ASSIMILATING CYBER TEAMS IN TEST AND EVALUATION

RESISTANCE IS FUTILE IF WE ARE TO RISE TO THE CHALLENGE OF STRATEGIC COMPETITION

A non-cyber person's introduction to Cyber T&E, Cyber Teams, and Developing Tomorrow's Cyber T&E Talent

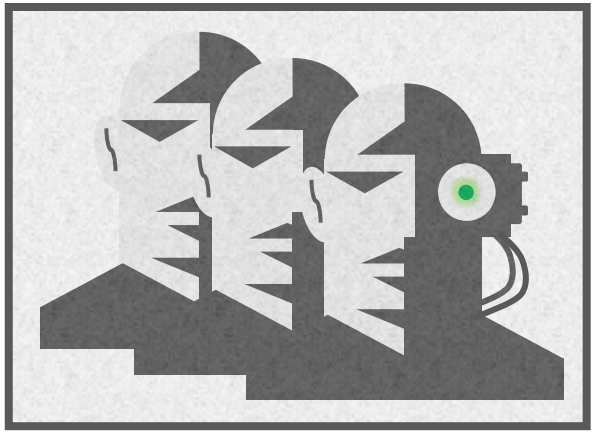
Unclassified
Cleared for public release

Created and Presented by
Mr. Steven Nastally, BCS, MBA, PMP

Disclaimer

- The following material is for academic purposes only and is the sole opinion of the author based on literature research and real-world experience.
- The appearance of U.S. Department of Defense visual information does not imply or constitute DOD endorsement.
- The Department of Defense [nor a respective Military Service or any other DOD Component] does not approve, endorse, or authorize any private company, its products or services.

Overview



- **Terminology:**
  - Nine cyber terms to help you connect with your teams.
- **Vectoring Change in Cyber T&E**
  - What, where, and who is operating in this domain.
- **Assimilation**
  - DOD Cyber T&E model viewed through the lens of Tuckman's Group Development stages and PMBOK's Organizational Structures.
  - Cybersecurity color wheel (Red/Purple/Blue/Green/Yellow/White) + DevSecOps.
  - CISA's career path tool – Highlight the variety of Cyber professional disciplines that enable Cyber T&E capabilities for your organization.
- **Re-cap**
- **Closing Thoughts – Lessons from the Captains**

DAU's Definition of Cybersecurity

- **Defense Acquisition University (DAU) Definition:**
  - "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

--DAU SE Brainbook, Cybersecurity Risk Mgt

Nine Cyber Terms (1-5) – Where and How

1. Cyberspace: JP 3-12

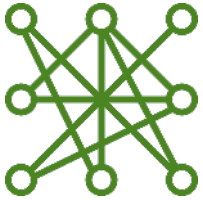
- A global domain within the information environment consisting of information technology infrastructures, data, networks, computers, and embedded systems.

2. Cyber Terrain: JP 3-12, Fidelis Blog

- A cumulative topography of cyber operational assets, security controls, data assets, and decision making.
- Malleable as new capabilities are introduced opening or closing attack vectors.
- Typically represented as layers illustrating physical connections, logical relationships, personas, and procedures/policies.

3. Key Cyber Terrain: MITRE

- Physical and logical elements of the domain that enable mission essential warfighting functions.



4. Attack Surface: NIST

- The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.

5. Attack Vector: Fortinet

- An attack vector is a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities.

Nine Cyber Terms (6-9) – Who

6. Blue Team (Defenders): NIST

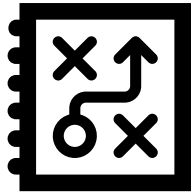
- Defends an enterprise's use of information systems by maintaining its security posture against real or simulated attacks over a significant period of time, in a representative operational context.
- During exercises, maintains security of information systems against the Red Team according to rules established and monitored with the help of a neutral group refereeing (i.e., the White Team).

7. Red Team (Aggressors): NIST

- A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture.
- To improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

8. Yellow Team (Builders): April Wright

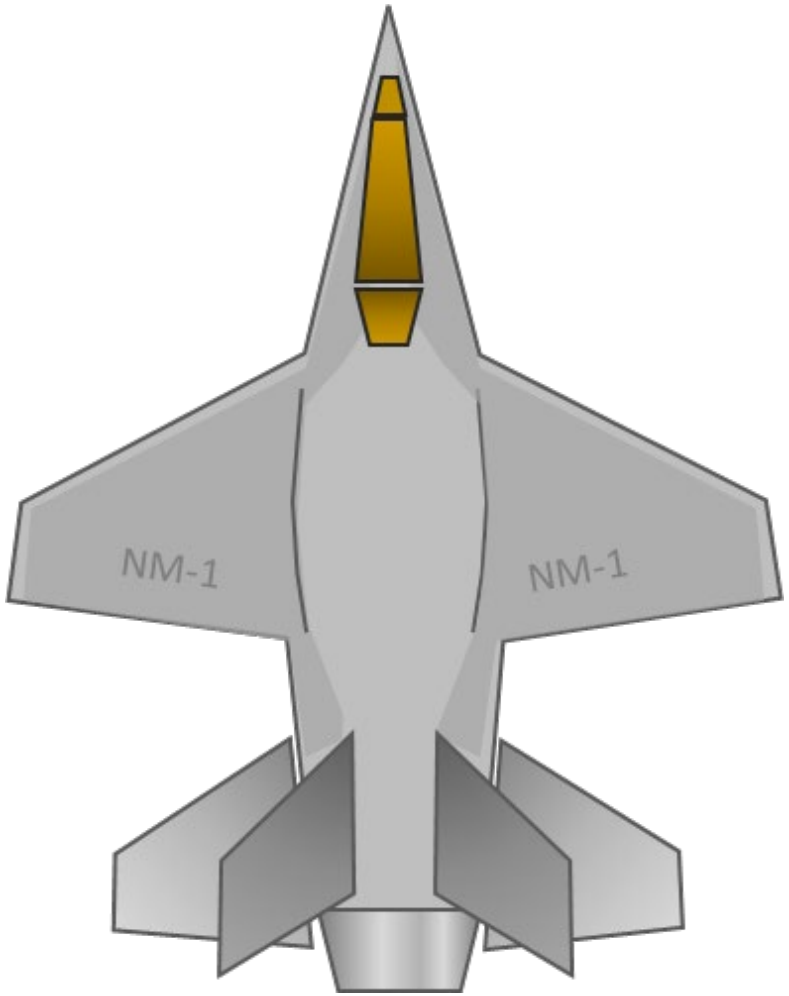
Practitioners in the art of coding to include programmers, application developers, software engineers and software architects.



9. White Team (Game Masters): April Wright

Oversees progress as an all-knowing, neutral, third-party, who defines exercises and testing rules of engagement, plans, organizes the other teams.

Notional Weapons Systems & Cyber Teams



Encryption & Decryption Modules

Storage Modules

Processing Modules

GPS & Geo Tagging Unit

RF Transmitters

Orange Team

Red Team Aggressors

Yellow Team Builders

Purple Team

Green Team

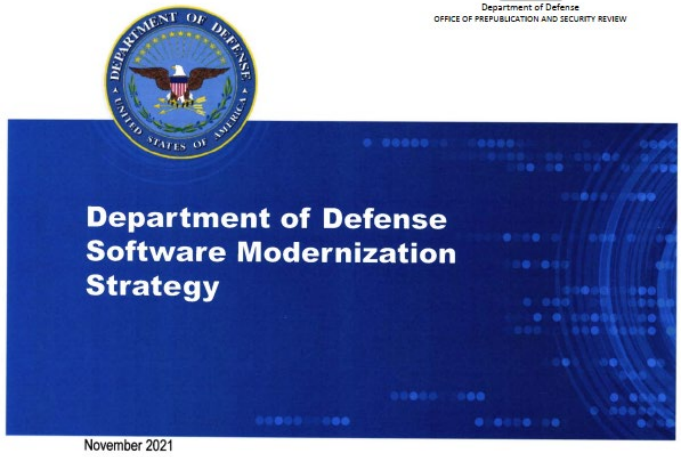
Blue Team Defenders

What's Vectoring Change In Cyber T&E?

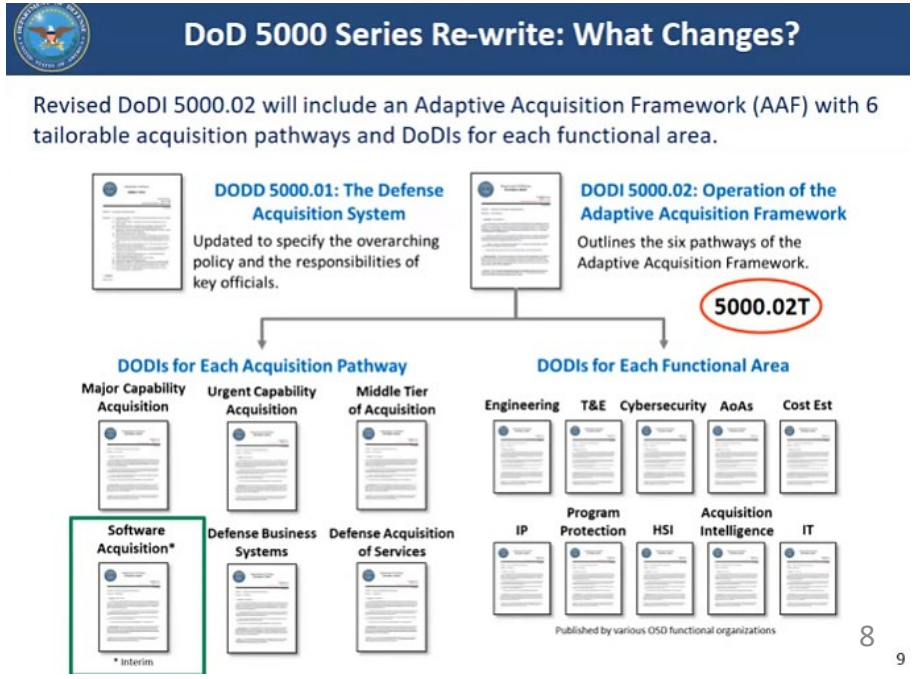
Unclassified

CLEARED
For Open Publication
Feb 02, 2022
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

- **DoD Software Modernization Strategy (Nov 2021):**
  - "**We must also lead this culture change, recognizing and instilling the notion that modernization is a perpetual journey** … one the Department must take to reinforce and guarantee the future of its warfighting dominance."



- **DODI 5000 Re-write**
  - "Recognize that **cybersecurity is a critical aspect of program planning**. It must **be addressed early and continuously** during the program life cycle to ensure cybersecurity operational and technical risks are identified and reduced and that fielded systems are capable, effective, and resilient."

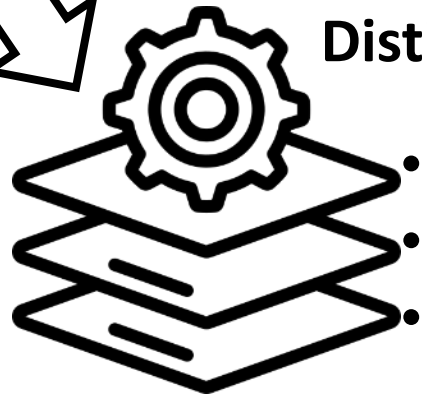


Where Are Changes In Cyber Occurring?

Cyberspace

Cyber Terrain

Decomposed Into Layers

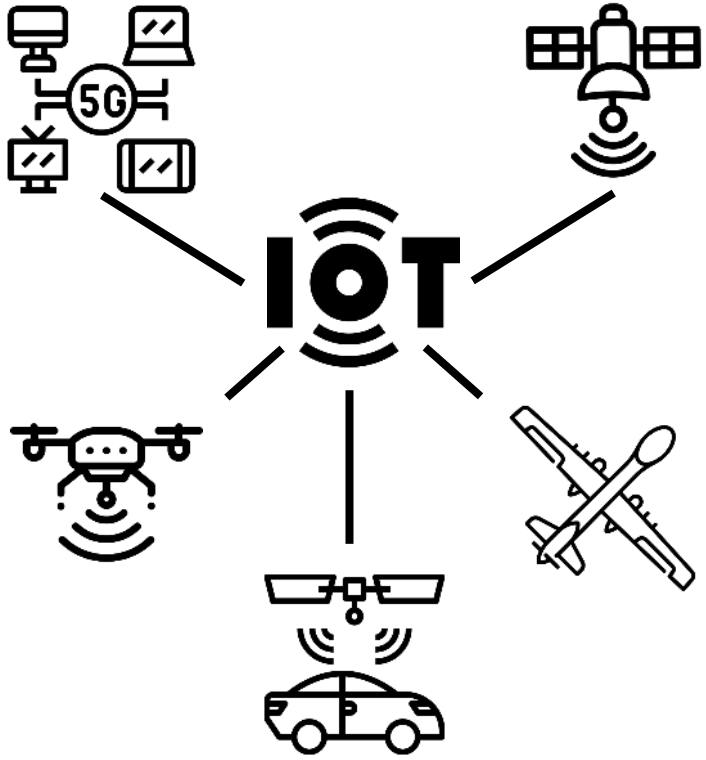


Distinct, Yet Interrelated

- Physical Network Layer
- Logical Network Layer
- Cyber-Persona Layer

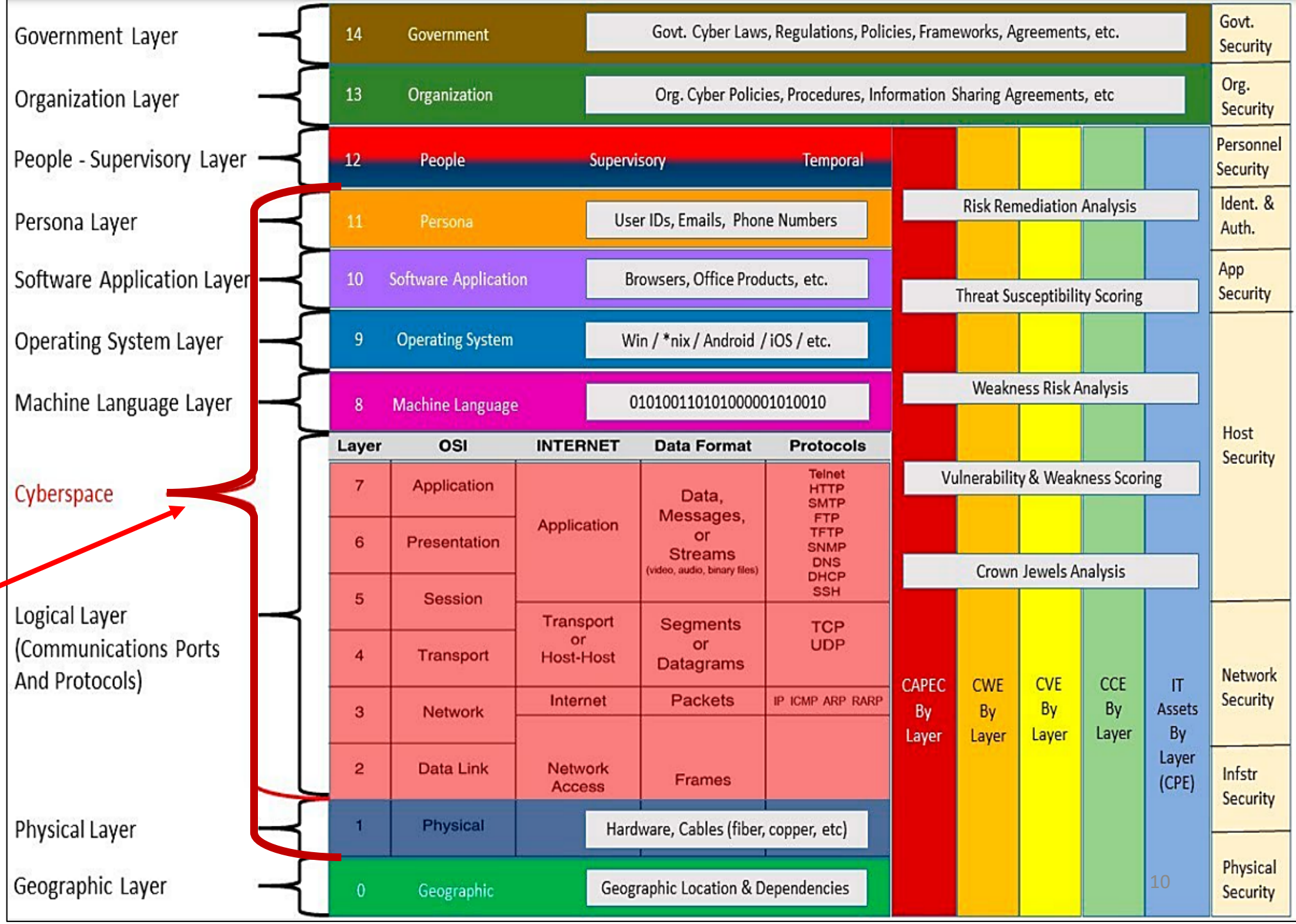
JP 3-12 Cyberspace Ops (page I-3)

The Growth in the Internet-Of-Things, Sensor Fusion, etc.

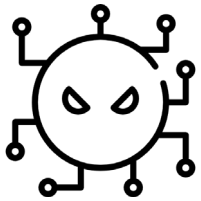


- **Another Layered View of the Cyber Terrain.**
- **Yep, It's an Eye Chart, but useful.**
- **Introduced by Shawn Riley in 2014.**
- **Chief Scientist at Orchestra Group**

Expanded for JP 3-12 Definition



Who is Vectoring Change in Cyber T&E



Advanced Persistent Threats (APT): NIST, NICCS

- An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).
- Establish and extend footholds within the information technology infrastructure of organizations.
- Continually exfiltrate information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future.
- Pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.

Strategic Competition - Nation State Actors: 2018 National Def Strategy Summary

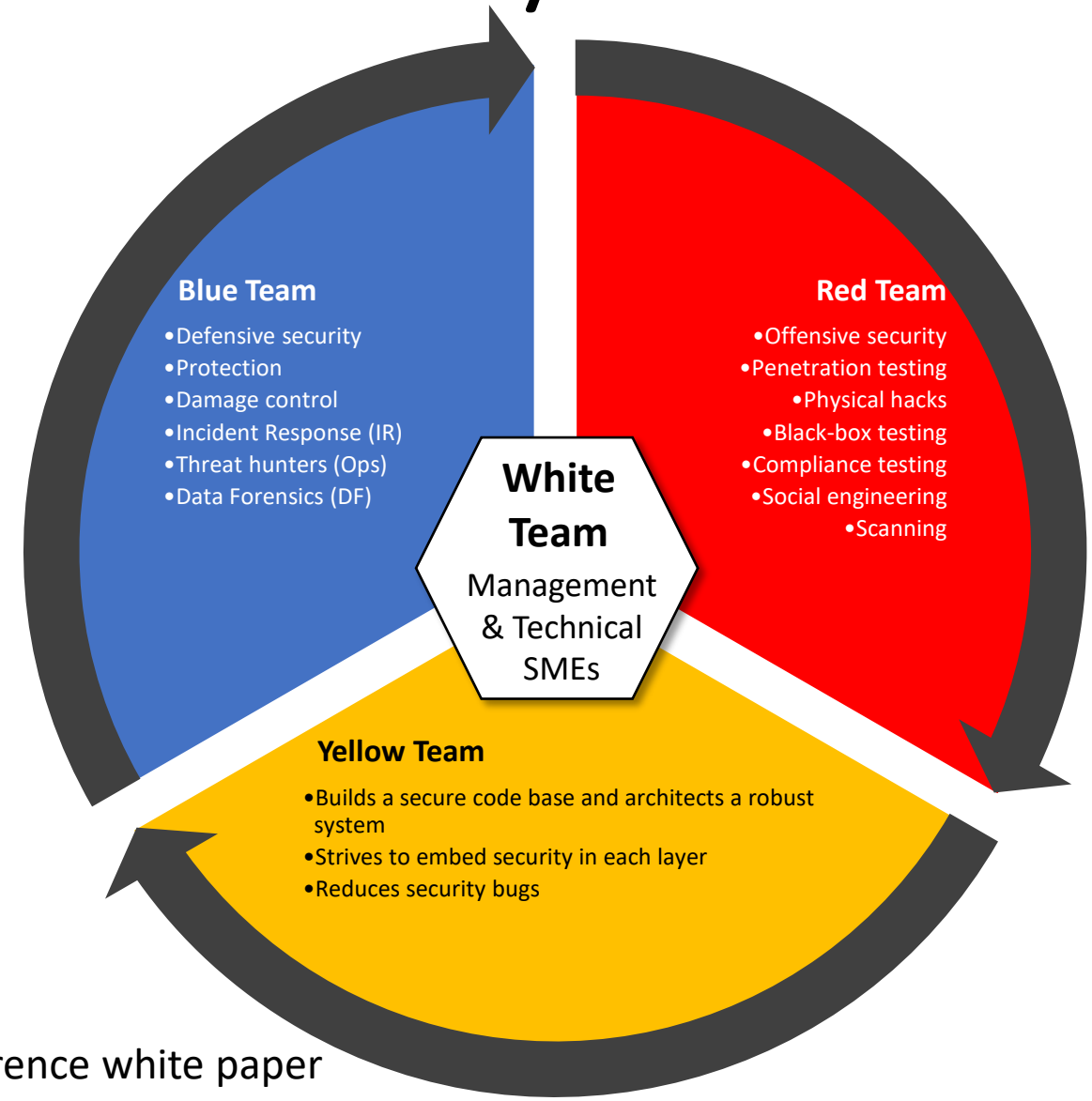
- Enemies, Economic Competitors, Allies.
- Instruments of National Power – Military, Informational, Diplomatic, Financial, Intelligence, Economic, Law, Development (MIDFIELD).

Stateless Actors – Terrorists & Violent Extremists

- Attackers with no borders.

Who Must We Assimilate into Cyber T&E?

- Red, Blue, and Yellow Teams have opposing goals.
- They share a mutual reliance on each other for each team's cybersecurity skills and perspective.



