisions**
- **Use SW engineering approaches to define threat activities**
- **Connect engineering data between DoDCAR, RMF, and DoD Architecture Framework (DoDAF)**



Threat Framework Cyber Capability Scoring and Decision Support

Threat Framework

| Threat | Threat Type | Threat Description | Threat Category | Threat Impact | Threat Mitigation | Threat Priority |
|-----------|-------------|--------------------|-----------------|---------------|-------------------|-----------------|
| Adversary | ... | ... | ... | ... | ... | ... |
| ... | ... | ... | ... | ... | ... | ... |

Threat Framework

- NSA Technical Cyber Framework (NCTCF)
- Use to select the scope of threat activities

Heat Map

| Threat | Impact | Priority | Weight | Concern |
|--------|--------|----------|--------|---------|
| ... | ... | ... | ... | ... |
| ... | ... | ... | ... | ... |

Threat Action Heat Map

- Structures prioritization and weights
- Based on actual intelligence data
- What are my concerns in my deployed environment?

Capability Mitigation Scoring

| Capability | Threat 1 | Threat 2 | Threat 3 | Threat 4 | Threat 5 |
|------------|----------|----------|----------|----------|----------|
| ... | ... | ... | ... | ... | ... |
| ... | ... | ... | ... | ... | ... |

Capability Mitigation Scoring

- Scores for Capability (row) against threat (column)
- Scores for Protect, Detect, and Respond
- Based on SME (threat and system) assessment

Security Capability Coverage

| Capability | Protect | Detect | Respond | Effectiveness |
|------------|---------|--------|---------|---------------|
| ... | ... | ... | ... | ... |
| ... | ... | ... | ... | ... |

Security Capability Coverage

- Effectiveness for Protect, Detect, Respond
- Gaps identified for requirements definition
- Early start on testable criteria for new products
- Strategic opportunity – How much? How soon?

Start Here

Decision Support Data

Assess Threat, Prioritize, Score Defenses, Identify Gaps

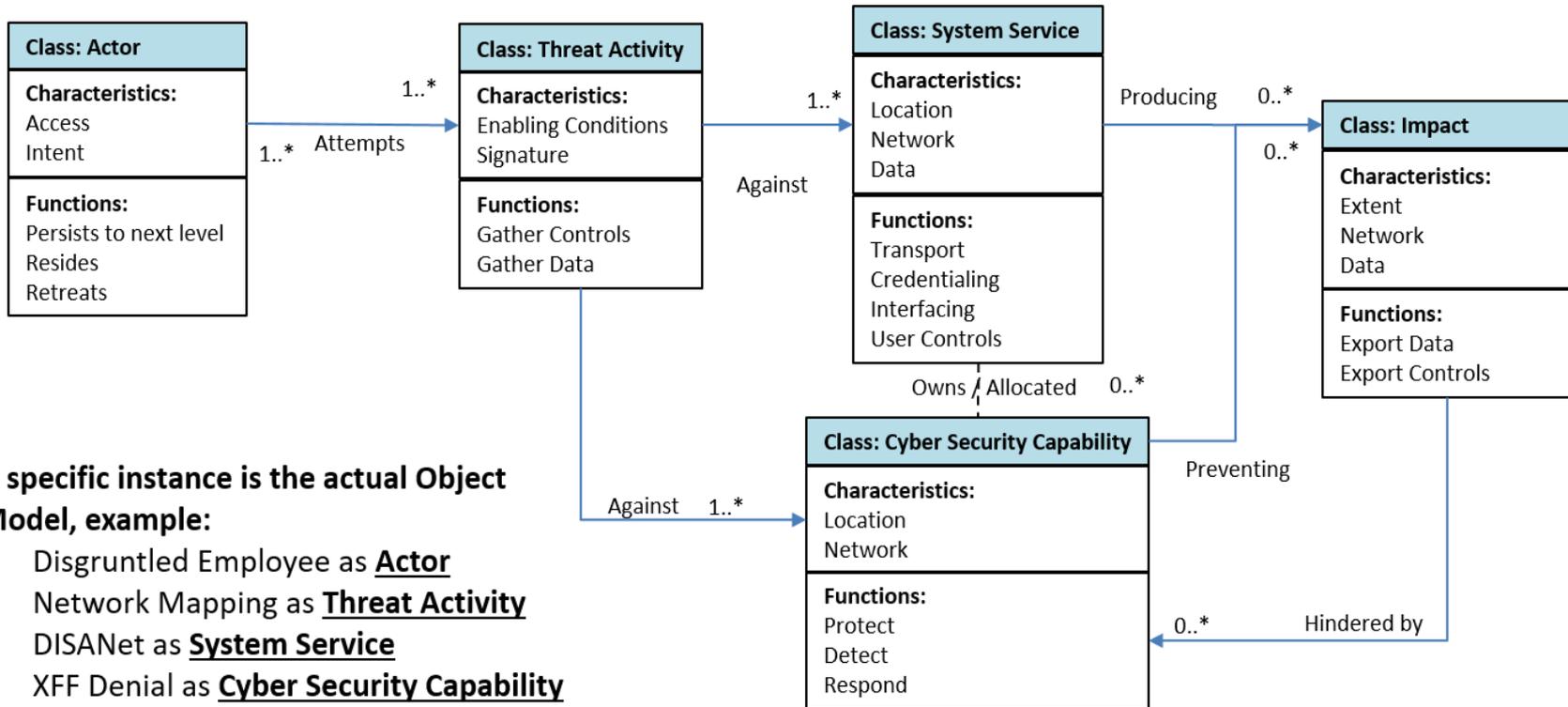


Threat Framework Engineering Input to Acquisition Decisions

| DoDCAR Process Artifacts | | Alignment with DAU Acquisition Phase and Associated Information | | | | | | | | | | | | | | |
|--------------------------|--|--|-----|--------------------|---|-----|-----------|---|-----|-----|---|-----|-----|--|------|-----|
| | | Material Solution Analysis | | | Technology Maturation and Risk Reduction | | | Engineering and Manufacturing Development | | | Production and Deployment | | | Operations and Sustainment | | |
| | | ICD | AoA | Draft CDD and TEMP | TEMP | RFP | CDD / TRA | PDR | CDR | CPD | LD | PRR | PPP | PIR | ECPs | EOL |
| DoDCAR Processes | Threat Models OV-5a OV-5b | Apply Framework (OV-5a) to proposed System's Threat Environment with Baseline of Mitigation Performance (i.e. MOE/KPP) | | | Identification of Test Environment, Test Cases, and Technical Performance Measures (TPMs) | | | Detailed system specific threat actions (OV-5b) for severity weighted most probable threat impact actions | | | Inform Red/Blue Team scenarios to most likely Threat Actions and Campaigns. CCORI and CCRI threat scenarios | | | Support 'tuning' of appliances configurations/rules/analytcs as adversary behaviors change | | |
| | Architecture Models | Cybersecurity performance and affordability parameters. System Functions (SV-1, SV-10, CV-2) for Threat Mitigation | | | System Tradeoffs and weighted Cybersecurity performance and affordability parameters. | | | Detailed system specific threat mitigation functions for corresponding threat actions (updated OV-5b) | | | Specific Network deployment models, Ports and Protocols | | | Threat-based ECP/Tech Refresh designs and functions | | |
| | Scoring Model CV-6 | Possible combinations of cyber system capabilities for TMRR (initial CV-6) | | | Cyber Effectiveness scores for capabilities in CV-6 for Trade-off Analyses | | | Updated scores from detailed design reviews to supplement selecting solutions | | | Establish capability measure of effectiveness (MOE) feedback loop for deployed systems | | | Adjusted scoring for threat-based ECP/Tech Refresh | | |