CREDIT:

Orange is the New Purple, April Wright's White Paper:

- Cyber color wheel is based on April Wright's 2017 BlackHat conference white paper and expanded on by Louis Cremen

Assimilate the Missing Pieces to Complete a Team

Orange Team

- Red educates Yellow on discovered vulnerabilities
- Ongoing interactions and working level meeting
- Red helps Yellow adopt a security mindset

Purple Team

- Joint Red and Blue activities
- Facilitate improvements in detection and defense
- Maximize Red's results
- Improve Blue's capability

Green Team

- Blue feedback to Yellow to improve code and design-based defense
- Improve data forensics capabilities such as logging

Blue Team

- Defensive security
- Protection
- Damage control
- Incident Response (IR)
- Threat hunters (Ops)
- Data Forensics (DF)

Red Team

- Offensive security
- Penetration testing
- Physical hacks
- Black-box testing
- Compliance testing
- Social engineering
- Scanning

White Team
Management & Technical SMEs

Yellow Team

- Developers
- Builds a secure code base
- Architects a robust system
- Strives for "correctness" with security embedded in each layer
- Reduce security bugs

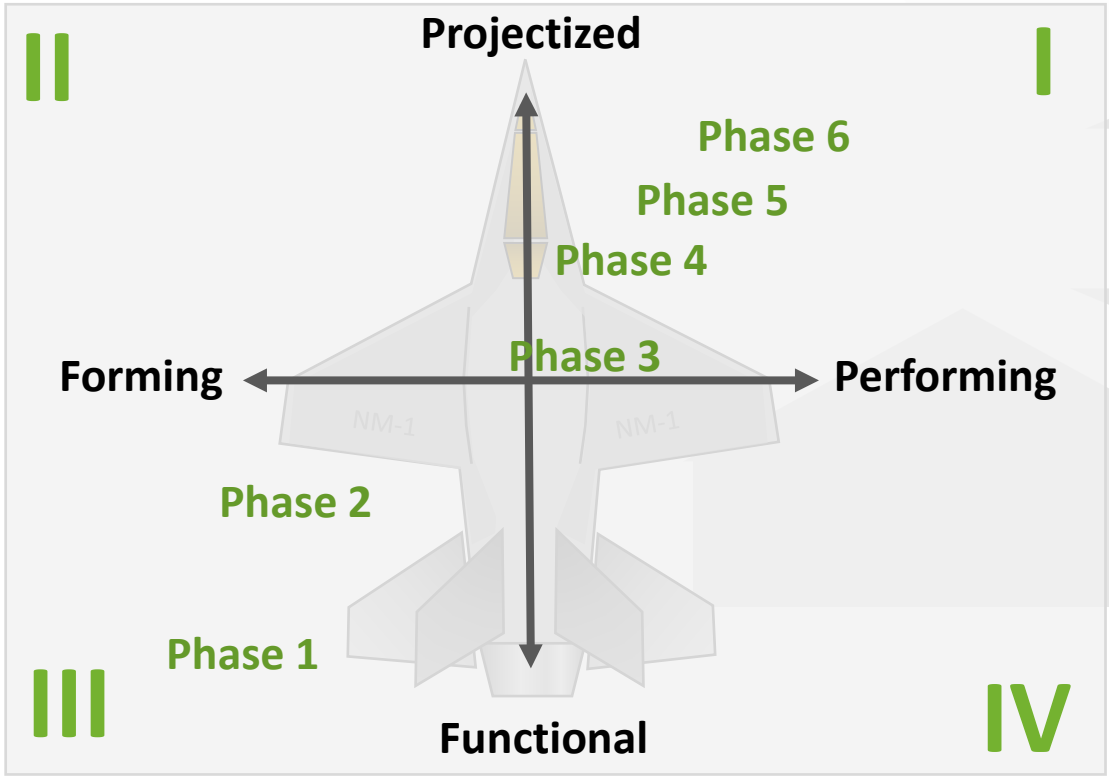
DevSecOps is a common software engineering approach, but we'll talk about that latter!

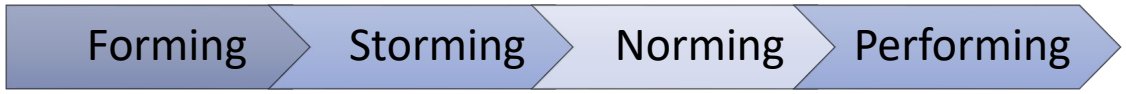
We Will Observe Through Two Lenses

PMBOK Organizational Structures

Leaders and functional managers **greatly influence** the autonomy of a team through its structure and **releasing control over time as the team matures**

- Projectized
- Strong Matrix
- Balanced Matrix
- Weak Matrix
- Functional





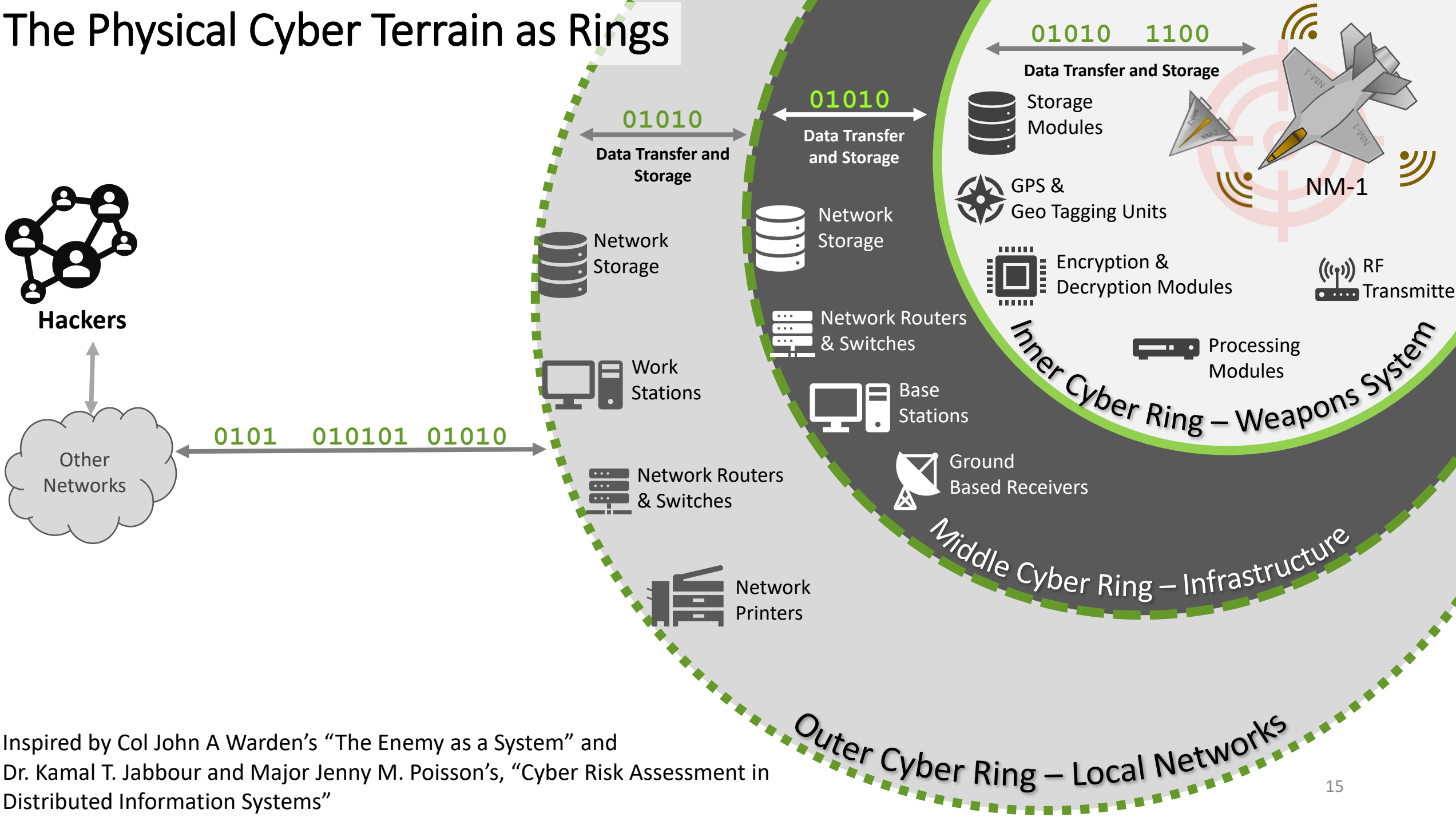
Tuckman's Stages of Group Development

- Positive conflict resolution eases the team into Norming
- Your mileage may vary!

Project managers and technical leads should observe their team's interactions and maturity **to set conditions** to reach performing

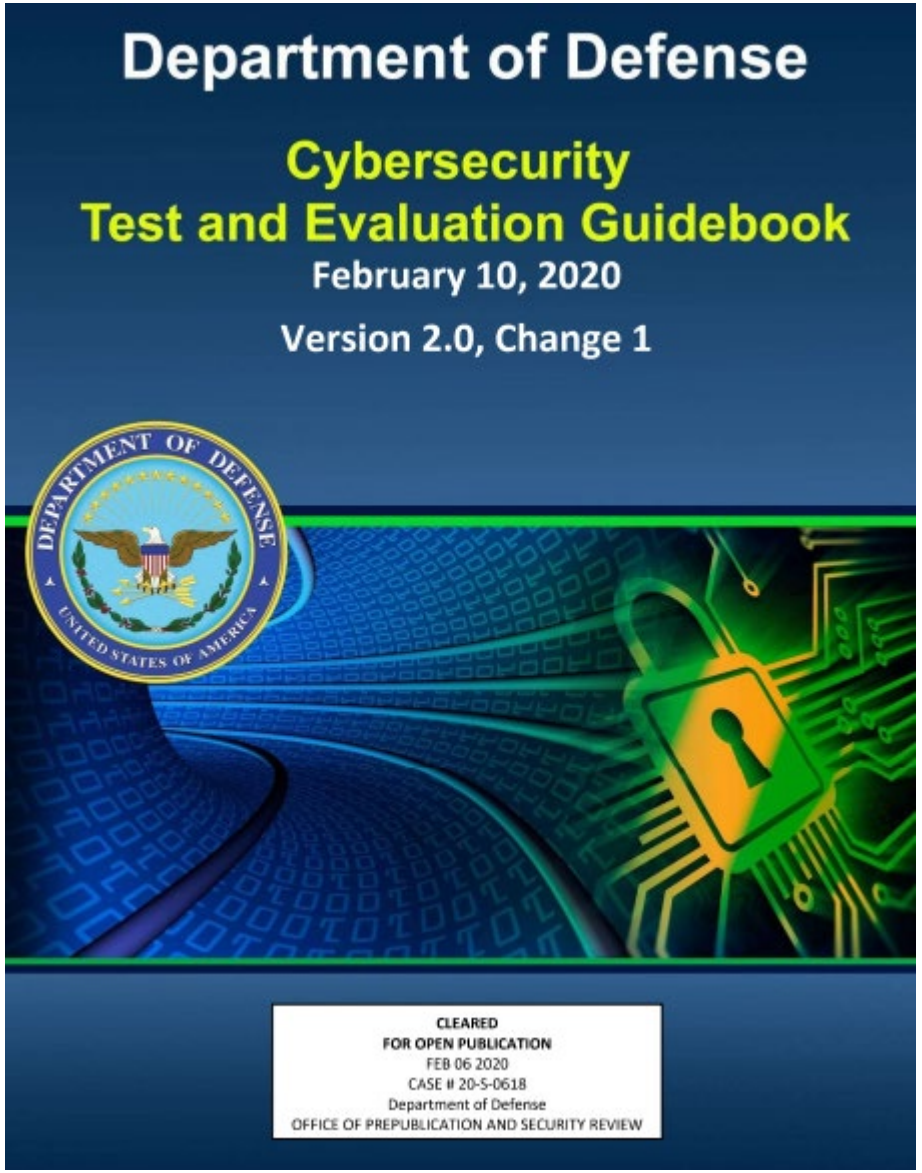
Project Management Institute (PMI)
Project Management Body Of Knowledge (PMBOK)

The Physical Cyber Terrain as Rings



Inspired by Col John A Warden's "The Enemy as a System" and
Dr. Kamal T. Jabbour and Major Jenny M. Poisson's, "Cyber Risk Assessment in Distributed Information Systems"

Assimilation During the Six Cyber T&E Phases



The goal of cybersecurity T&E is to identify and mitigate exploitable system vulnerabilities impacting operational resilience of military capabilities before system deployment to include safety, survivability, and security. (page 9)

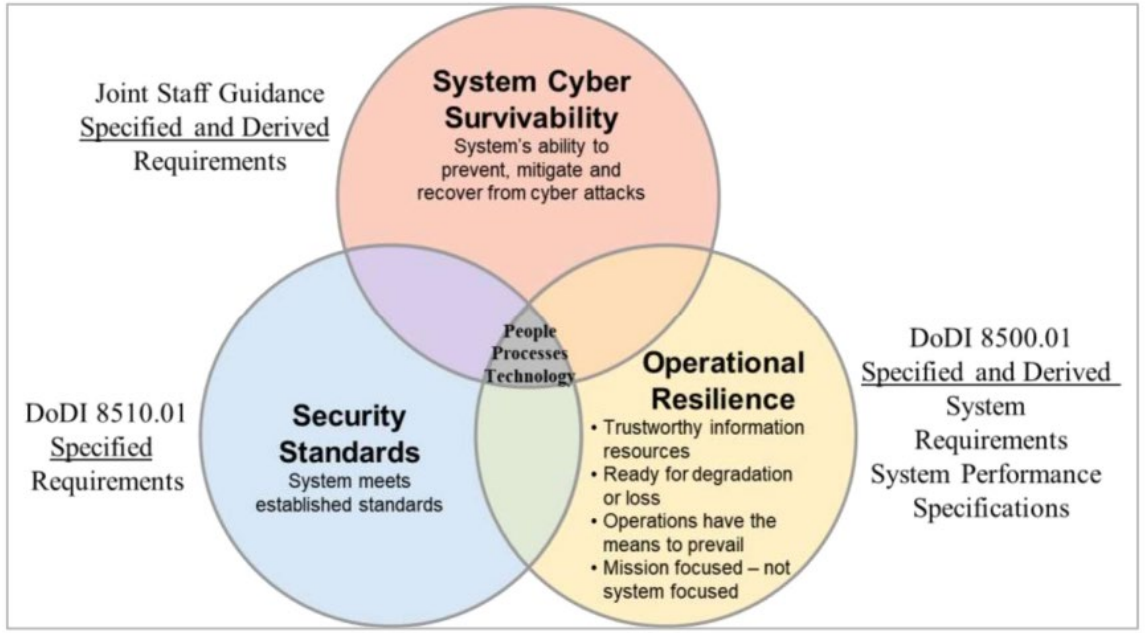
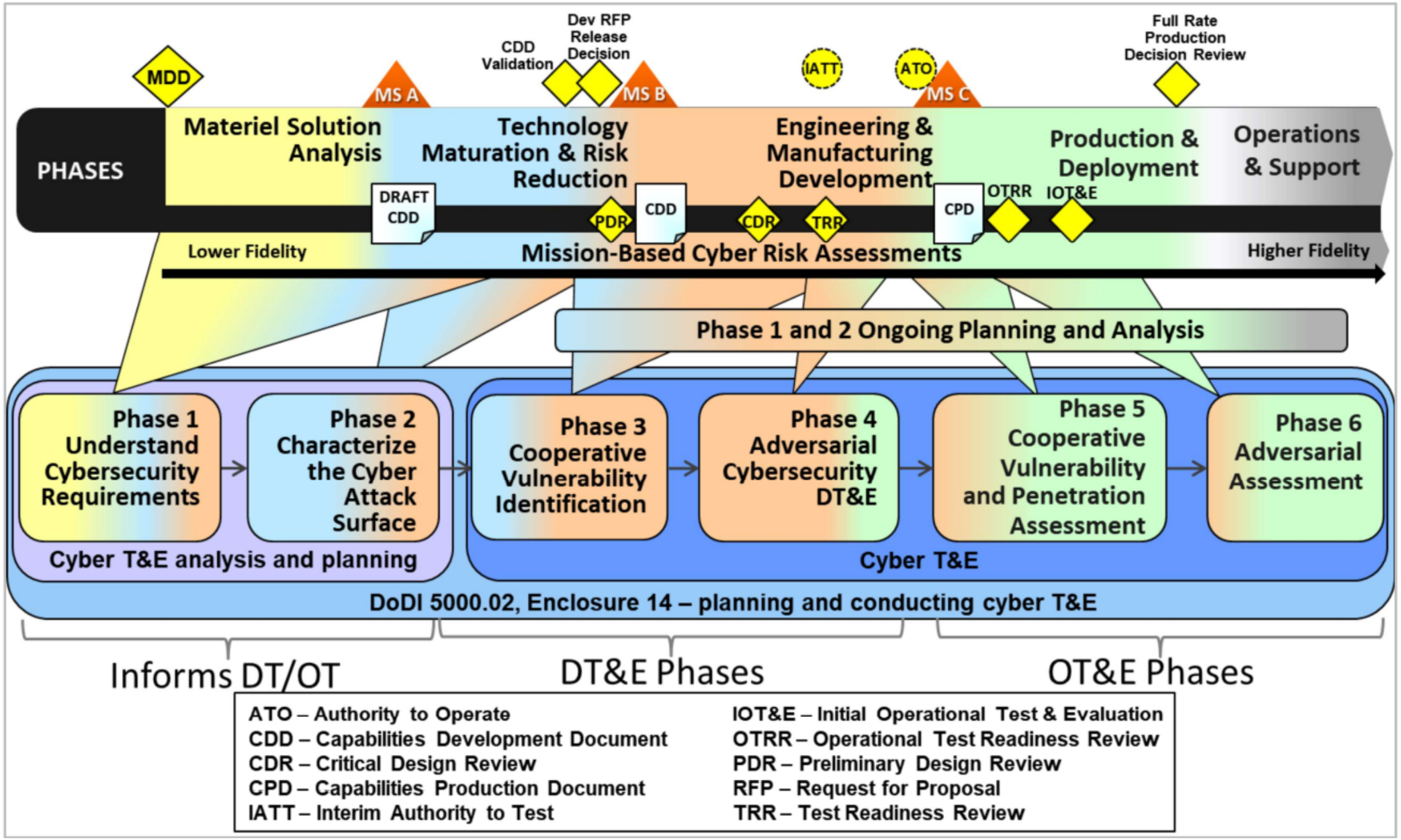


Figure 3-4. Cybersecurity Testing Requirement Venn Diagram



DOD Cybersecurity Test and Evaluation Guidebook, February 10, 2020, Version 2.0, Chg 1, pg 8

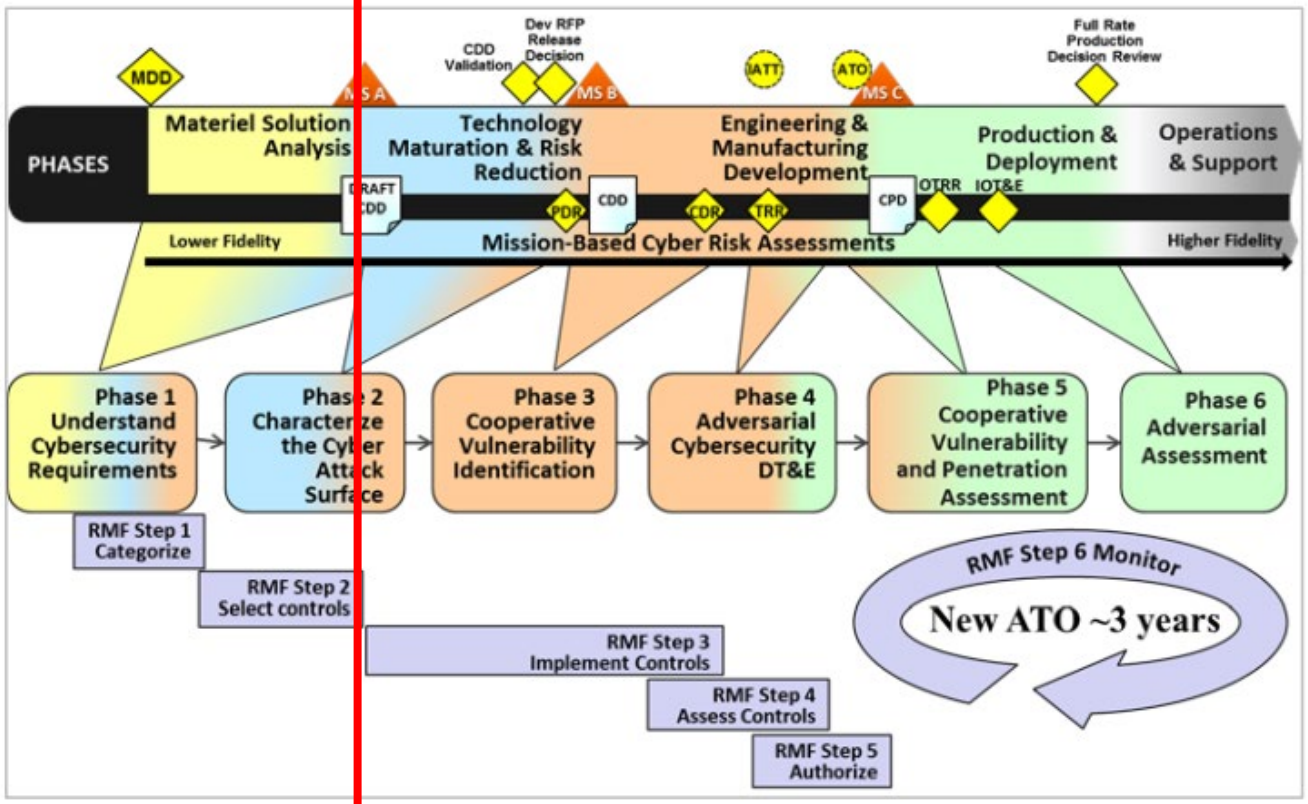
Before You Start, Form a Cybersecurity Working Group

- **The recommended participants in the CyWG are:**
  - CDT or system test lead if the CDT has not yet been appointed
  - SSE
  - ISSM
  - Lead Systems Engineer Representative
  - Lead Software Engineer/Architect
  - Lead DT&E Organization Representative
  - Critical or specialized sub-component, component or functionality developers and engineers
  - Operational Test Agency Representative
  - Cybersecurity DT&E Technical Experts (testers/analysts/assessors)
  - Cybersecurity OTA Technical Experts (testers/analysts/assessors)
  - Security Controls Assessor (SCA)
  - Cybersecurity Subject Matter Experts (SMEs)
  - Cyber-Intelligence SME
  - Software Assurance Testing SME
  - Scientific Test and Analysis Techniques (STAT) and/or Design of Experiments SME
  - Cyber Test Range Representative
  - Modeling and Simulation SME
  - Anti-tamper (AT) Representative
  - Interoperability Engineers, Representatives and Testers
  - CSSP and DCO Representatives
  - Active Duty System Operators
  - System Maintainers and Logisticians
  - Service-Specific T&E Policy Representative, if needed
  - Oversight organizations and stakeholders, if appropriate
  - Developers
  - Prime Contractor, if appropriate

DOD Cybersecurity Test and Evaluation Guidebook, February 10, 2020, Version 2.0, Chg 1, pg 11-12

Phase 1: Understand the Cybersecurity Requirements

- Examine the system's cybersecurity, system cyber survivability, and operational resilience requirements for developing initial and subsequent approaches and plans for conducting contractor and government cybersecurity T&E.