Cyber Threat Activity Definition in SW Engineering Model



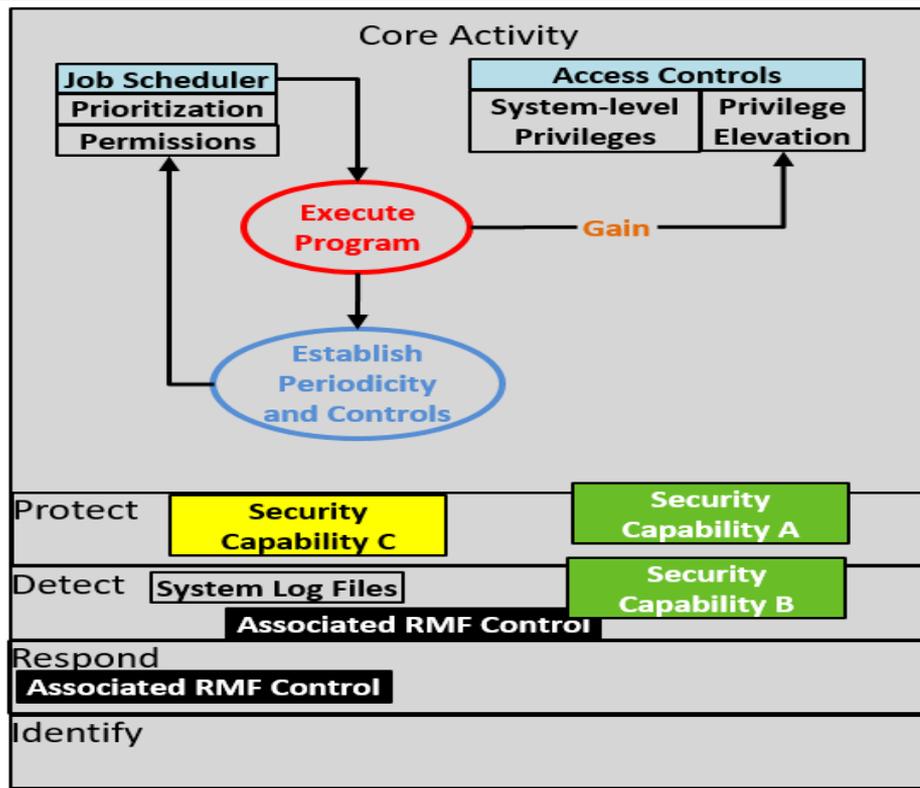
A specific instance is the actual Object Model, example:

- Disgruntled Employee as **Actor**
- Network Mapping as **Threat Activity**
- DISANet as **System Service**
- XFF Denial as **Cyber Security Capability**
- Exported Paths as **Impact**