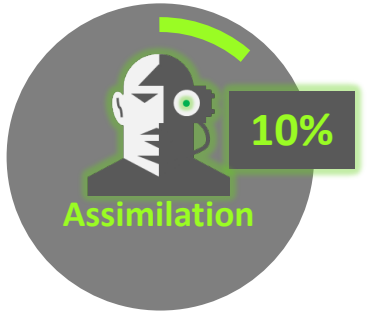


Red Team Aggressors

Yellow Team Builders

Blue Team Defenders

DOD Cybersecurity Test and Evaluation Guidebook, February 10, 2020, Version 2.0, Chg 1, pg 8

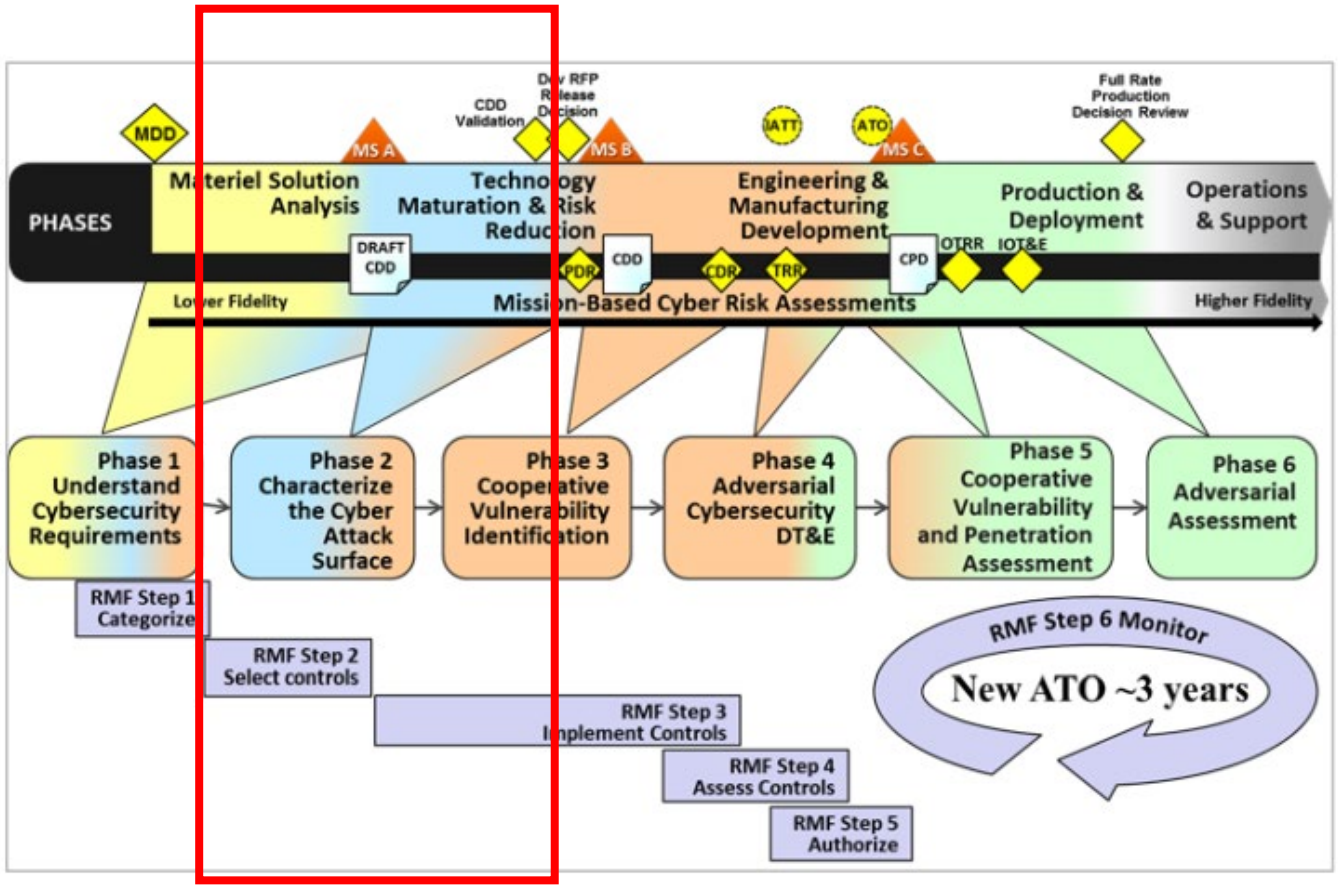


Phase 1: Understand the Cybersecurity Requirements

- **Tuckman:** Forming.
- **PMI Org:** Functional.
- Experienced members guiding junior members in T&E practices.
- Roles and lines of authority may be unclear—avoid this with a RACI chart!
- Team is gathering situational awareness regarding requirements.
- Categorize and select controls in Risk Management Framework (RMF).
- Still highly polished cylinders of excellence and more functionally aligned than aligned with a multi-disciplined matrixed team.

Phase 2: Characterize the Attack Surface

- Government and contractor test teams identify vulnerabilities and avenues of attack an adversary may use to exploit the system and develop plans to evaluate the impacts to the mission.



Red Team Aggressors

Yellow Team Builders

Blue Team Defenders

DOD Cybersecurity Test and Evaluation Guidebook, February 10, 2020, Version 2.0, Chg 1, pg 8

Phase 2: Identifying the Key Cyber Terrain

- Mission driven analysis.
- Example is a layered view linking mission to component.
- The teams gain a shared understanding of how the system is logically linked.
- Key Cyber terrain is the physical and logical elements of the domain that enable mission essential warfighting functions.

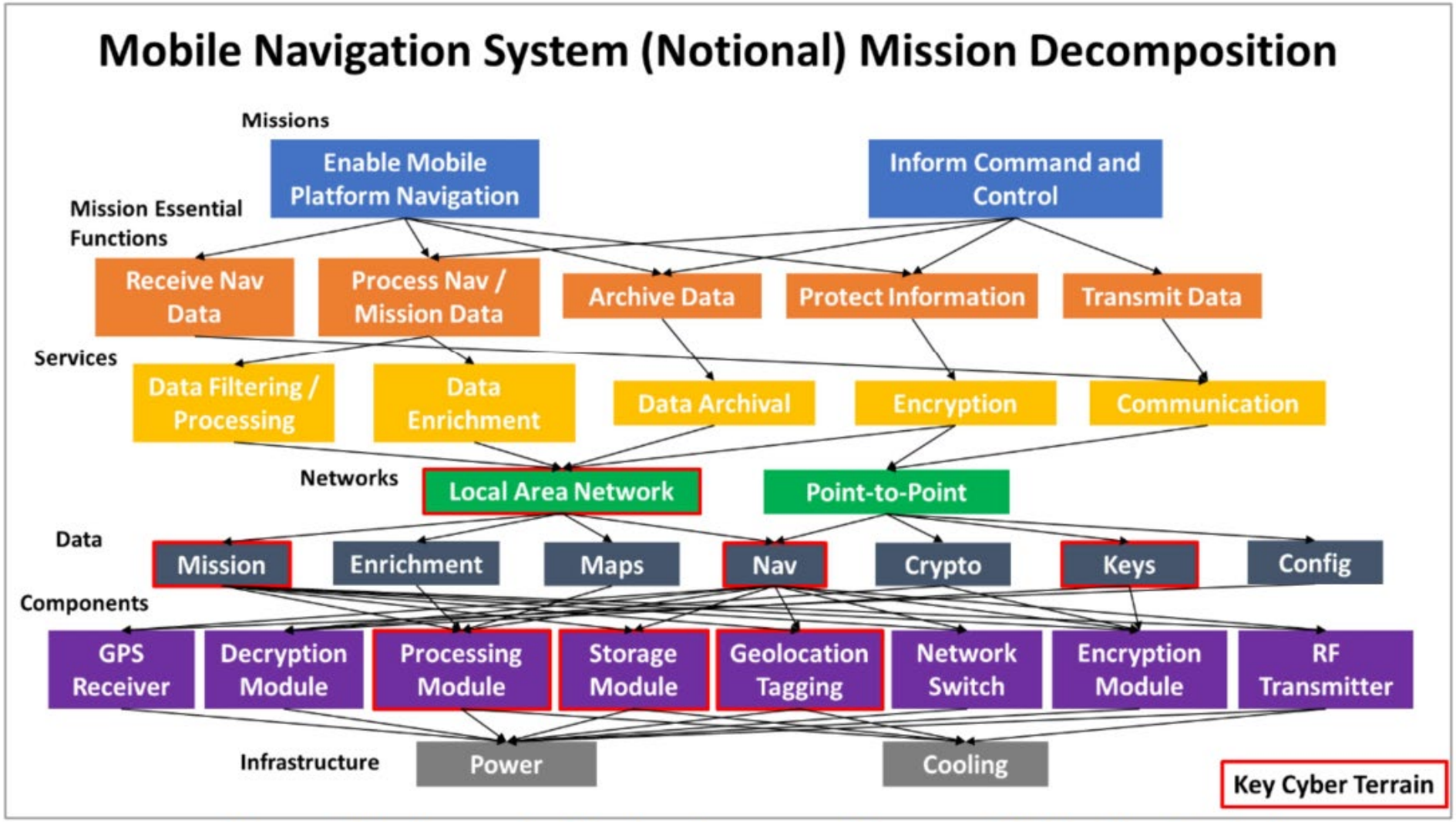


Figure 5-3. Example Mission Decomposition and Criticality Analysis

Phase 2: Characterizing the System's Attack Surface

- Example of a System Map and possible attack points.
- Red team has an opportunity to feed potential attack information back to Yellow team members and leading to Phase 3 – Cooperative Vulnerability Identification.

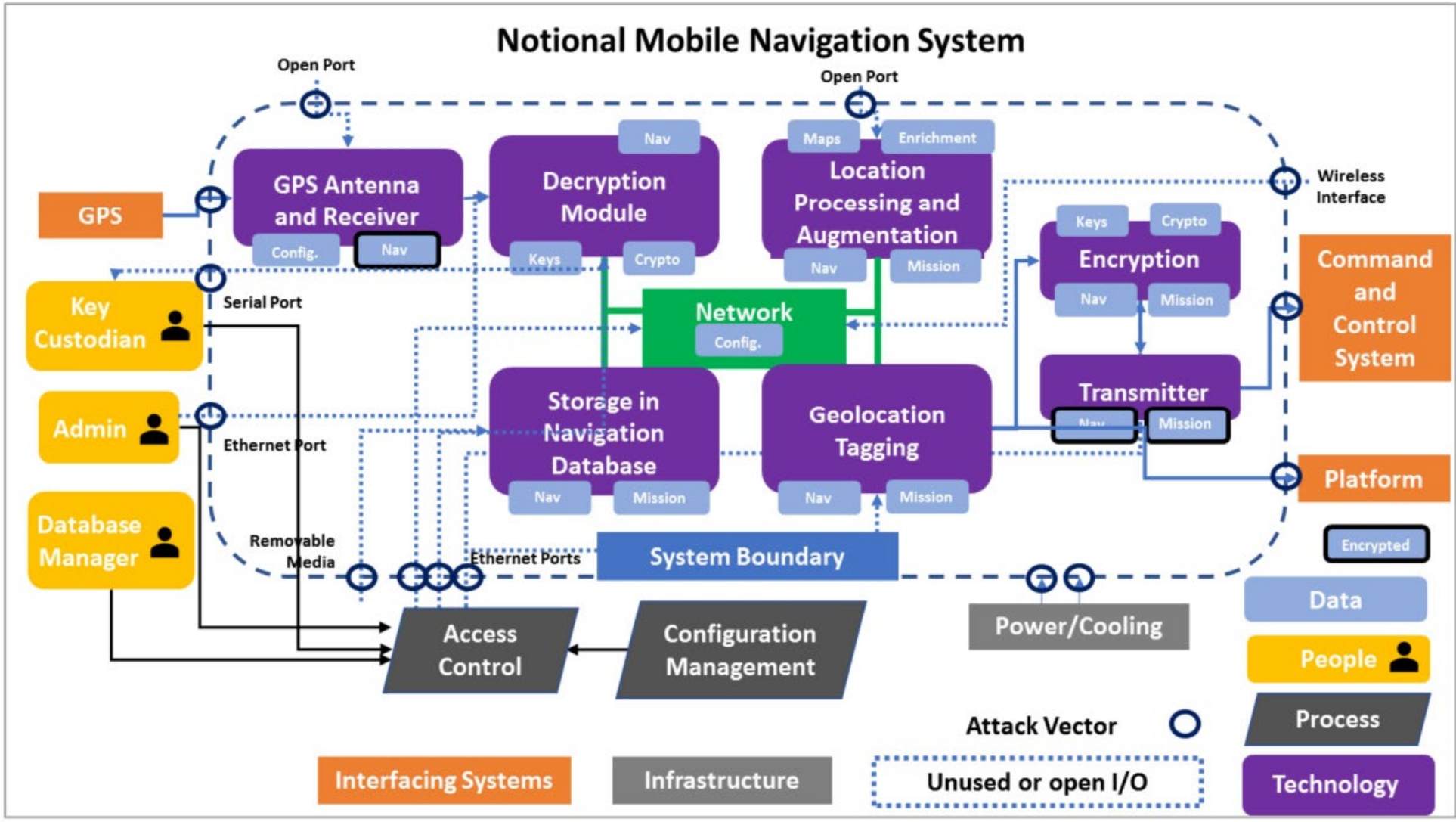
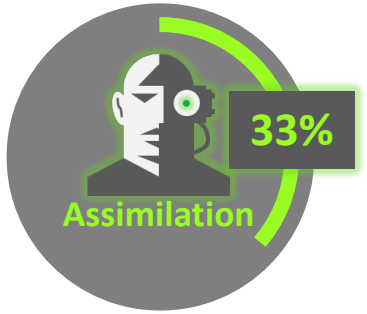


Figure 5-4. Example Cyber-Attack Surface System Diagram

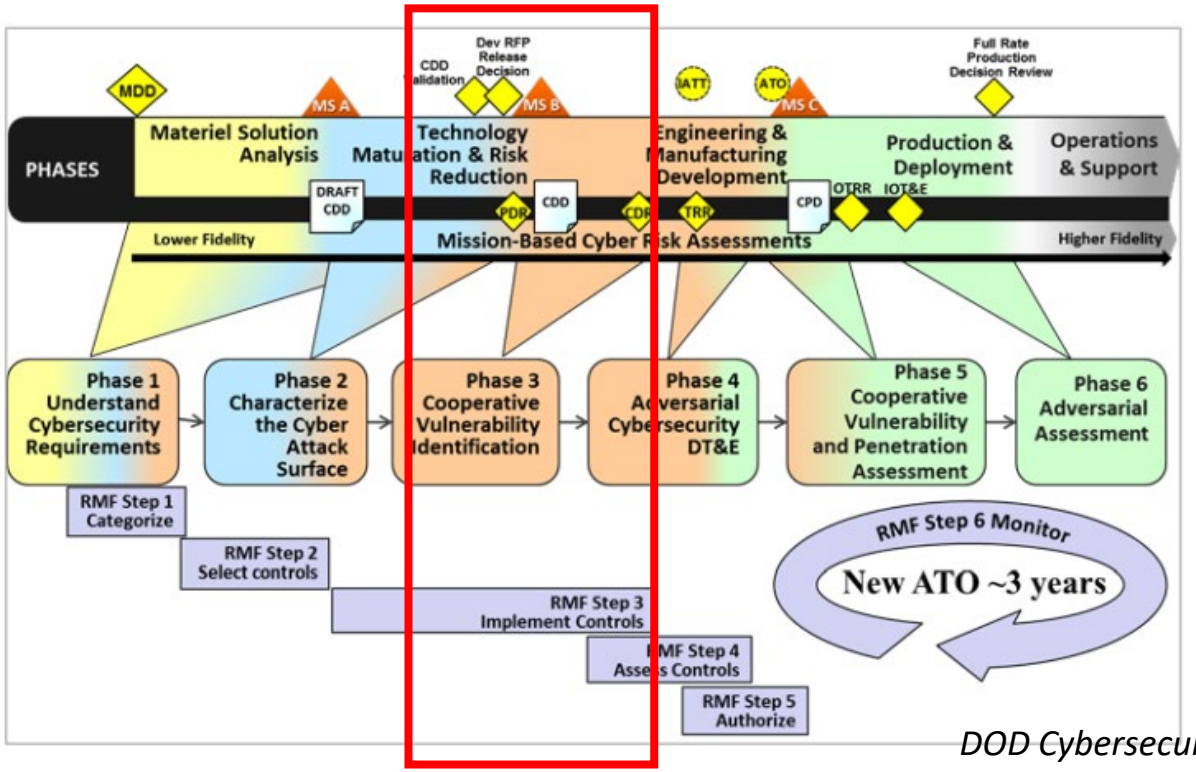


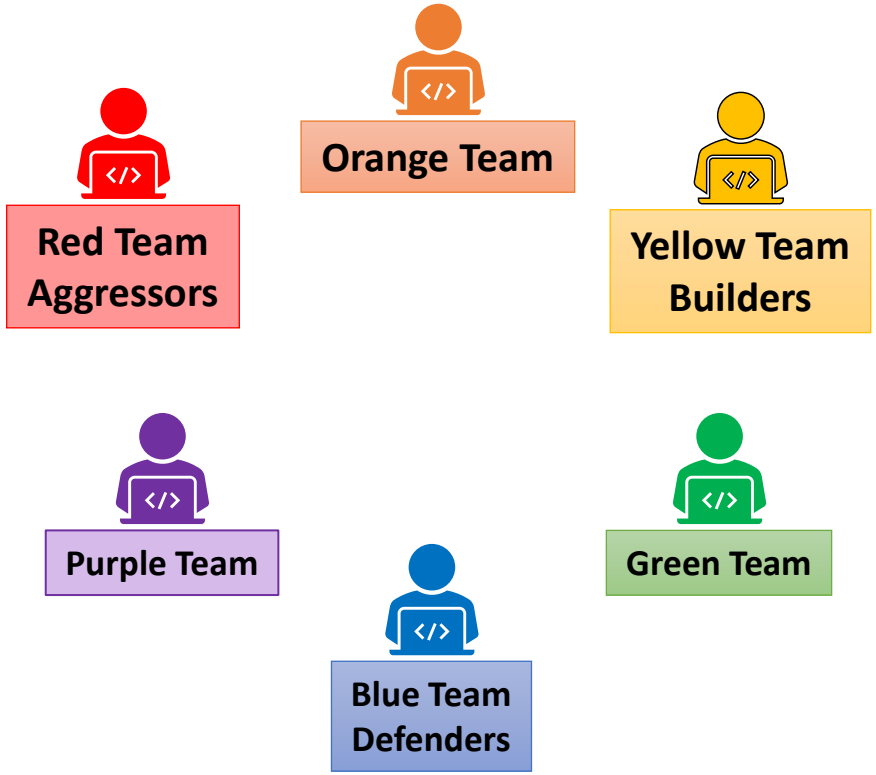
Phase 2: Characterize the Attack Surface

- **Tuckman:** Forming to Storming.
- **PMI Org:** Weak Matrix.
- Focus is on documented system data flow and architecture.
- Team may still be enthusiastic, but the workload and time constraints may start to take its toll.
- Selecting and implementing Risk Management Framework (RMF) controls.
- Communication barriers eroding and less functionally aligned moving toward a matrixed team.

Phase 3: Cooperative Vulnerability Identification

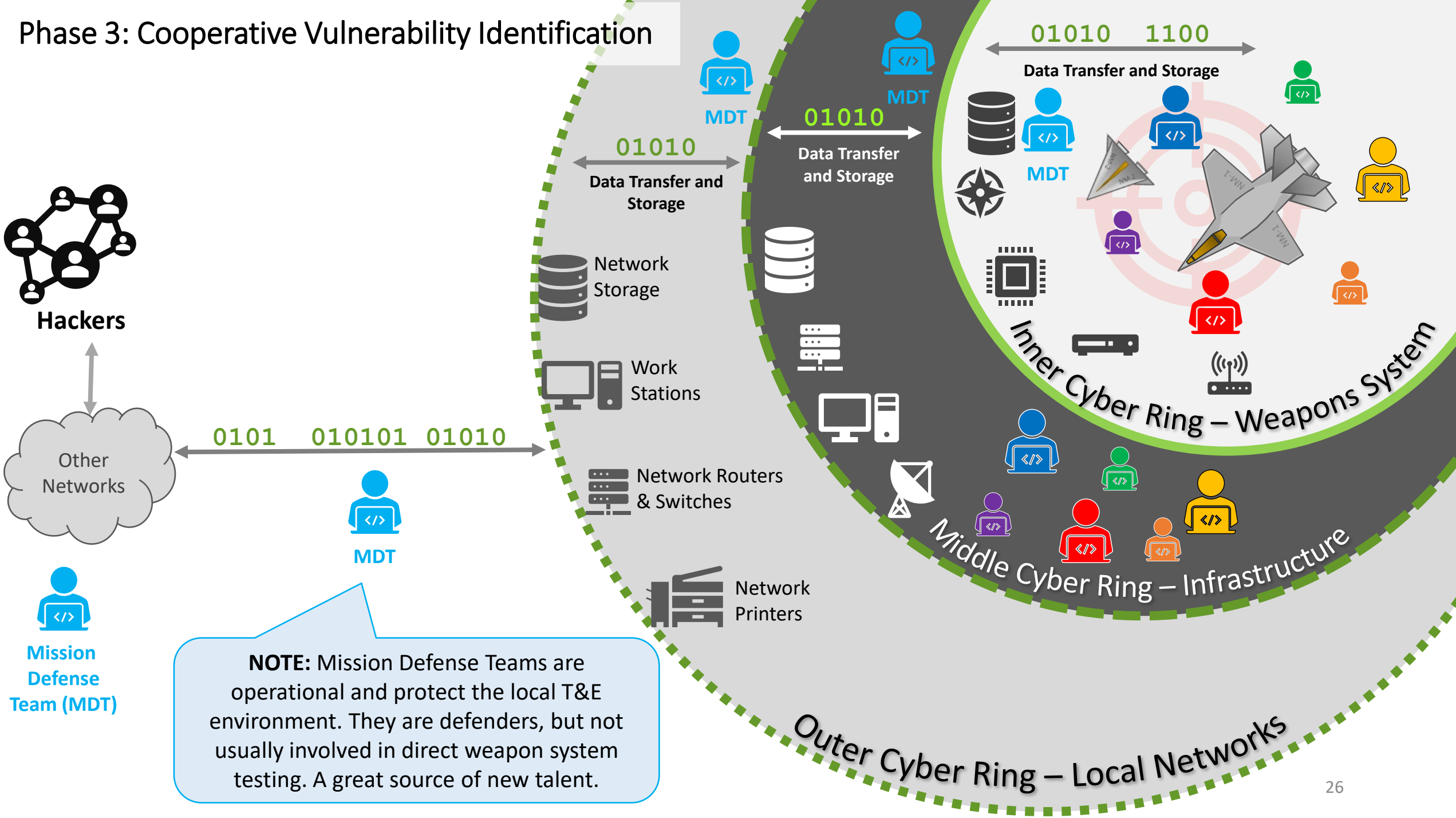
- Testing early to verify cybersecurity and operational resilience and identify vulnerabilities and inform implementing any needed mitigations.
- Using multiple tailored test events, vulnerability identification informs contractor and government system designers, developers, and engineers of needed system cyber survivability and operational resilience improvements to reduce risk. Phase 3 is iterative during contractor development and includes regression testing to verify implemented mitigations.
- Iterative during government DT&E.



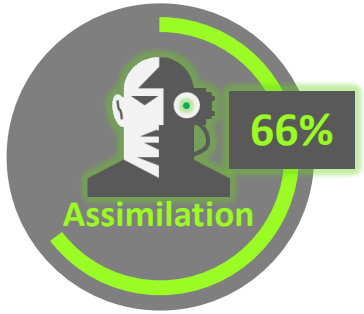


DOD Cybersecurity Test and Evaluation Guidebook, February 10, 2020, Version 2.0, Chg 1, pg 8

Phase 3: Cooperative Vulnerability Identification

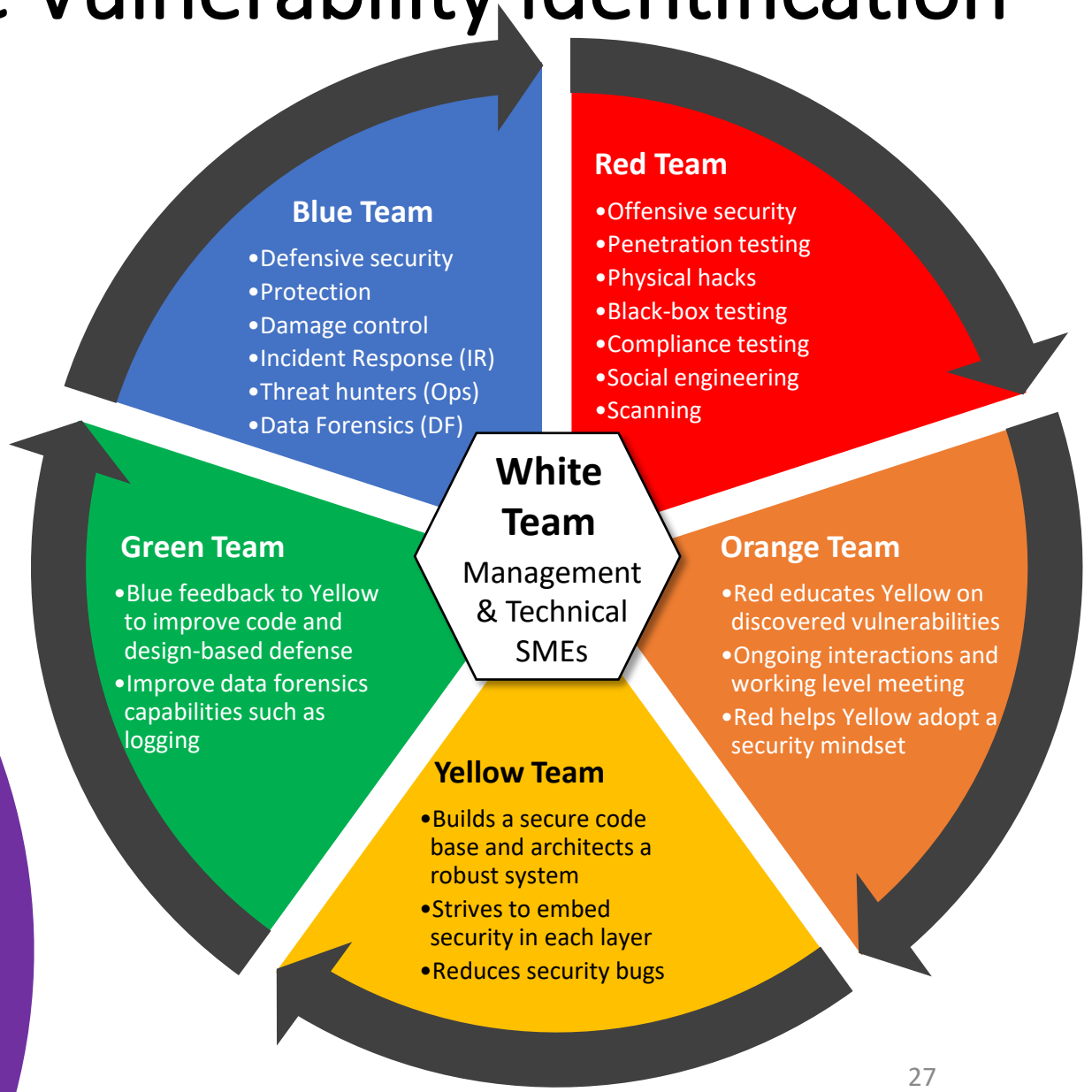


NOTE: Mission Defense Teams are operational and protect the local T&E environment. They are defenders, but not usually involved in direct weapon system testing. A great source of new talent.



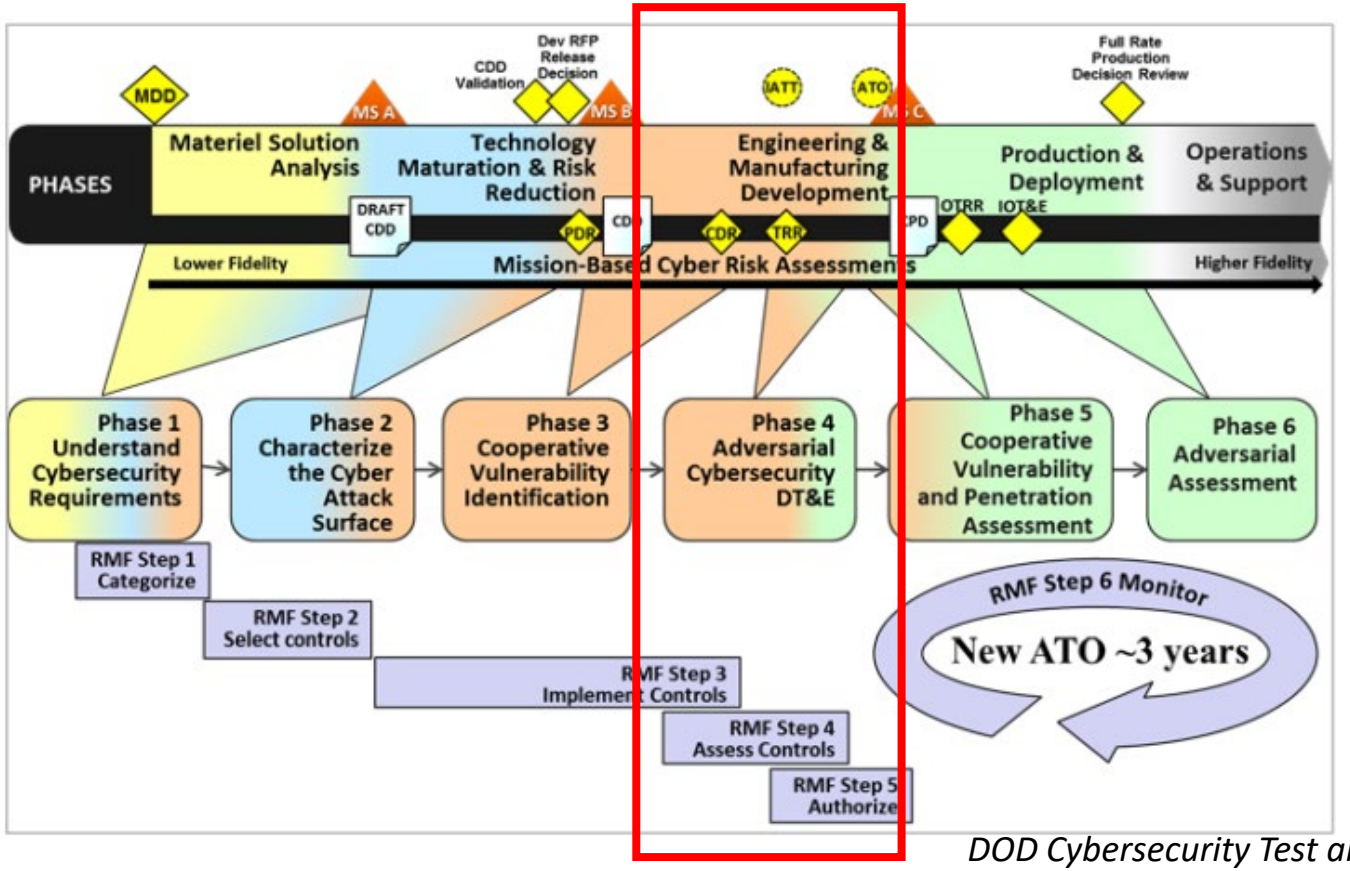
Phase 3: Cooperative Vulnerability Identification

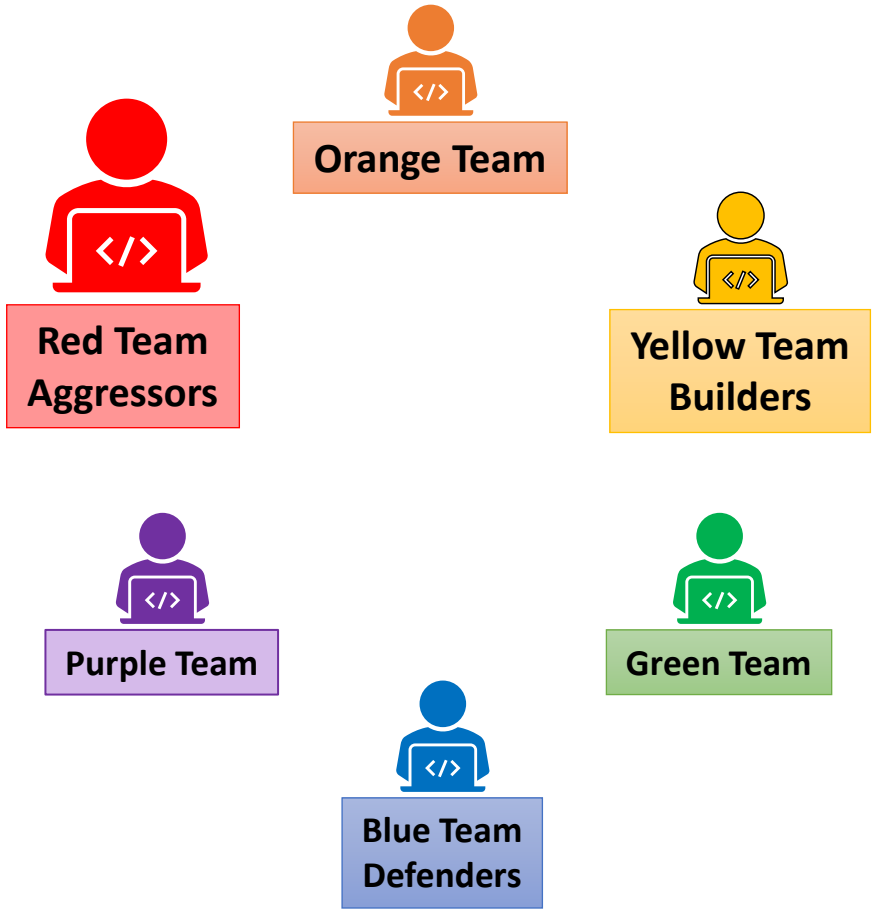
- **Tuckman:** Storming to Norming.
- **PMI Org:** Strong Matrix.
- Implementing and assessing Risk Management Framework (RMF) controls.
- Communication barriers eroding and relationships are forming.
- Iterative testing requires interaction and cooperation.
- There's another Blue team!
  - Mission Defense Teams.
  - Threat hunters and data forensics.



Phase 4: Adversarial Cybersecurity DT&E

- Integrated contractor and government adversarial test teams test critical functionality.
- Cybersecurity and operational resilience testing are conducted during system development using a mission context.
- Iterative during contractor system development.





DOD Cybersecurity Test and Evaluation Guidebook, February 10, 2020, Version 2.0, Chg 1, pg 9

Phase 4: Adversarial Cybersecurity DT&E

- Heavy interaction between contractor and government Cyber T&E subject matter experts.
- Focus is on discovering bugs and defects early (Shift Left).
- Unit, Integration, System, and Integrity Tests.

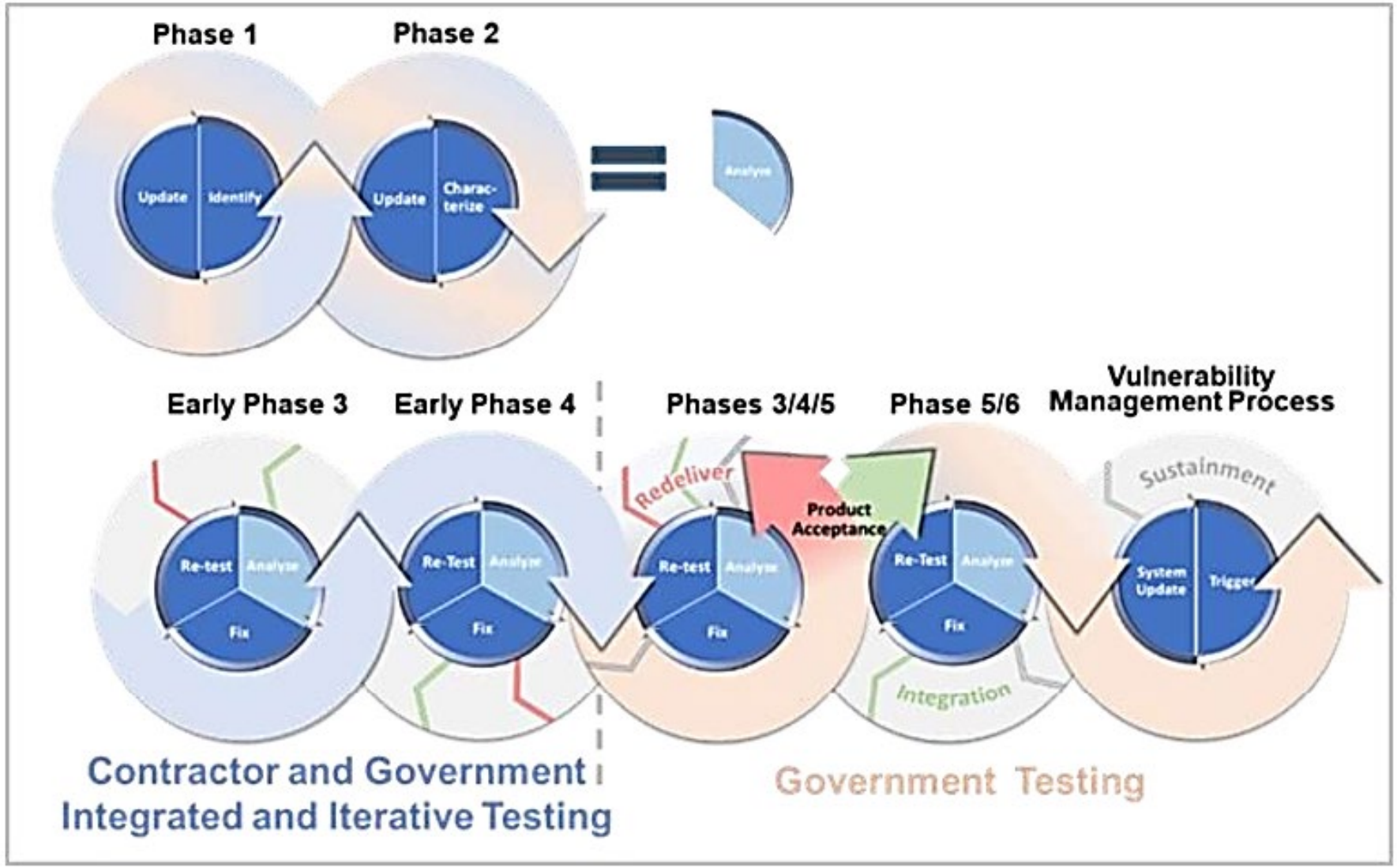
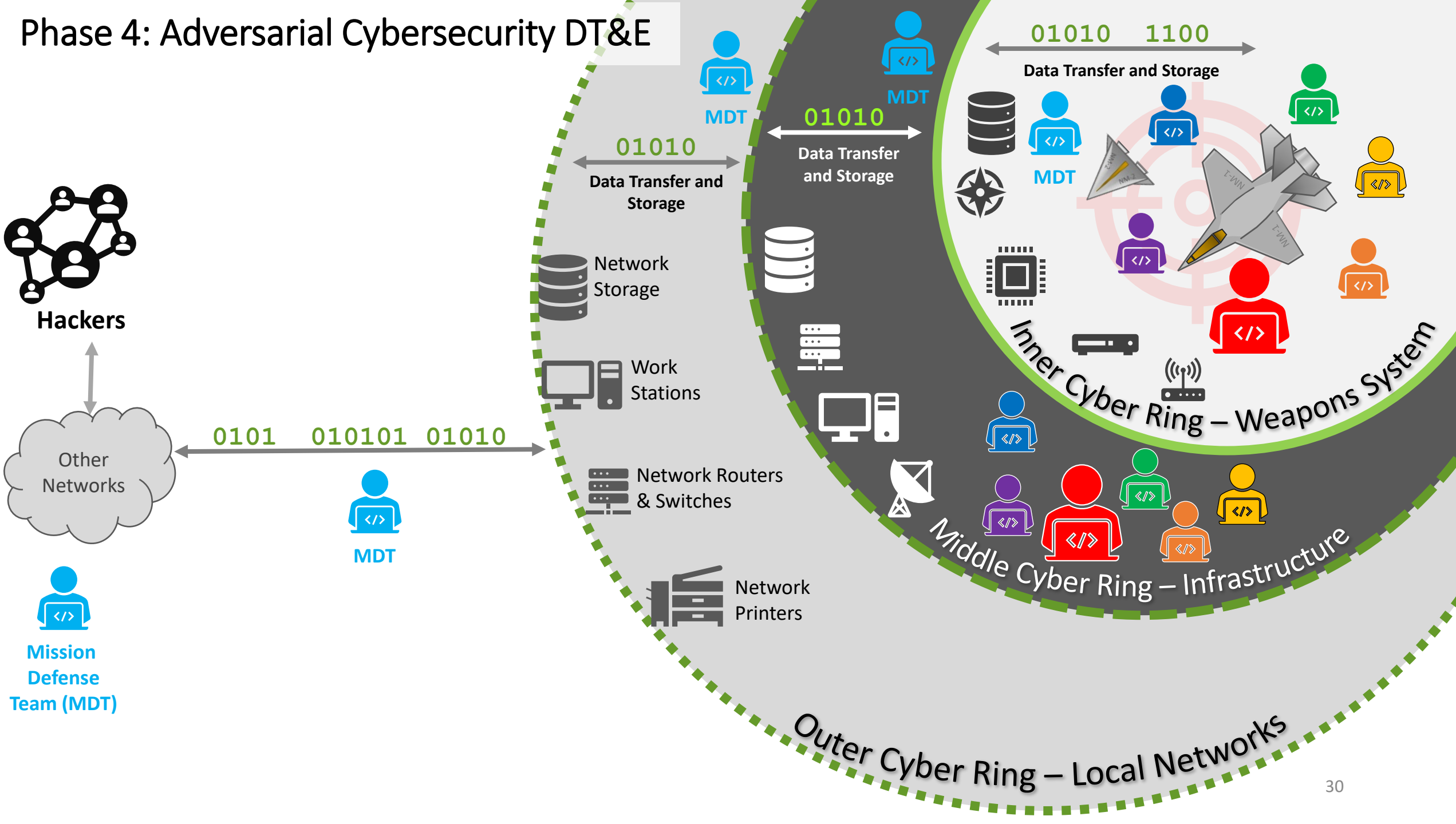


Figure C-2. Tailored Cybersecurity T&E 6 Phase Process

Phase 4: Adversarial Cybersecurity DT&E

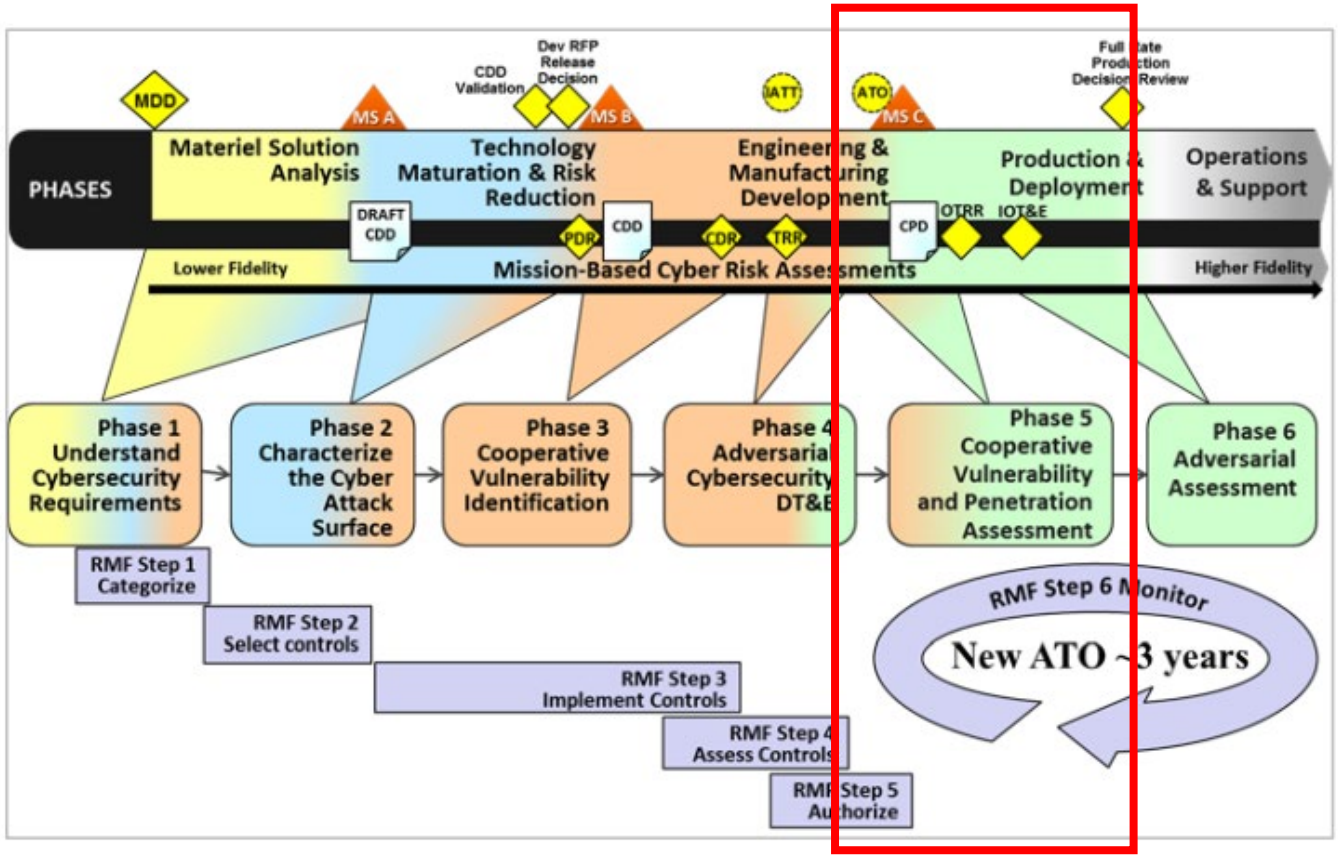


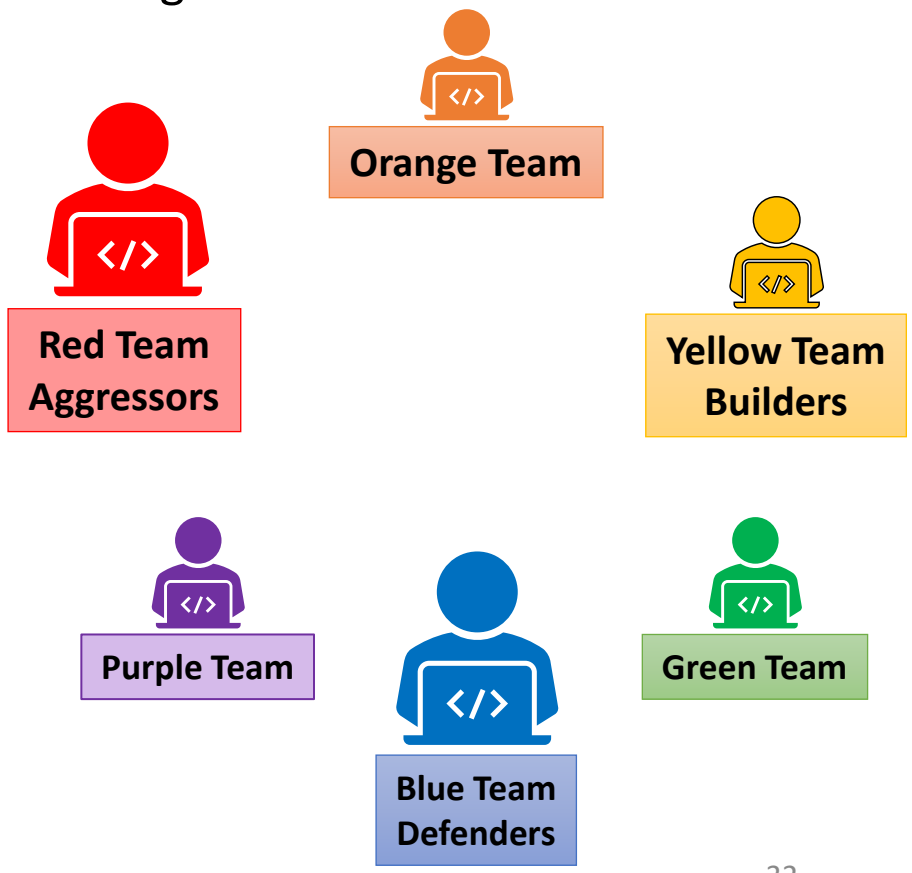
Phase 4: Adversarial Cybersecurity DT&E

- **Tuckman:** Performing.
- **Matrix:** Strong Matrix.
- Storming may occur with test failures.
- “All we hear is criticism and failure!”
- Teams are forged in the fire of battle!
- Implementing and assessing Risk Management Framework (RMF) controls.
- Obtaining Authorizations.
- Team more familiar with the T&E mission and attuned to the system under test’s requirements.