Logical Class Model approach prepares us for Cloud



Connecting DoDCAR, RMF, and DoDAF Activity Models



Create scheduled task

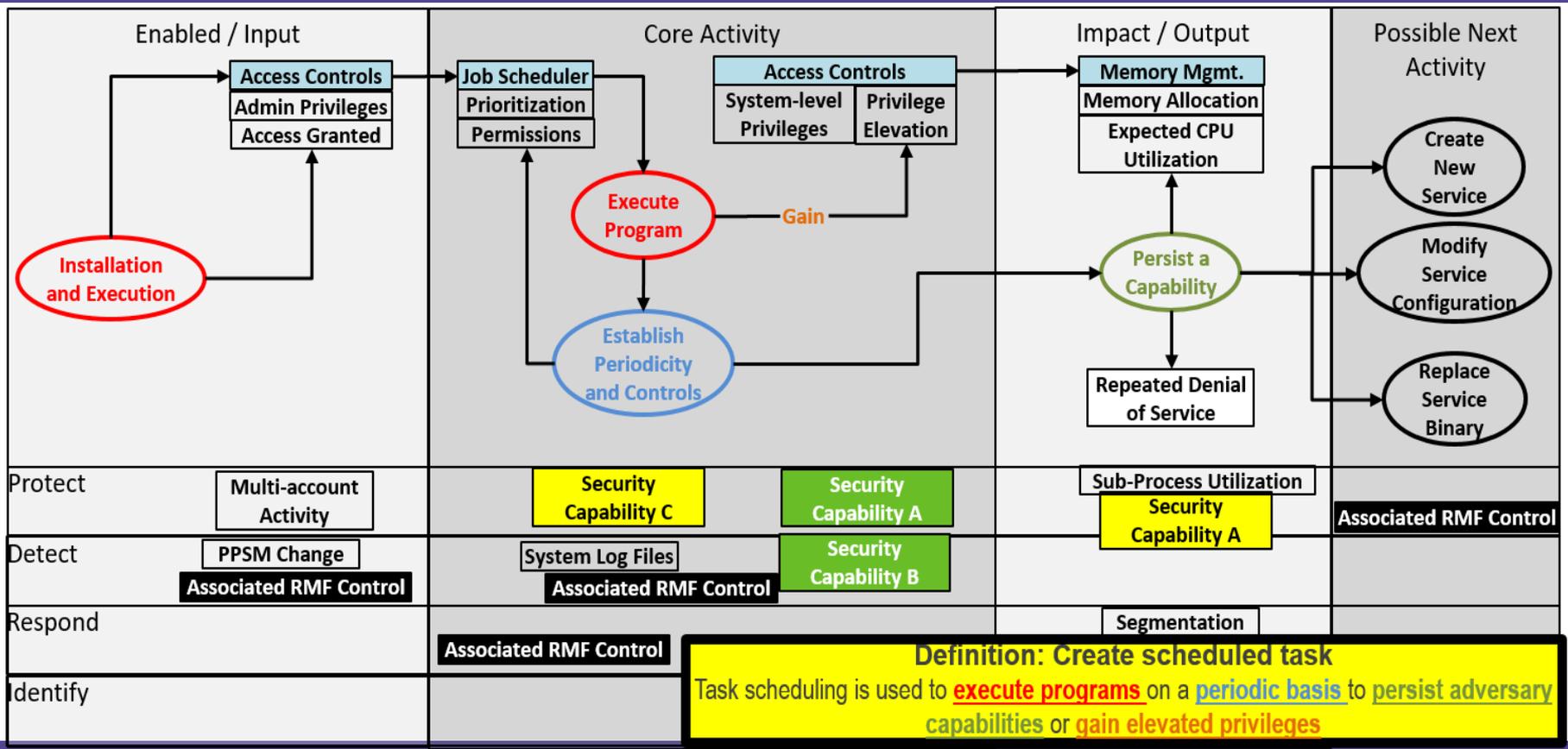
Task scheduling is used to **execute programs** on a **periodic basis** to **persist adversary capabilities** or **gain elevated privileges**

- System Component(s) Affected
 - Component/Object (Blue Boxes)
 - Features of the component
- Threat Actions (Process Oval)
- Cyber Swim lanes: Protect, Detect, Respond, Identify
 - Security capability mapping & rough score (color)
 - For inserting RMF mappings to Threat Activity (Controls)

Challenges: The best tool; Getting the right systems engineers



Conceptual Threat Activity Diagram – Create Scheduled Task (Inside the State of Persistence)





Cyber SE benefits to Program

Communication, Management, and Portfolio Planning

- **Method for communicating architecture, diagrams, and projects**
- **Technical Roadmap and functional WBS for planning**
- **Consistent and measurable data from Technical Reviews and IBRs**
- **Data for integrating Program Management**
- **Processes for rapid change in requirements**
- **Justification for funding**

visit us

DISA
Booth **1929**

follow us



Facebook/USDISA



Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at www.disa.mil/about/industry-partners.



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency



www.disa.mil



[/USDISA](https://www.facebook.com/USDISA)



[@USDISA](https://twitter.com/USDISA)