Phase 5: Cooperative Vulnerability and Penetration Assessment

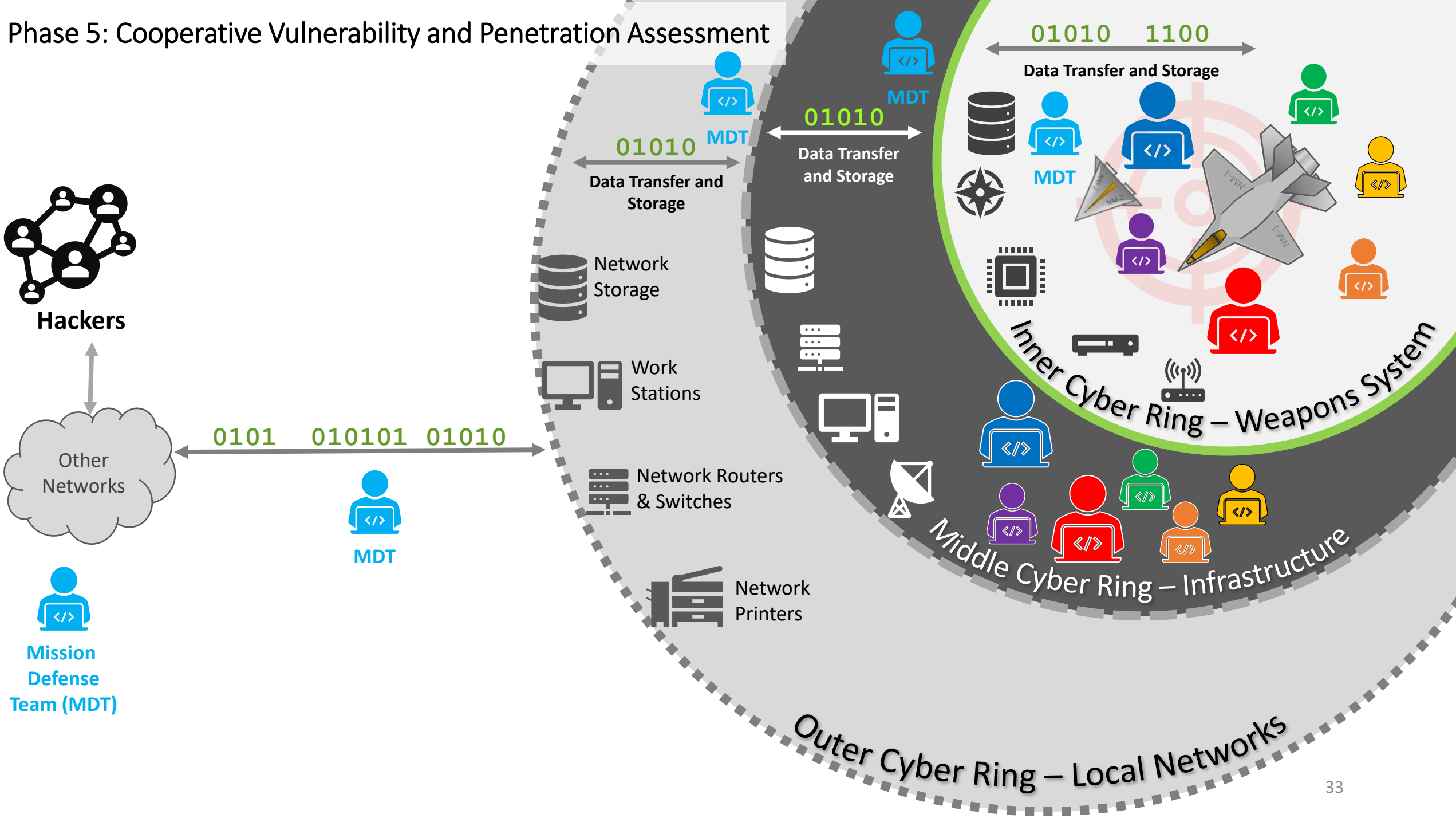
- Use data from cooperative cybersecurity test events to characterize the cybersecurity and resilience of a system in an operational context and provide reconnaissance of the system in support of the Adversarial Assessment.
- This Phase includes assessing all test data from prior testing and is not a single test event.





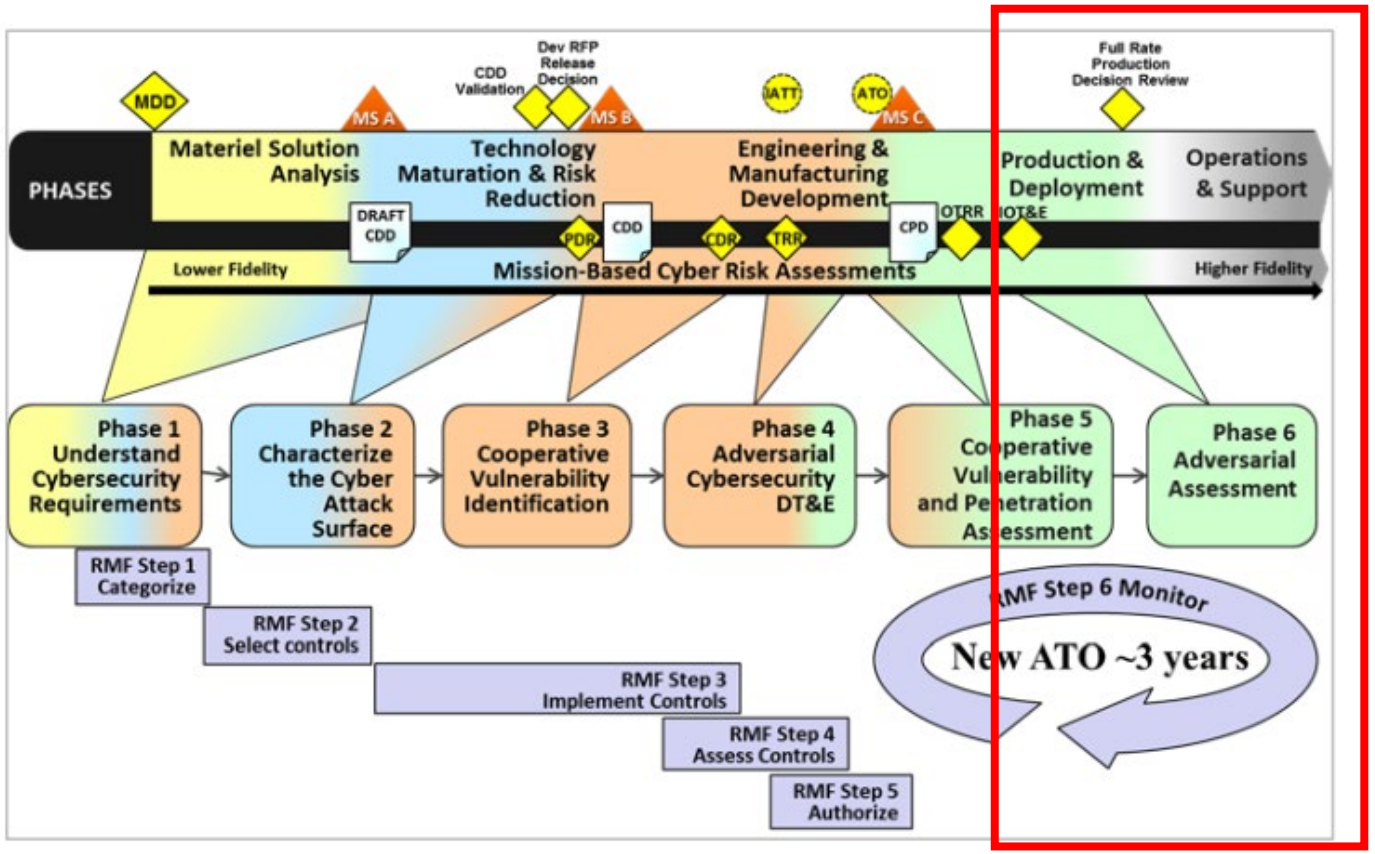
DOD Cybersecurity Test and Evaluation Guidebook, February 10, 2020, Version 2.0, Chg 1, pg 9

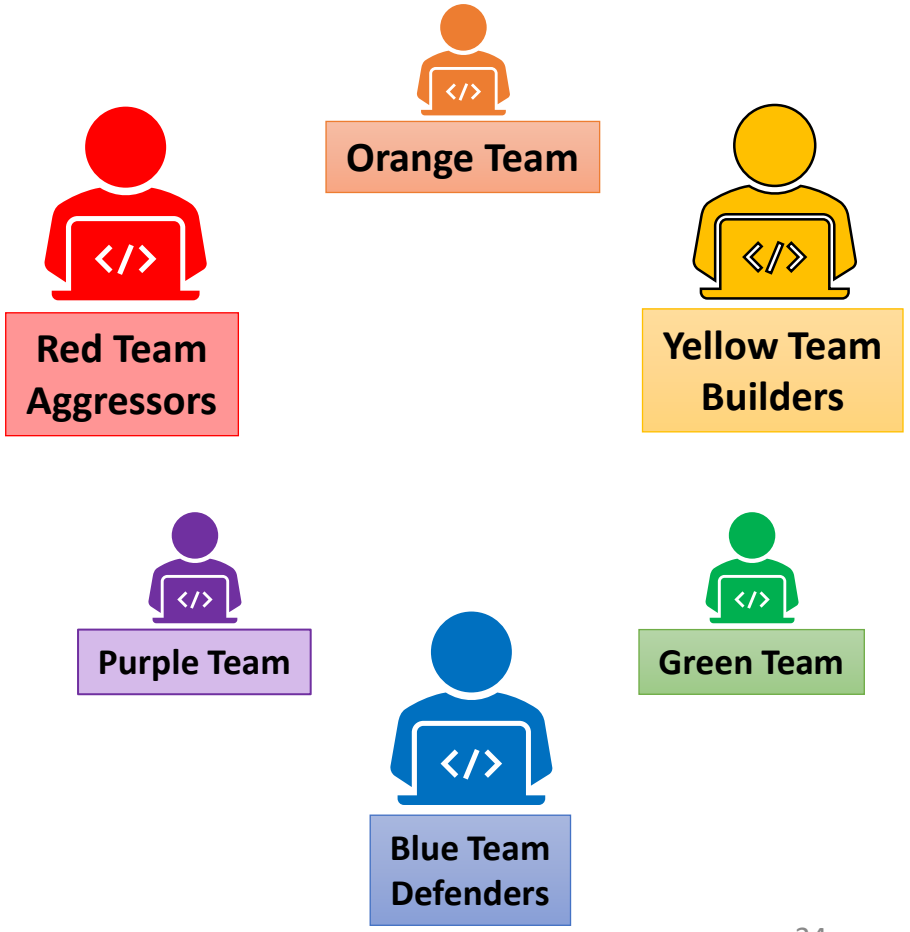
Phase 5: Cooperative Vulnerability and Penetration Assessment



Phase 6: Adversarial Assessment

- Characterize the operational mission effects to critical missions caused by threat-representative cyber activity against a unit trained and equipped with a system, as well as the effectiveness of defensive capabilities.





DOD Cybersecurity Test and Evaluation Guidebook, February 10, 2020, Version 2.0, Chg 1, pg 9

Phase 6: Adversarial Assessment

- **Tuckman:** Performing to Adjourning.
- **PMI Org:** Strong Matrix to Projectized.
- Gaining cybersecurity teams execute step 7, Monitor, of the Risk Management Framework (RMF) – as of 2018.
- System enters its sustainment and vulnerability management phases.

Assimilate Through DevSecOps

- Cross functional or multi-disciplined teams.
- Co-locate when possible; video conference when in hybrid mode.
- Employ Agile principles where practical for the environment and security level.

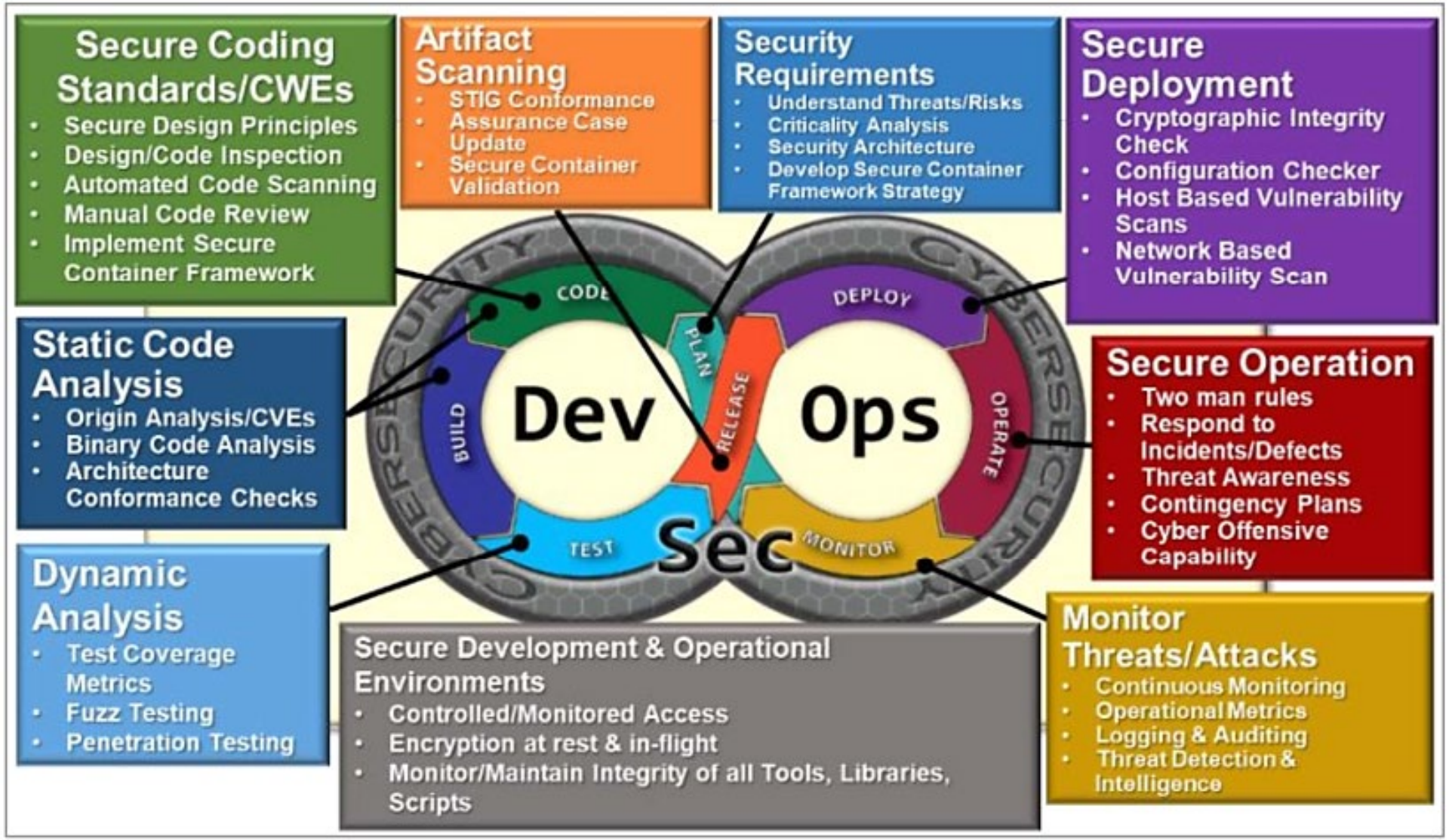


Figure C-4. The Sec in DevSecOps[32]

Assimilate Through Career Growth

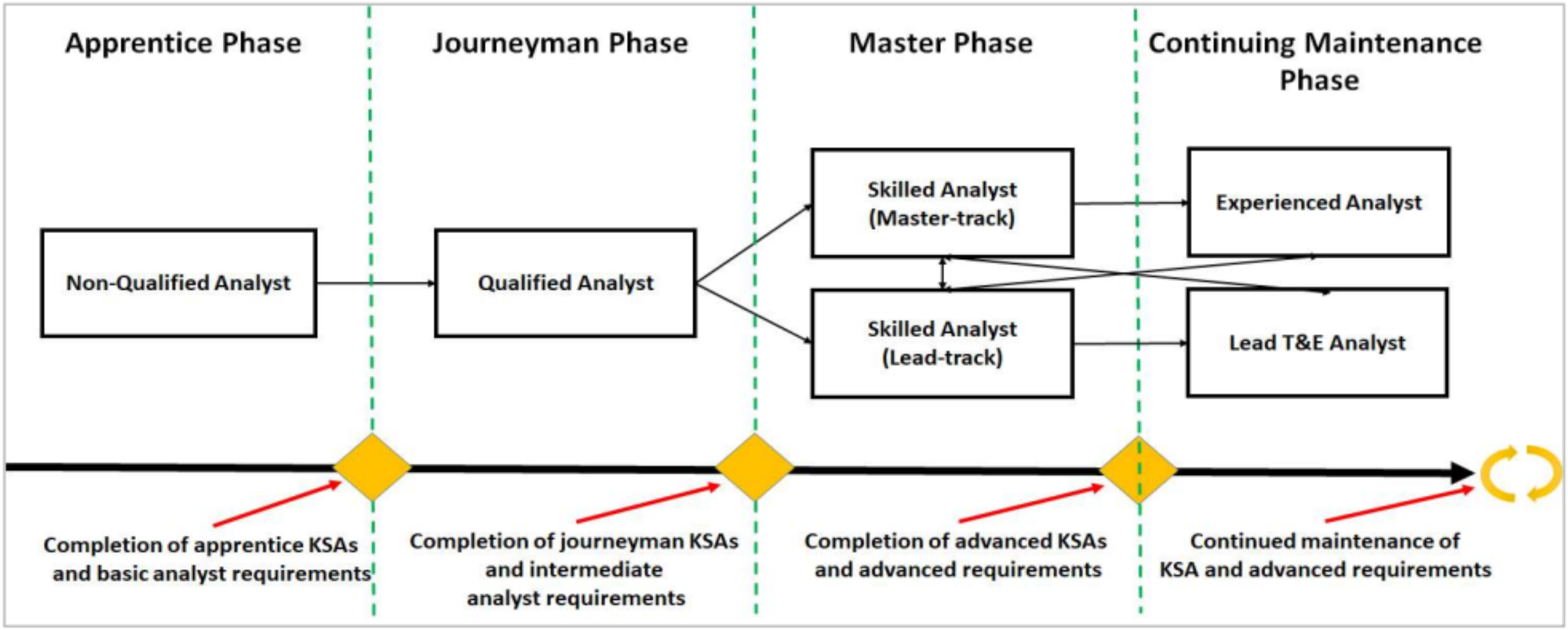


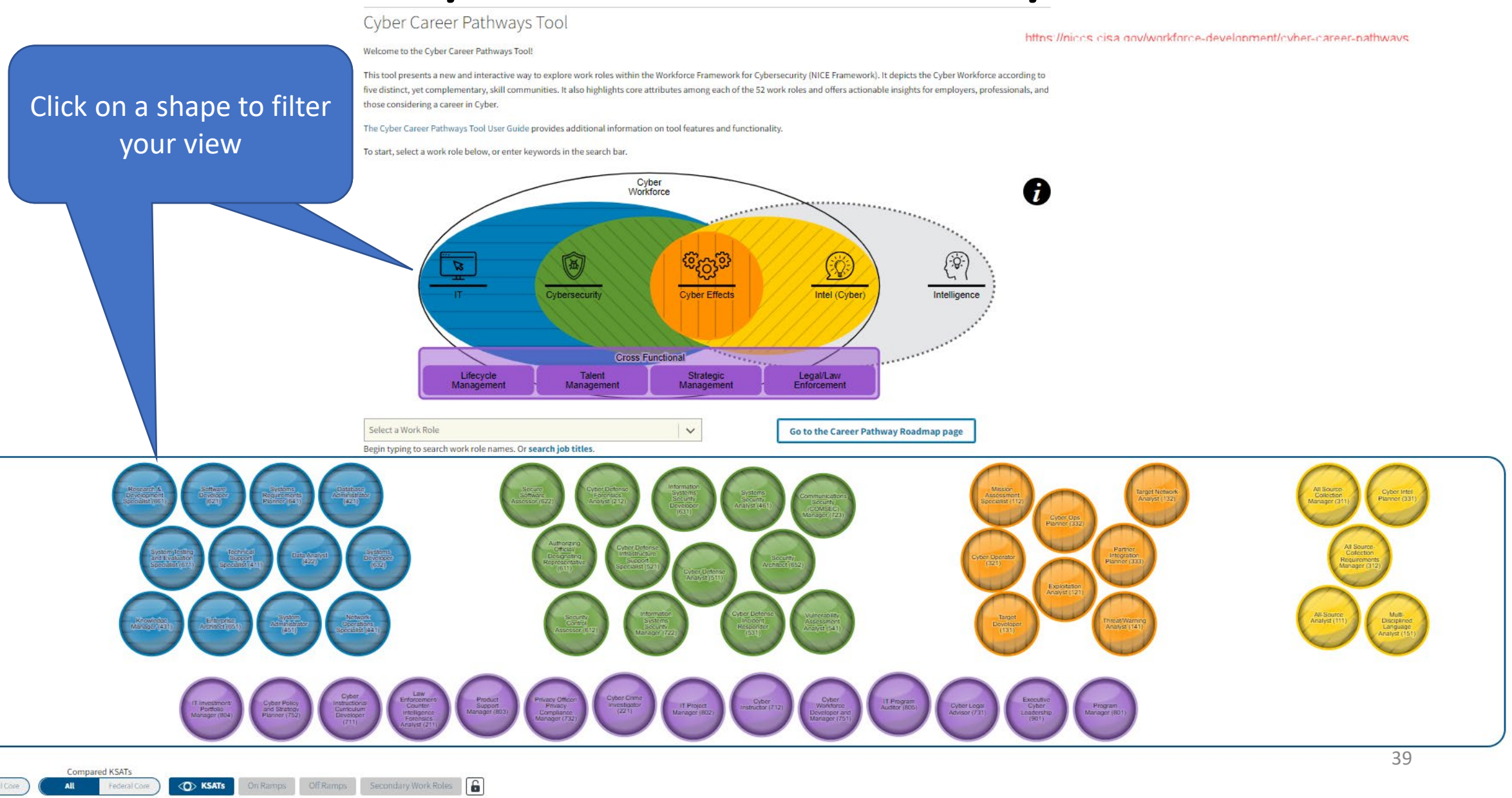
Figure F-1. Vulnerability Analyst Proficiency and Maturity Levels

In the People Game? Try the NICE Framework!

- National Initiative for Cybersecurity Education (NICE).
- **20** governmental departments and agencies, private sector, and academia developed the framework.
- NIST Special Publication 800-181 (Updated 2020).
- **The NICE Framework is comprised of the following components:**
  - Categories **(7)** – A high-level grouping of common cybersecurity functions.
  - Specialty Areas **(33)** – Distinct areas of cybersecurity work.
  - Work Roles **(52)** – The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role.

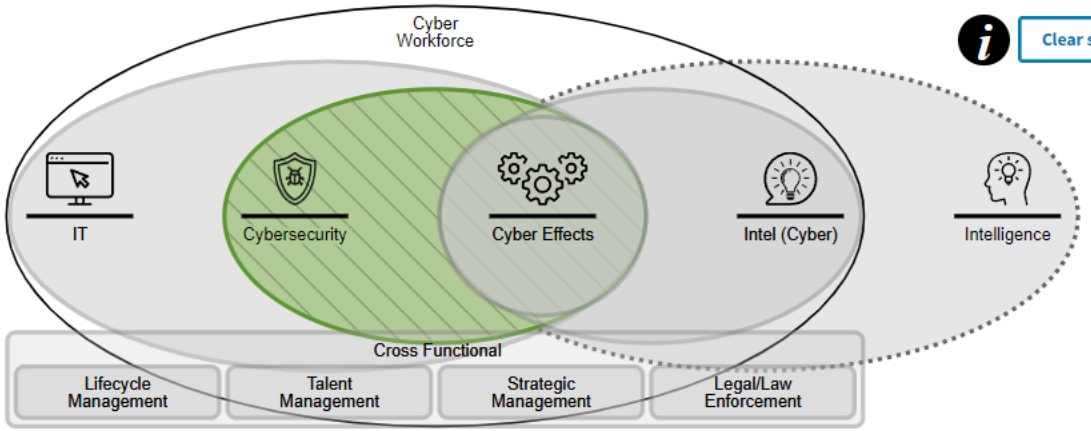
NICCS Cyber Career Pathways Tool

Click on a shape to filter your view



NICCS Cyber Career Pathways Tool

Selecting a work role will bring up this view



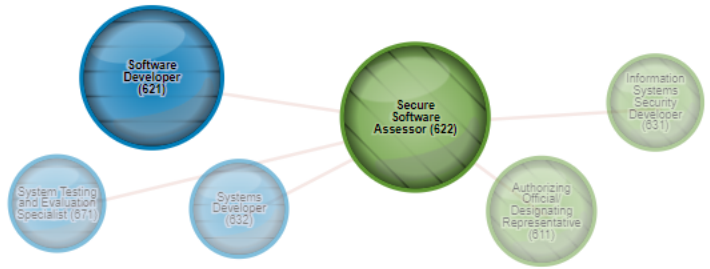
Clear selection

Secure Software Assessor

Begin typing to search work role names. Or **search job titles**.

Software Developer

Search job titles.



Details
All to All Overlap
All to All Tasks
All to All KSAs
Capability Indicators
Common Relationships
Federal Data

The below list defines the most common occupational series used in the Federal Government for this specific work role. This can be used as an indicator for users for things like position descriptions. Some work roles require multiple codes to illustrate the breadth and depth of a work role. The secondary work roles listed below can help users to identify potential work role pairing. This data was pulled from The Office of Personnel Management (OPM) Federal Government-wide data as reported in 2020.

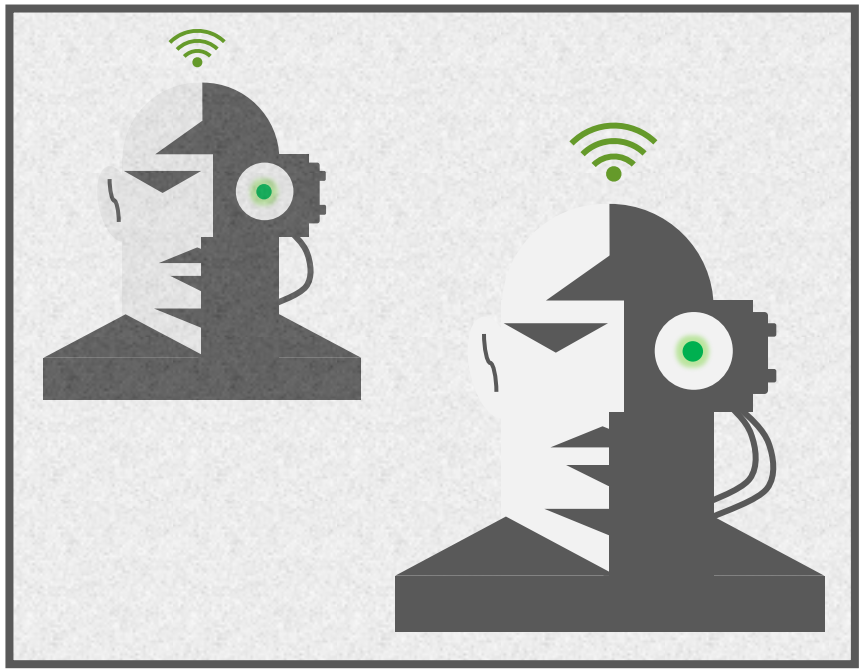
Top 5 Occupational Series | Top 5 Secondary Work Roles

Secure Software Assessor		Software Developer
63.61%	**2210-INFORMATION TECHNOLOGY MANAGEMENT**	60%
14.98%	**1550-COMPUTER SCIENCE**	25.71%
7.65%	**0854-COMPUTER ENGINEERING**	6.2%
3.67%	**0855-ELECTRONICS ENGINEERING**	2.91%
3.36%	**0801-GENERAL ENGINEERING**	✖
✖	**0850-ELECTRICAL ENGINEERING**	0.83%

Relationship filters:

Selected KSATs | Compared KSATs

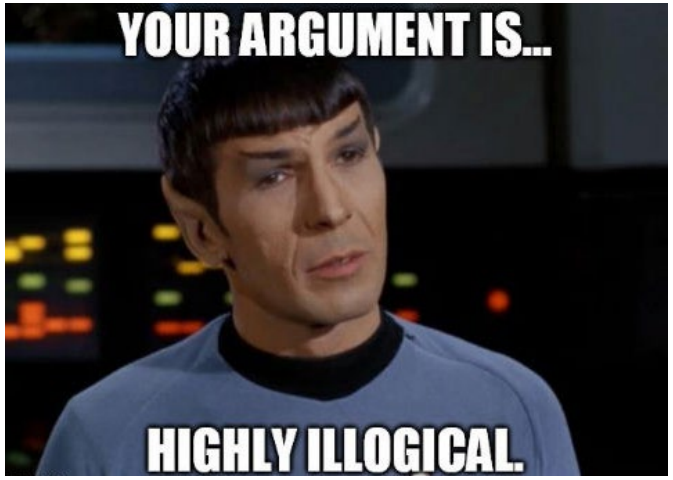
Re-cap



- **Terminology:**
  - Nine cyber terms to help you connect with your teams.
- **Vectoring Change in Cyber T&E**
  - What, where, and who is operating in this domain.
- **Assimilation**
  - DOD Cyber T&E model viewed through the lens of Tuckman's Group Development stages and PMBOK's Organizational Structures.
  - Cybersecurity color wheel (Red/Purple/Blue/Green/Yellow/White) + DevSecOps
  - CISA's career path tool – Highlighted the variety of Cyber professional disciplines that enable Cyber T&E capabilities for your organization.

Closing Thoughts: Remember, It's about Leadership

From Geekboss.com:



- **Speak to people in their own language**
  - Empathize with others and understand their culture
- **Join the away team**
  - A good captain doesn't just command from the bridge
  - Treat staff like colleagues and not minions
  - Participate, help, guide, and empower your team and save some Red Shirts!
    - **73% of Captain Kirk's crew deaths were Red Shirts (David Axe, wired.com)**
- **Have a set of values, and stay true to them**
- **Encourage disagreement, ask for advice and embrace diversity**
- **Stay hydrated**
  - Picard's Earl Grey or Janeway's long black, staying hydrated helps you maintain your mood, energy, and concentration levels
  - Maintain morale! Take the time to build what the Swedish call "fika" by getting together, away from screens and data to socialize and provide mutual support.

REFRENCES FOR RED, BLUE, YELLOW, AND WHITE TEAMS

Material we had to cut from this presentation. Hope you find some of it useful

Figure 1 Summarizes and Shows the Key Leadership Lessons Gathered from Star Trek

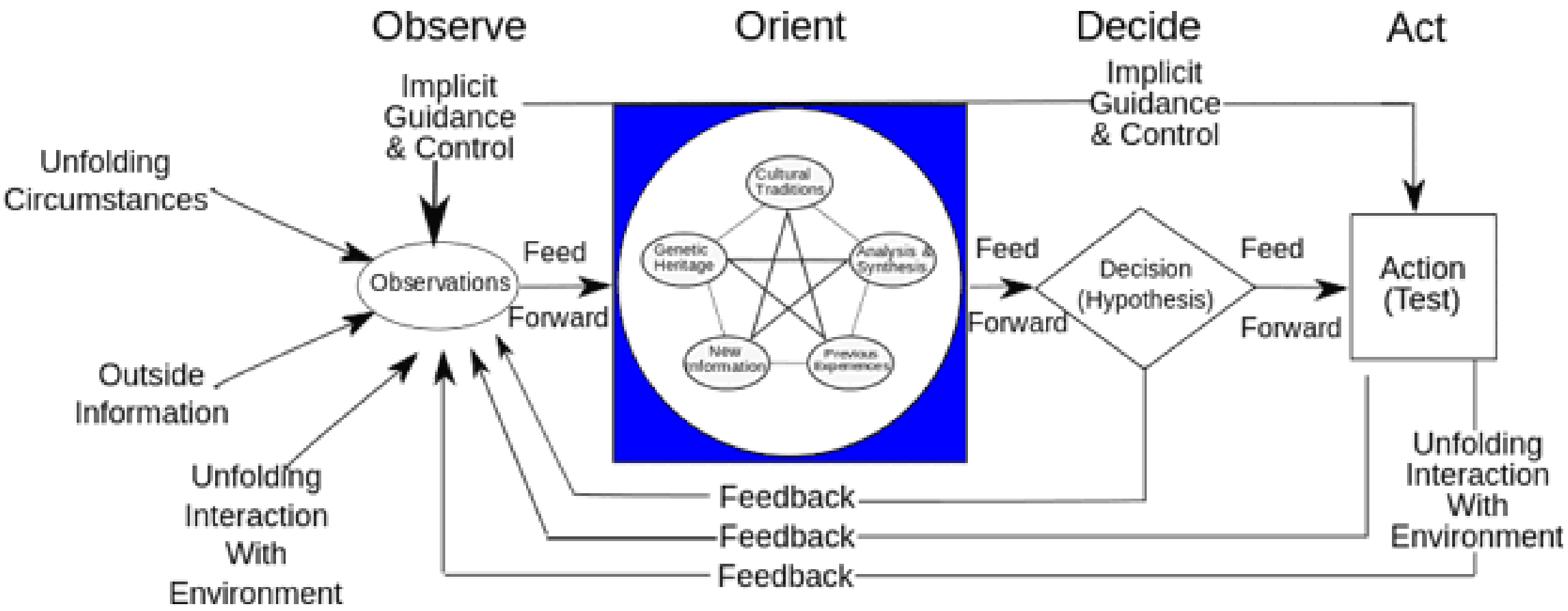
Red Team - Resources

- SANS – Offensive Operations Training
  - https://www.sans.org/offensive-operations/
- Carnegie Mellon Software Engineering Institute
  - https://www.sei.cmu.edu/publications/podcasts/
- The following slides:
  - JP 3-12 Definition of Red, Blue, and Gray cyberspace
  - OODA Loop by Col John Boyd
    - Useful when requiring an adaptive mindset
    - An Aggressor's or Defender's Mindset must change during operations
  - Cyber Kill Chain
    - A model to aid in sequencing a cyber attack
  - Links to ethical hacking tools and DAU Sys Eng
  - Ciso-central.org threat intelligence cycle

Cyber Operation's View of Cyberspace JP 3-12, I-4, I-5

- c. **Viewing Cyberspace Based on Location and Ownership.** Maneuver in cyberspace is complex and generally not observable. Therefore, staffs that plan, execute, and assess CO benefit from language that describes cyberspace based on location or ownership in a way that aids rapid understanding of planned operations. The term "blue cyberspace" denotes areas in cyberspace protected by the US, its mission partners, and other areas DOD may be ordered to protect. Although DOD has standing orders to protect only the Department of Defense information network (DODIN), cyberspace forces prepare, on order, and when requested by other authorities, to defend or secure other United States Government (USG) or other cyberspace, as well as cyberspace related to critical infrastructure and key resources (CI/KR) of the US and PNs. The term "red cyberspace" refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, "controlled" means more than simply "having a presence on," since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others. All cyberspace that does not meet the description of either "blue" or "red" is referred to as "gray" cyberspace.

OODA Loop



John Boyd's Observe Orient Decide Act loop: creator of the specific diagram above unknown

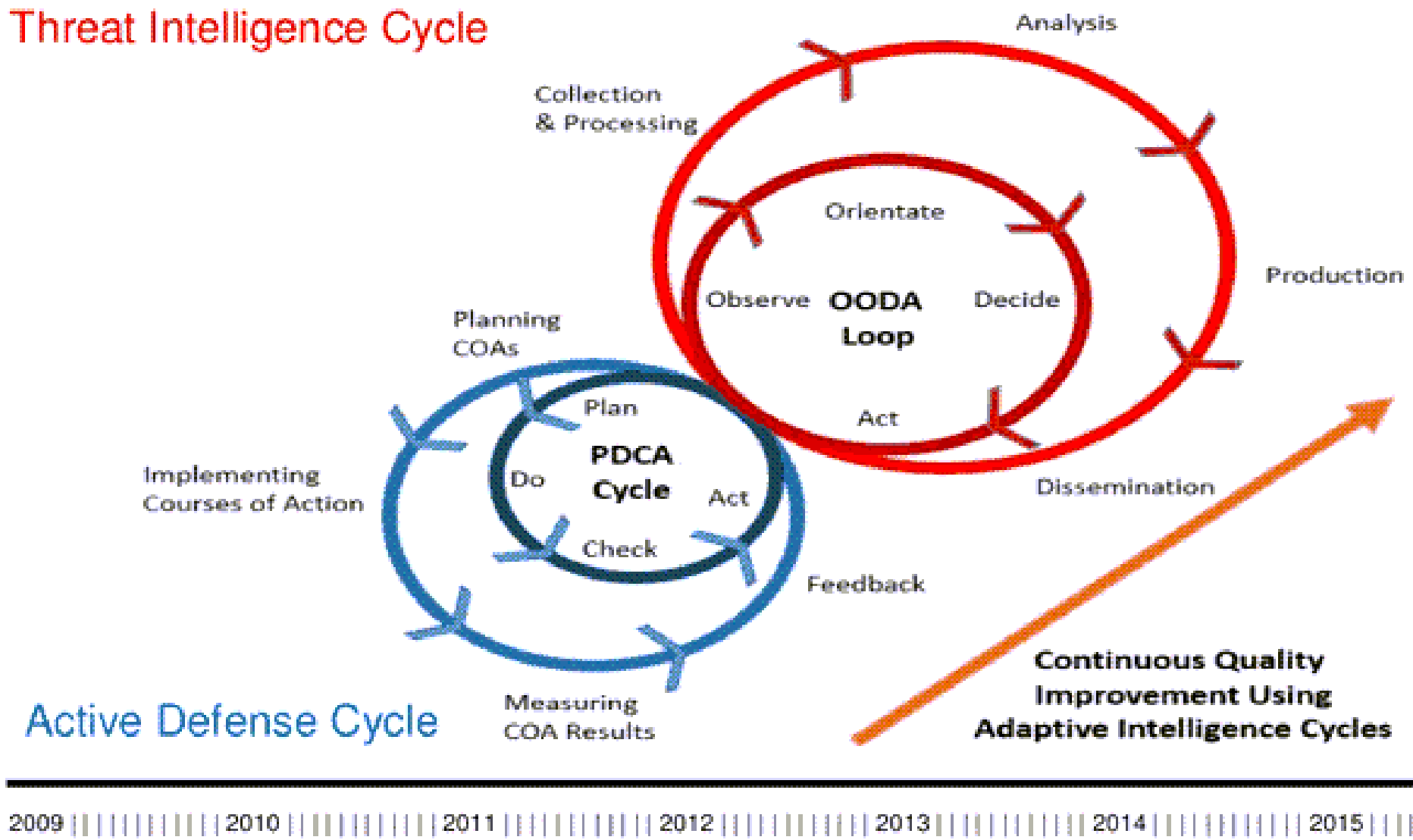
Figure 5-5. Cyber Kill Chain

DOD Cybersecurity Test and Evaluation Guidebook, February 10, 2020, Version 2.0, Chg 1, Chp 2, Pg 39

Tools of the Trade

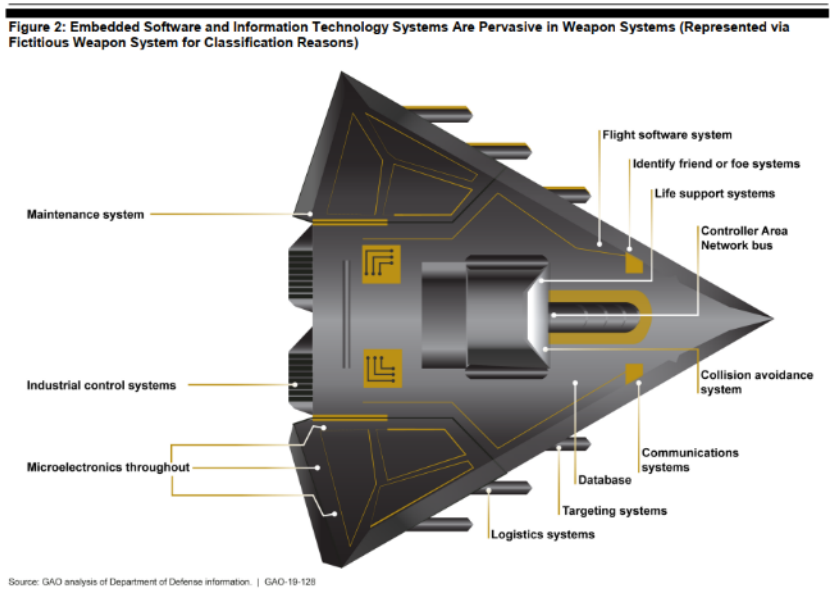
- https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/
  - One-stop-shop for US Law, NIST Standards, DoD Policies , and DoD Strategies for cybersecurity
- https://www.shodan.io/
  - Shodan is the world's first search engine for Internet-connected devices.
- https://www.kali.org/
  - Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.
- DAU – Systems Engineering Brainbook
  - https://www.dau.edu/tools/se-brainbook
  - Cybersecurity and Risk Mgt Framework:
    - https://www.dau.edu/tools/se-brainbook/Pages/Management%20Processes/Cybersecurity-Risk-Management-Framework.aspx#:~:text=The%20official%20definition%20of%20cybersecurity,to%20ensure%20its%20availability%2C%20integrity%2C

https://www.ciso-central.org/organisation/cyber-hygiene-attack-analysis



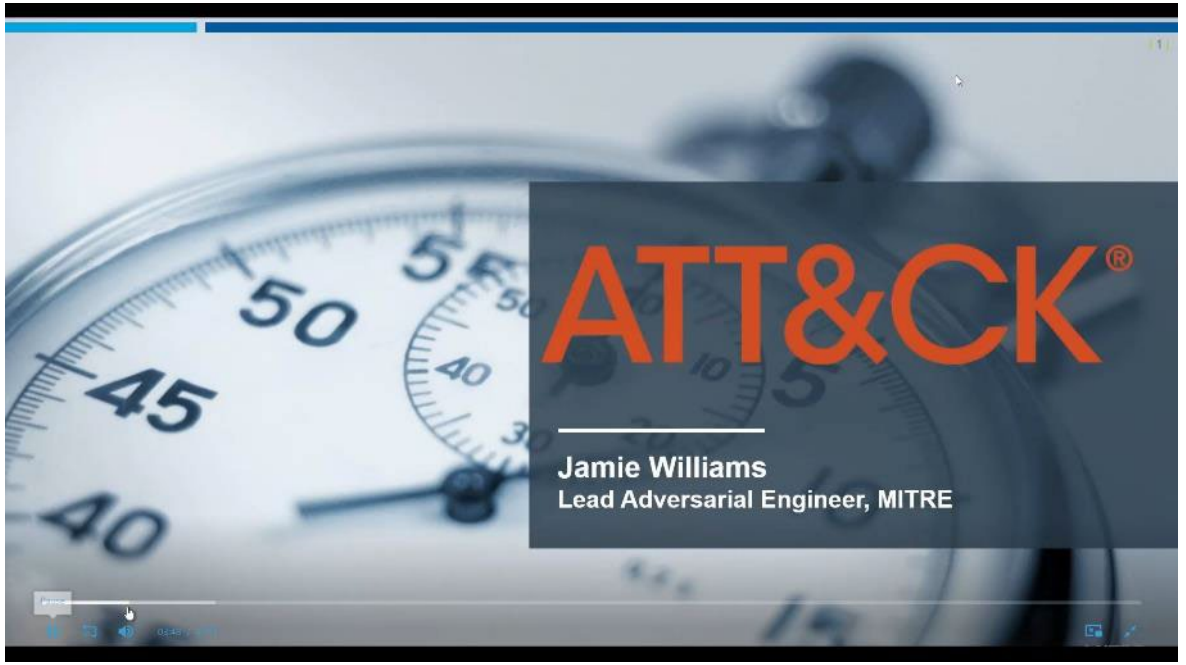
Blue Team - References

- DoDIN compliance chart
  - https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/
- GAO Report
  - "WEAPON SYSTEMS CYBERSECURITY, DOD Just Beginning to Grapple with Scale of Vulnerabilities"
  - https://www.gao.gov/assets/gao-19-128.pdf
- **The Following Slides**
  - ITEA Plug - MITRE ATT&CK Overview lunch and learn video
  - DAU SE Brainbook Testing process example
  - Cyber T&E Threat Vignette



MITRE ATT&CK

- ITEA Lunch and Learn Video is a Great ~1 hr lesson on the fundamentals of ATT&CK
  - Free to ITEA members!
- Aids Blue and Red teams in formulating defensive and offensive TTPs



DAU SE Brainbook: Red & Blue Team Testing Process

- Input to Controls Selection / Risk Assessment / Pre-Test
- User Reps / Focused Mission Areas

Event Preparation → ~ weeks → **Event Execution** → ~ 3 days → **Post Mission Analysis** → ~ weeks → **Reporting**

- Analyze Architecture, CONOPS, Intelligence
- Define Mission
- Identify Control, Blue, Red, Analysis, and Reporting Teams

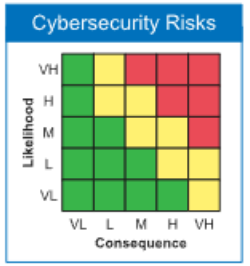
- Define Attack Paths and Vulnerabilities
- Analyze adversary attacks

- Determine Cyber effects: F/P/NMC
- Risk: Likelihood, Consequence

- Risk Matrix
- Mitigations
- Executive, Detailed and Full Report

Operational (Blue) Team: Develop Mission Plan → Describe Effects → Develop Mitigations

Adversarial (Red) Team: Define Access Paths → Execute Attacks



Example of a Threat Vignette

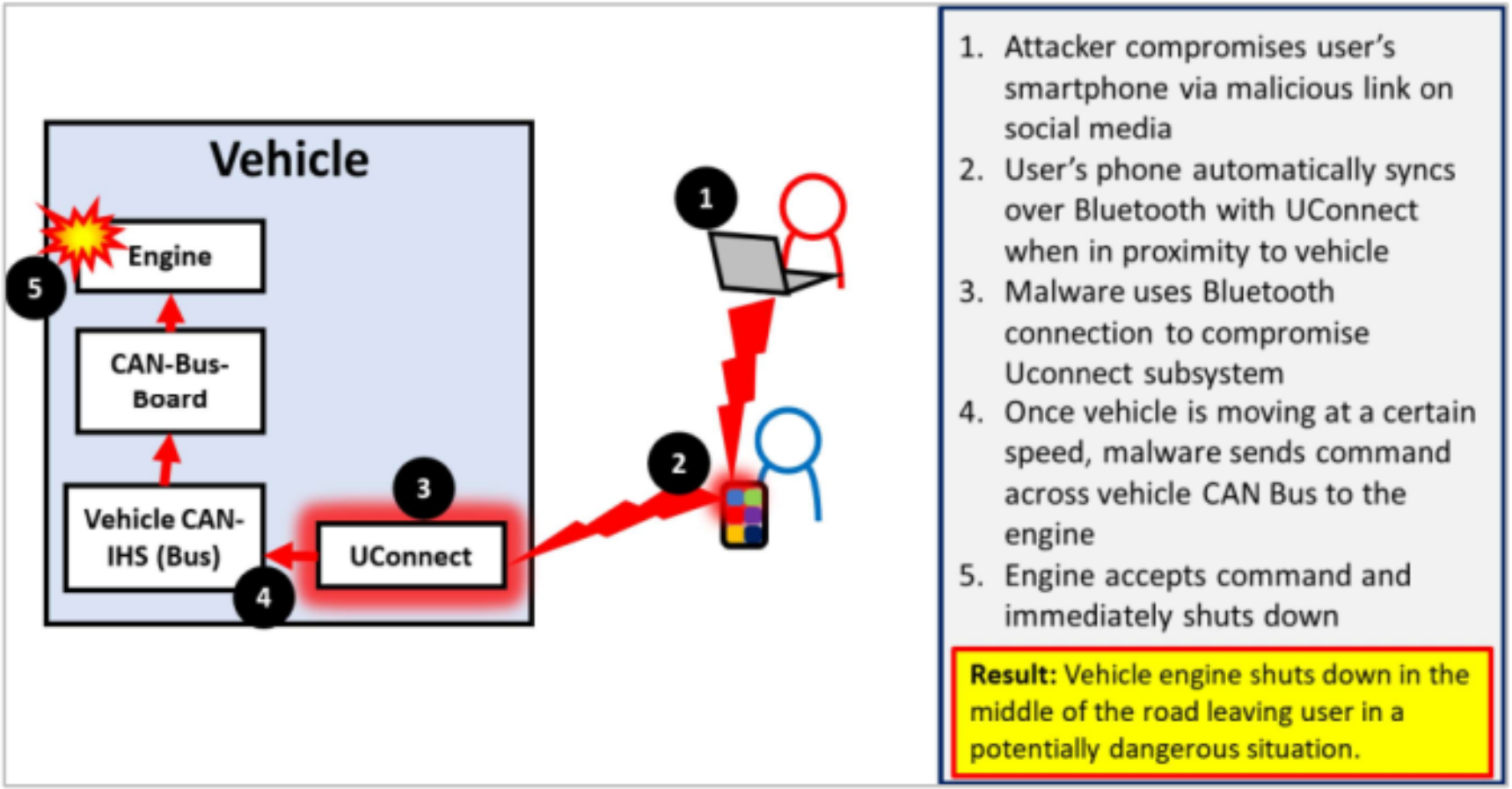


Figure 5-7. Threat Vignette Illustration

Yellow Team - References

- **The following slides**
  - Cyber T&E software testing and types of analysis
  - Sample Cyber T&E process for testing a business system
  - Cloud-based computing/platforms
  - Agile Principles at Work – DoD Focus on Speed and Seamlessness
    - Software Factory / Software Practice
  - Software development challenges from DAU
    - Screen shots from Chad Reynolds- 24 Sep 2020
    - https://media.dau.edu/media/t/1_5pqhiza4

Software Testing & Types of Analysis

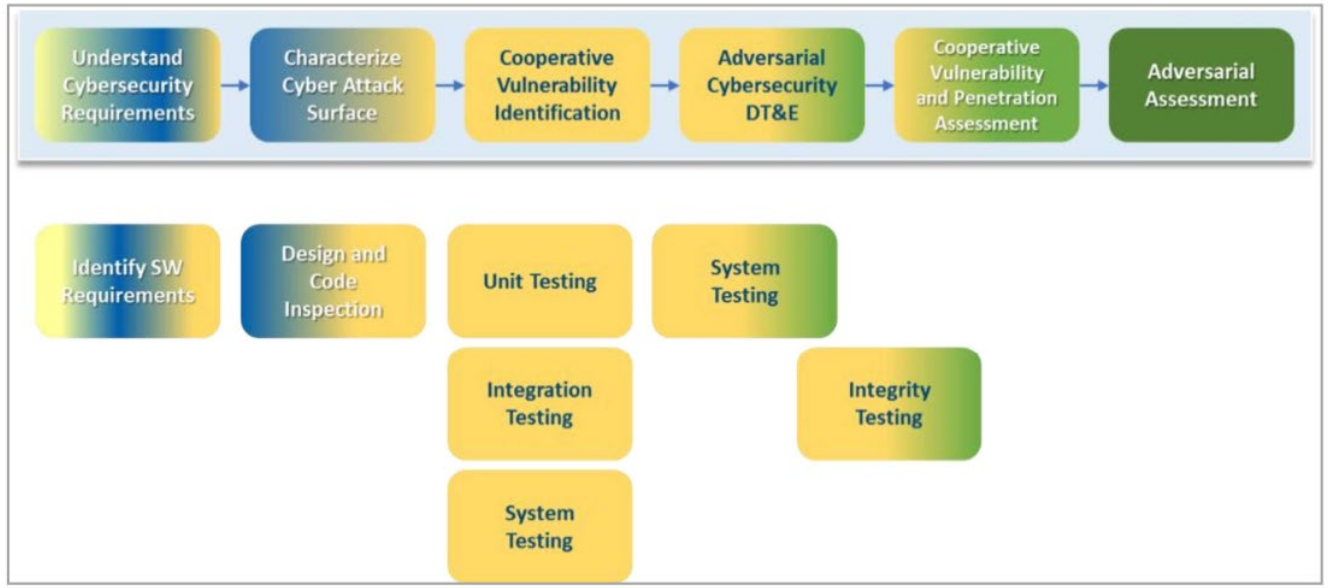


Figure G-5. Software Testing Schedule

When to Test

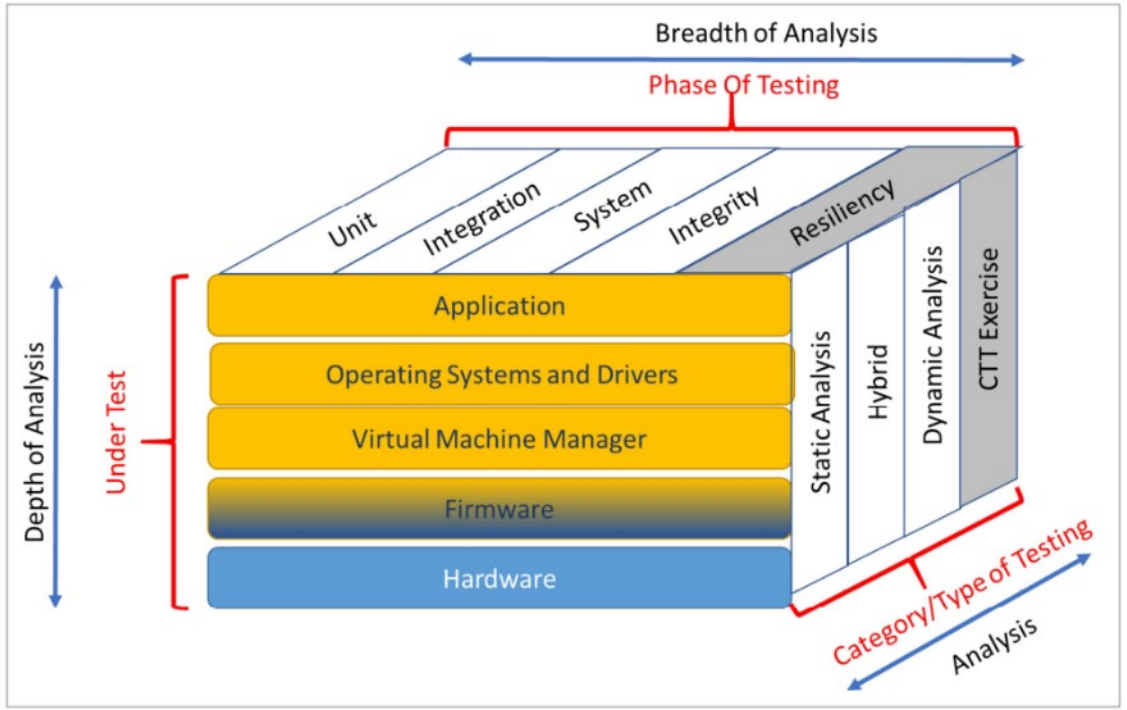


Figure G-6. Testing Rigor

How rigorous to test IAW Mil Std 882 E

Cyber T&E for a Business System

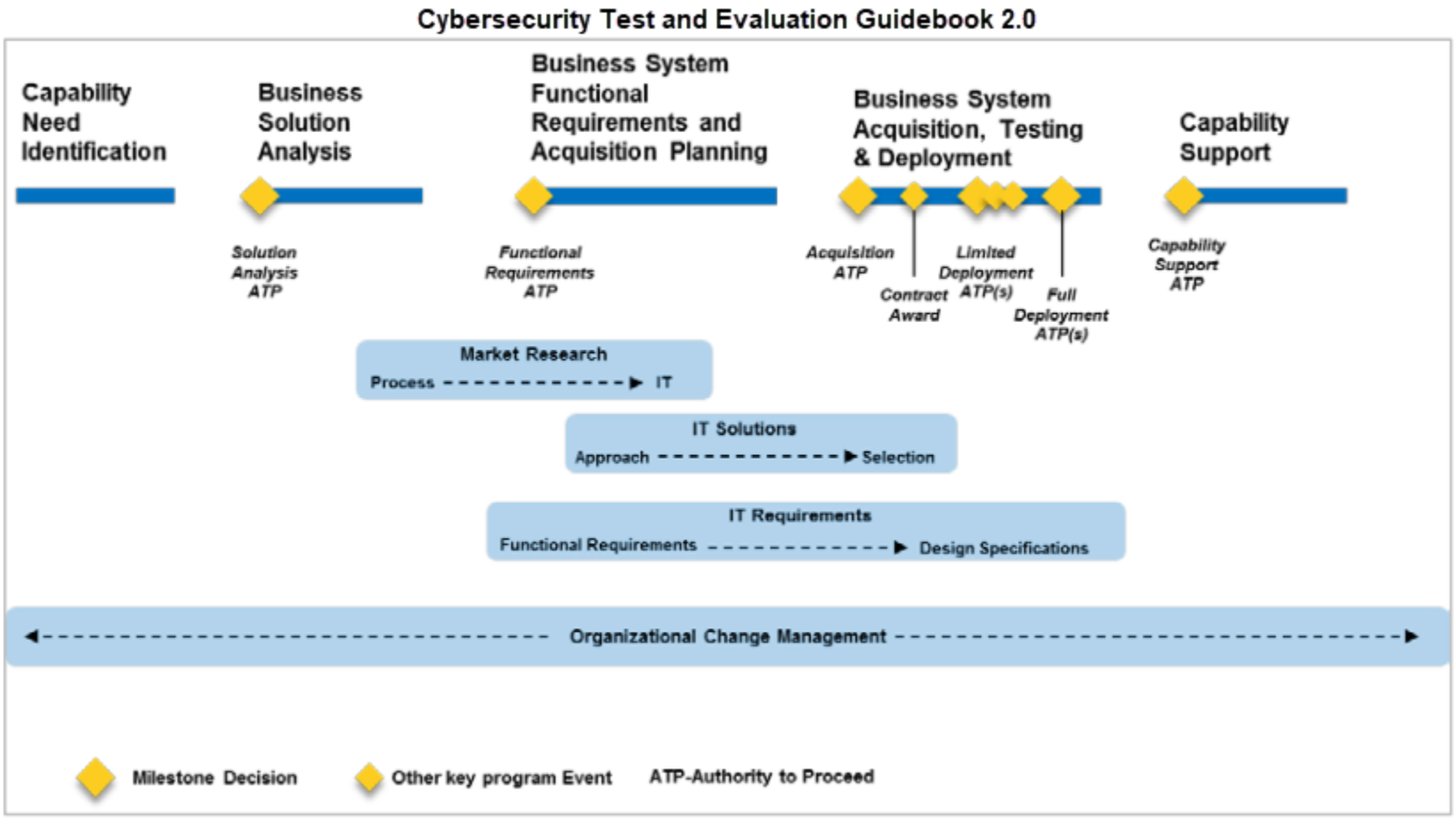


Figure 2-1. Business Capability Acquisition Cycle

Page 4

Secure Cloud Computing

- USAF
- https://software.af.mil/dsop/services

Platform One

- USN
- https://www.blackpearl.us

Black Perl

- FedRamp
- https://www.fedramp.gov

Federal

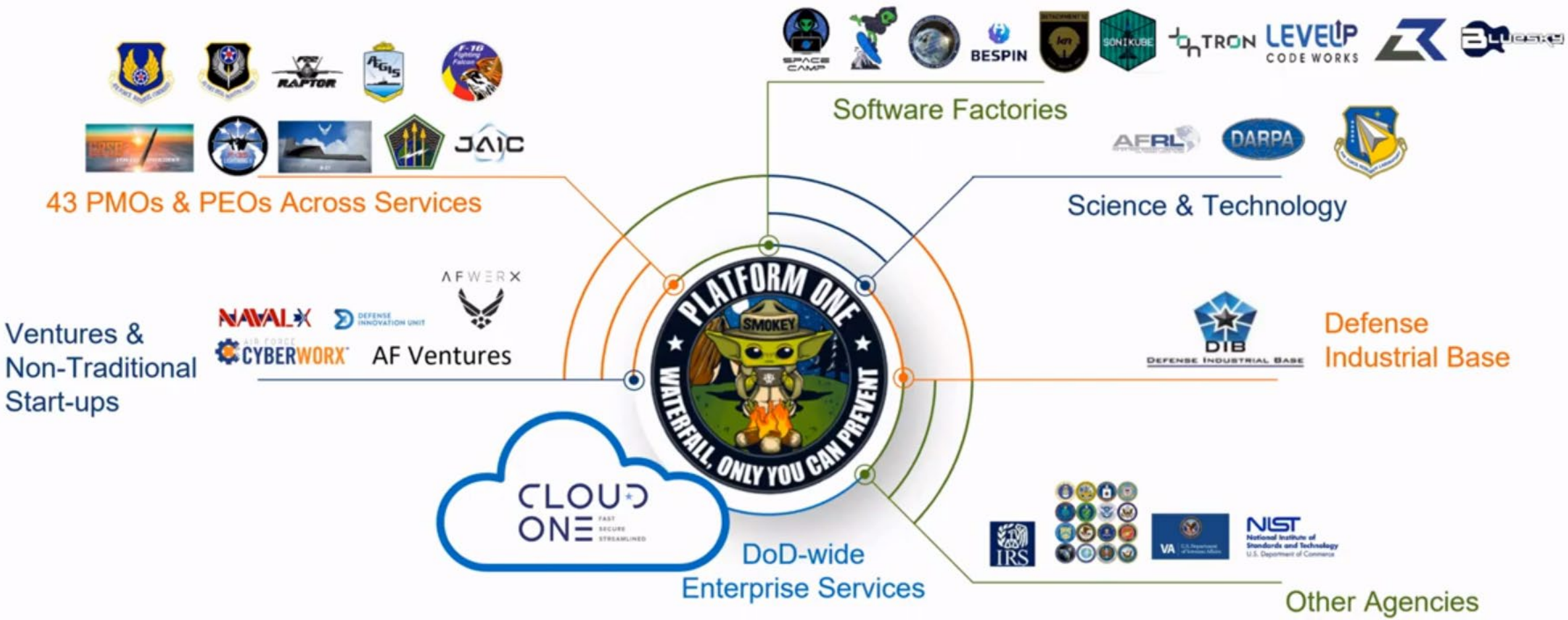
FedRAMP

- https://www.fedramp.gov
- Federal Risk and Authorization Management Program (FedRAMP)
- Focused on providing cloud-based infrastructure
- Common security controls against a common baseline
  - Federal Information Security Modernization Act (FIMSA) compliant
  - OMB Circular A-130
  - Supported by
- Required for all federal system
- Security package allows for re-use by an agency

USAF Platform One

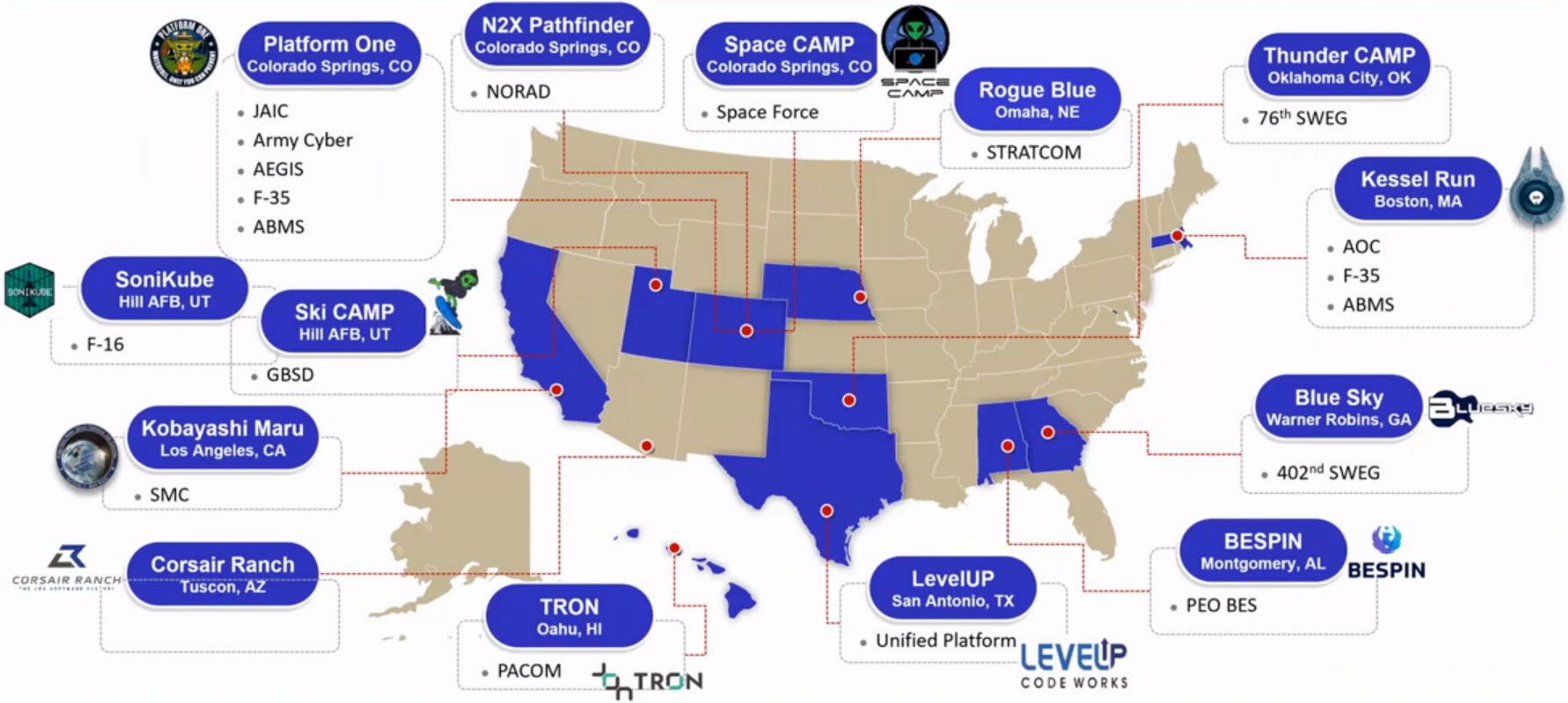
- 85% baseline capabilities
- DevSecOps platform
- Bottom up driven with technical people driving decisions
- **Culture:**
  - Co-location of teams, dropped uniforms, badges, and encourage risk taking through adoption of industry best practices
  - Supporting SpaceCamp
- Leadership awards within weeks
- On-board 100K DoD developers
- Leadership enables and resources

Software Ecosystem
Multiple Innovation Hubs – One Platform



Software Ecosystem

Multiple Innovation Hubs, One Platform



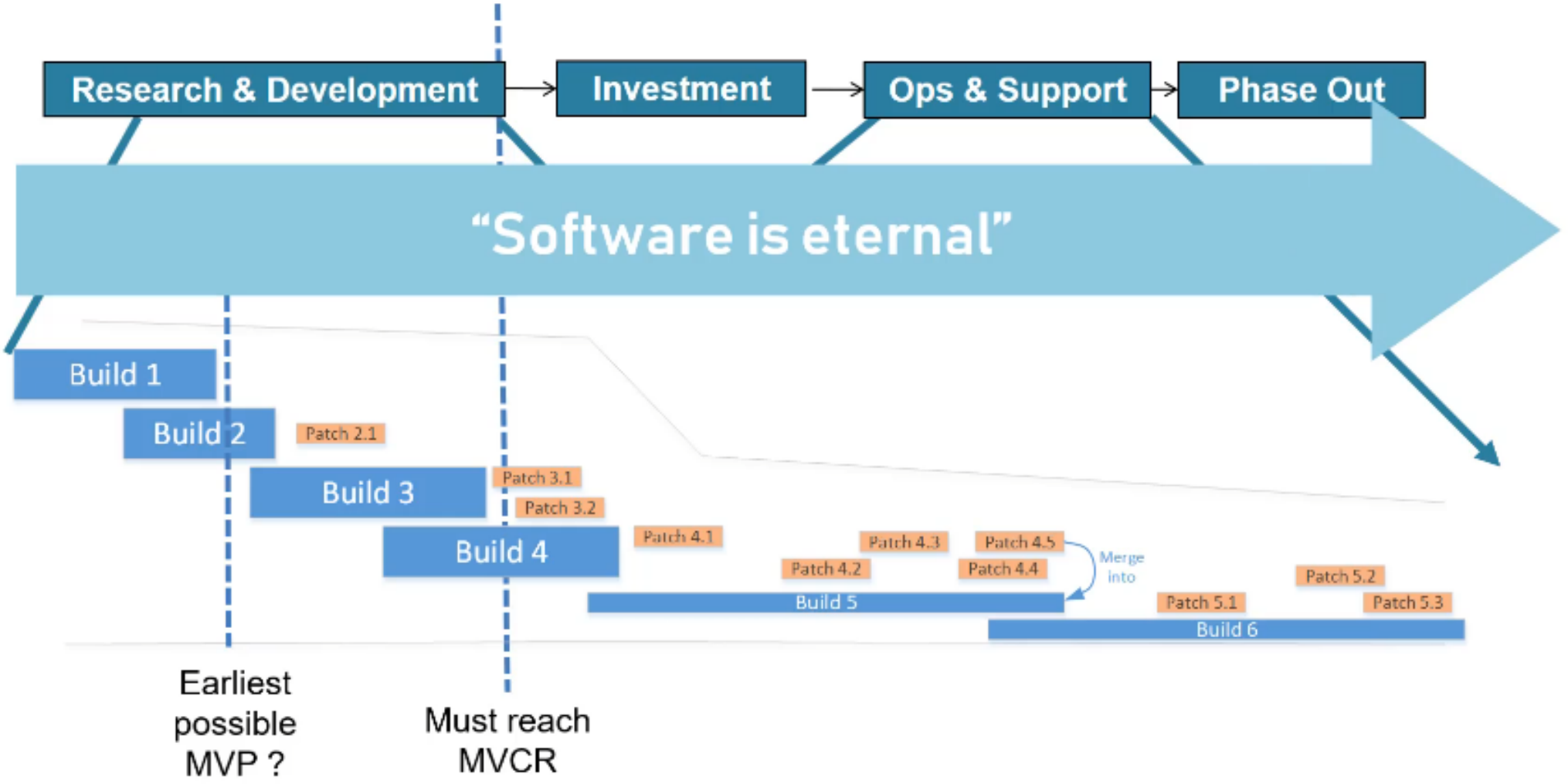
USN Black Perl

- https://www.blackpearl.us
- **Who We Are**
  - Black Pearl is a group of Military, Civilian, and Contractor personnel with experience solving software delivery issues across the Naval Enterprise. Our team understands the problems and needs of Naval programs seeking to accelerate delivery of capability to the warfighter.
- **What We Are**
  - **We are NOT a software factory, we are a software practice.** It means that we build your workforce by engaging your team from platform to development, from greenfield to refactor. We as seasoned DevSecOps practitioners and agilists are here to share our experiences, thoughts, and expertise with your team to move the Naval enterprise's technology forward towards a more lethal Navy

KESSELRUN Example of USAF Software Factories

- **KesselRun**
  - https://kesselrun.af.mil
  - “The Air Force set the precedent for software and DevSecOps methodologies and getting it into a user environment.”
    -- Hannah Hunt, Chief Product and Innovation Officer at Army Futures Command (Kate Marci, governmentciomedia.com, 15 Sep 2021)
- **Software.af.mil**
  - https://software.af.mil

Software Development vs. Hardware Development

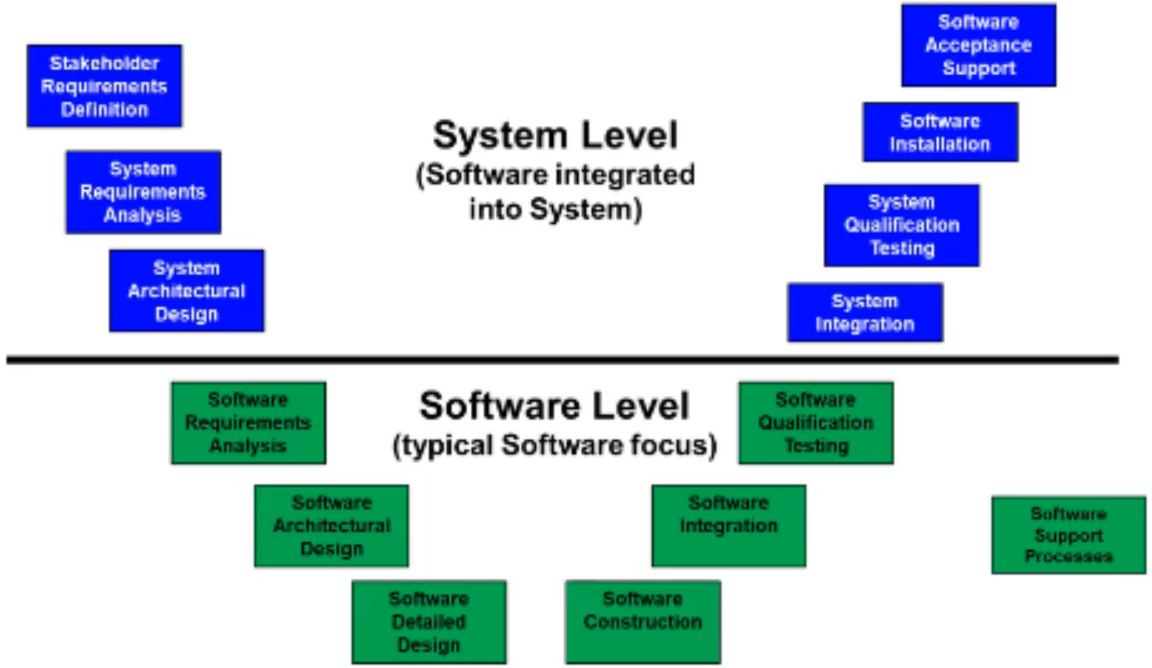


Software Development (Chad Reynolds- 24 Sep 2020): https://media.dau.edu/media/t/1_5pqhiza4

Software Always Exists in the Context of a System

System-Context Processes:
All of the interacting items/elements in a system that includes both software and hardware items

Software-Specific Processes:
Each software item in the system, to fulfill specific item-level requirements



The International Standard ISO/IEC 12207 on "software life-cycle processes" does not prescribe a particular software life-cycle model

Software Development (Chad Reynolds- 24 Sep 2020): https://media.dau.edu/media/t/1_5pqhiza4

Emphasis on the Process to Ensure Sustainability

SOFTWARE DEVELOPMENT EFFORT SUPPORT / MANAGEMENT ACTIVITIES

- Activities which span the entire development and are not steps
- These activities can be rolled up into overall software development effort or in separate lines

SW Document Management

Develop and maintain the recorded software information produced

SW Configuration Management

Establish and maintain the integrity of the software

SW Quality Assurance

Assure that the products and processes comply with the predefined plans and thresholds

SW Verification

Confirm that the software and process properly reflects the specified requirements

SW Validation

Confirm that the requirements for the a specific intended use of the software work product are fulfilled

SW Review

Maintain common understanding with the stakeholders of progress against the objectives of the agreement

SW Audit

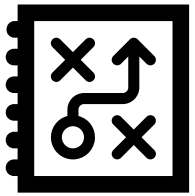
Independently determine compliance of selected products and processes with the requirements, plans, and agreement

SW Problem Resolution

Ensure that all discovered problems are identified, analyzed, managed and controlled to resolution

Methods to build hardware are usually of less importance during V&V because if it meets the needs it usually doesn't matter how it was built.

Software is more difficult to



White Team – References

- DoD CIO
  - https://dodcio.defense.gov/library/
- DAU T&E Community of Practice: https://www.dau.edu/cop/test/lists/test%20and%20evaluation%20policy%20links/allitems.aspx
- **The following Slides**
  - DODIN Cybersecurity and Policy Chart
    - https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/
  - Software acquisition pathway
    - Adaptive Acquisition Framework (Emmet Simmons)
    - https://media.dau.edu/media/t/1_4vfnv4qv
    - https://aaf.dau.edu/aaf/software/
  - Developing People Resources
  - Suggested work roles mapped to Red, Blue, and Yellow teams from the Cybersecurity wheel and NICE framework
  - NICE Disciplines
  - CyWG RACI Chart
  - Cyber T&E phases inputs/tasks/outputs
  - A suggested method for plotting the assimilation of your multi-disciplined teams

Cyber Security & Information Systems Information Analysis Center

Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Issuances
Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: February 22, 2022
Send questions/suggestions to contact@csiac.org

ORGANIZE

Lead and Govern

- Interim National Security Strategic Guidance
- United States Intelligence Community Information Sharing Strategy
- 2019 National Intelligence Strategy
- U.S. Int'l Strategy for Cyberspace
- National Cyber Strategy
- National Strategy to Secure 5G
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- National Strategy to Secure Cyberspace
- National Defense Strategy (NDS)
- DoD Software Modernization Strategy
- 2018 DoD Cyber Strategy
- DoD Digital Modernization Strategy
- *DoD Cybersecurity Risk Reduction Strategy*
- Summary of the 2018 DoD Artificial Intelligence Strategy
- DoD Cloud Strategy
- DoD Data Strategy
- DoD Identity, Credential, and Access Management (ICAM) Strategy
- DoD 5G Strategy
- National Military Strategy (NMS)
- DoD Information Sharing Strategy

ORGANIZE

Design for the Fight

- NIST SP 800-119 Guidelines for the Secure Deployment of IPv6
- CNSSP-11 Nat'l Policy Governing the Acquisition of IA and IA-Enabled IT
- CNSS National Secret Fabric Architecture Recommendations
- DFARS Subpart 208.74, Enterprise Software Agreements
- DoDD O-5100.19 (CAC req'd) Critical Information Communications (CRITCOM) System
- DoDD 5200.47E Anti-Tamper (AT)
- DoDD 7045.20 Capability Portfolio Management
- DoDD 8115.01 IT Portfolio Management
- DoDI 5000.02 Operation of the Adaptive Acquisition Framework
- DoDI 5000.87 Operation of the Software Acquisition Pathway
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN
- DoDI 7000.14 Financial Management Policy and Procedures (PPBE)
- DoDI 8115.02 IT Portfolio Management Implementation
- DoDI 8310.01 Information Technology Standards in the DoD
- DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)
- DoDI 8510.01 Risk Management Framework for DoD IT
- DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
- *RMF Knowledge Service*
- MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
- DODAF (Version 2.02) DoD Architecture Framework
- DTM 20-004 Enabling Cyberspace Accountability of DoD Components and Information Systems
- Common Criteria Evaluation and Validation Scheme (CCEVS)
- CJCSI 5123.01H Charter of the JROC and Implementation of the JCID
- Joint Publication 6-0 Joint Communications System

Develop the Workforce

- NIST SP 800-181 R1 Workforce Framework for Cybersecurity
- CNSSD-500 Information Assurance (IA) Education, Training, and Awareness
- NSTISSD-501 National Training Program for INFOSEC Professionals
- CNSSD-504 Protecting National Security Systems from Insider Threat
- CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment
- NSTISSI-4011 National Training Standard for INFOSEC Professionals
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- CNSSI-4013 National IA Training Standard For System Administrators (SA)
- CNSSI-4014 National IA Training Standard For Information Systems Security Officers
- NSTISSI-4015 National Training Standard for System Certifiers
- CNSSI-4016 National IA Training Standard For Risk Analysts
- DoDD 8140.01 Cyberspace Workforce Management
- DoDM 3305.09 Cryptologic Accreditation and Certification
- DoD 8570.01-M Information Assurance Workforce Improvement Program

Partner for Strength

- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP 800-171, R2 Protecting CUI in Nonfederal Systems and Organizations
- NIST SP 800-172 Enhanced Security Requirements for Protecting CUI
- CNSSP-14 National Policy Governing the Release of IA Products/Services…
- CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
- DoDI 5205.13 Defense Industrial Base (DIB) Cyber Security (CS) / IA Activities
- *DoDM O-5205.13 DIB CS/IA Program Security Classification Manual*
- DoD 5220.22-M, Ch. 2 National Industrial Security Program Operating Manual (NISPOM)
- Cybersecurity Maturity Model Certification (CMMC)
- MOA Between DoD and DHS (Jan. 19, 2017)

ENABLE

Secure Data in Transit

- FIPS 140-3 Security Requirements for Cryptographic Modules
- NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks
- CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
- CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS
- CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info
- CNSSP-19 National Policy Governing the Use of HAIPE Products
- CNSSP-25 National Policy for PKI in National Security Systems
- NSTISSP-101 National Policy on Securing Voice Communications
- *NACSI-2005 Communications Security (COMSEC) End Item Modification*
- CNSSI-5000 Voice Over Internet Protocol (VoIP) Computer Telephony (Annex I, VoSIP)
- CNSSI-5001 Type-Acceptance Program for VoIP Telephones
- NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's
- CNSSI-7003 Protected Distribution Systems (PDS)
- DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG
- DoDD 8521.01E Department of Defense Biometrics
- DoDI 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum
- DoDI 8100.04 DoD Unified Capabilities (UC)
- DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies
- DoDI 8523.01 Communications Security (COMSEC)
- DoDI S-5200.16 Objectives and Min Stds for COMSEC Measures used in NC2 Comms
- *CJCSI 6510.02E Cryptographic Modernization Plan*
- *CJCSI 6510.06C Communications Security Releases to Foreign Nations*

Manage Access

- HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors
- FIPS 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST SP 800-210 General Access Control Guidance for Cloud Systems
- NIST SP 1800-16 Securing Web Transactions: TLS Server Certificate Management
- CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
- CNSSP-10 Nat'l Policy Gov. Use of Approved Sec. Containers in Info Security Applications
- CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
- CNSSP-200 National Policy on Controlled Access Protection
- CNSSD-507 National Directive for ICAM Capabilities…
- CNSSD-506 National Directive to Implement PKI on Secret Networks
- CNSSI-1300 Instructions for NSS PKI X.509
- NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
- CNSSI-4001 Controlled Cryptographic Items
- CNSSI-4003 Reporting and Evaluating COMSEC Incidents
- CNSSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSS-008-14
- CNSSI-4006 Controlling Authorities for COMSEC Material
- DoDI 1000.25 DoD Personnel Identity Protection (PIP) Program
- DoDI 5200.01 DoD Information Security Program and Protection of SCI
- DoDI 5200.08 Security of DoD Installations and Resources and the DoD PSRB
- DoDI 5200.48 Controlled Unclassified Information(CUI)
- DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- DoDI 8520.03 Identity Authentication for Information Systems
- DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle
- DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual

Assure Information Sharing

- CNSSP-24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
- DoDI 8170.01 Online Information Management and Electronic Messaging
- DoDI 8320.02 Sharing Data, Info, and IT Services in the DoD
- DoDI 8582.01 Security of Non-DoD Info Sys Processing Unclassified Nonpublic DoD Information
- CJCSI 3213.01D, Joint Operations Security
- CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities

ANTICIPATE

Understand the Battlespace

- FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
- NIST SP 800-59 Guideline for Identifying an Information System as a NSS
- NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories
- NIST SP 800-92 Guide to Computer Security Log Management
- NISTIR 7693 Specification for Asset Identification 1.1
- CNSSD-520 Use of Mobile Devices to Process Nat'l Sec.Info Outside Secure Spaces
- CNSSP-28 Cybersecurity of Unmanned National Security Systems
- DoDI S-5240.23 Counterintelligence (CI) Activities in Cyberspace

Prevent and Delay Attackers and Prevent Attackers from Staying

- FIPS 200 Minimum Security Requirements for Federal Information Systems
- NIST SP 800-37 R2 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
- NIST SP 800-53 R5 Security & Privacy Controls for Federal Information Systems
- NIST SP 800-53A R5 Assessing Security & Privacy Controls in Fed. Info. Systems & Orgs.
- NIST SP 800-61, R2 Computer Security Incident Handling Guide
- NIST SP 800-124, R1 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems
- NIST SP 800-163, R1 Vetting the Security of Mobile Applications
- NIST SP 1800-26 Data Integrity: Detecting & Responding to Ransomware
- CNSSI-1011 Implementing Host-Based Security Capabilities on NSS
- CNSSI-1013 Network Intrusion Detection Sys & Intrusion Prevention Sys (IDS/IPS)
- CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
- CNSSI-1253F, Atchs 1-5 Security Overlays
- CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS
- DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers
- DoDI 5200.39 CPI Identification and Protection within RDT&E
- DoDI 5205.83 DoD Insider Threat and Management and Analysis Center
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
- DoDI 8531.01, DoD Vulnerability Management
- DoDI 8551.01 Ports, Protocols, and Services Management (PPSM)
- DoD O-8530.1-M (CAC req'd) CND Service Provider Certification and Accreditation Program
- DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
- DTM 17-007, Ch. 2, Defense Support to Cyber Incident Response
- CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)
- CJCSM 6510.01B Cyber Incident Handling Program
- *CJCSM 6510.02 IA Vulnerability Mgt Program*

ABOUT THIS CHART

- This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking* on the box directs users to the most authoritative publicly accessible source.
- *Policies in italics indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.*
- The linked sites are not controlled by the developers of this chart. We regularly check the integrity of the links, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
- CNSS policies link only to the CNSS site.
- Boxes with red borders reflect recent updates.
- *Note: It is best to open this PDF directly in a browser. However, if you are unable to open the links directly from this PDF document, place your cursor over the target box and right-click to copy the link location. Open a web browser and paste the copied link into the address bar.
- For the latest version of this chart or email alerts to updates go to https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

PREPARE

Develop and Maintain Trust

- CNSSP-12 National IA Policy for Space Systems Used to Support NSS
- CNSSP-21 National IA Policy on Enterprise Architectures for NSS
- NIST 800-160, vol.1, Systems Security Engineering: … Engineering of Trustworthy Secure Systems
- CNSSI-5002, Telephony Isolation Used for Unified Comms. Implementations w/ in Physically Protected Spaces
- DoDD 3020.40 Mission Assurance
- DoDD 3100.10 Space Policy

Strengthen Cyber Readiness

- NIST SP 800-207 Zero Trust Architecture
- NIST SP 800-18, R1 Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-30, R1 Guide for Conducting Risk Assessments
- NIST SP 800-39 Managing Information Security Risk
- NIST SP 800-126, R3 SCAP Ver. 1.3
- NIST SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware
- NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government
- CNSSD-505 Supply Chain Risk Management
- CNSSD-520 The Use of Mobile Devices to Process National Security Information Outside…
- DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
- *DoDD S-3710.01 National Leadership Command Capability*
- DoDI 8140.02 Identification, Tracking, And Reporting of Cyberspace Workforce Requirements
- DoDD 5101.21E Unified Platform and Joint Cyber Command and Control (JCC2)
- DoDI 8500.01 Cybersecurity
- DoDI 8560.01 COMSEC Monitoring
- Joint Special Access Program (SAP) Implementation Guide (JSIG)

Sustain Missions

- NIST SP 800-34, R1 Contingency Planning Guide for Federal Information Systems
- NIST SP 800-82, R2 Guide to Industrial Control Systems (ICS) Security
- *CNSSP-18 National Policy on Classified Information Spillage*
- CNSSP-22, IA Risk Management Policy for National Security Systems
- *CNSSP-300 National Policy on Control of Compromising Emanations*
- *CNSSI-1001 National Instruction on Classified Information Spillage*
- *CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Class. Material*
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- *CNSSI-7000 TEMPEST Countermeasures for Facilities*
- *NSTISSI-7001 NONSTOP Countermeasures*
- DoDD 3020.26 DoD Continuity Policy
- DoDD 3020.44 Defense Crisis Management
- DoDD 5144.02 DoD Chief Information Officer
- DoDD 8000.01 Management of the DOD Information Enterprise
- DoDI 5000.83 Technology & Program Protection to Maintain Technological Advantage
- DoDI 8410.02 NetOps for the Global Information Grid (GIG)
- ICD 503 IT Systems Security Risk Management and C&A
- UFC 4-010-06, Cybersecurity of Facility-Related Control Systems
- *NSA IA Directorate (IAD) Management Directive MD-110 Cryptographic Key Protection*
- Defense Acquisition Guidebook Program Protection

Color Key - OPRs

- ASD(NII)/(ASD(C3I)/DOD CIO
- CNSS/NSTISS
- DISA
- DHI
- JCS
- NIAP
- NIST
- NSA
- OSD
- CYBERCOM
- USD(A&S)
- USD(C)
- USD(I&S)
- USD(P)
- USD(P&R)
- Other Agencies
- Recently updated policy and/or link
- Expired, Update pending

AUTHORITIES

- Title 10, US Code Armed Forces (§§2224, 3013(b), 5013(b), 8013(b))
- Title 14, US Code Cooperation With Other Agencies (Ch. 7)
- Title 32, US Code National Guard (§102)
- Title 40, US Code Public Buildings, Property, and Works (Ch. 113: §§11302, 11315, 11331)
- Title 44, US Code Federal Information Security Mod. Act, (Chapter 35)
- Title 50, US Code War and National Defense (§§3002, 1801)
- Clinger-Cohen Act, Pub. L. 104-106
- UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

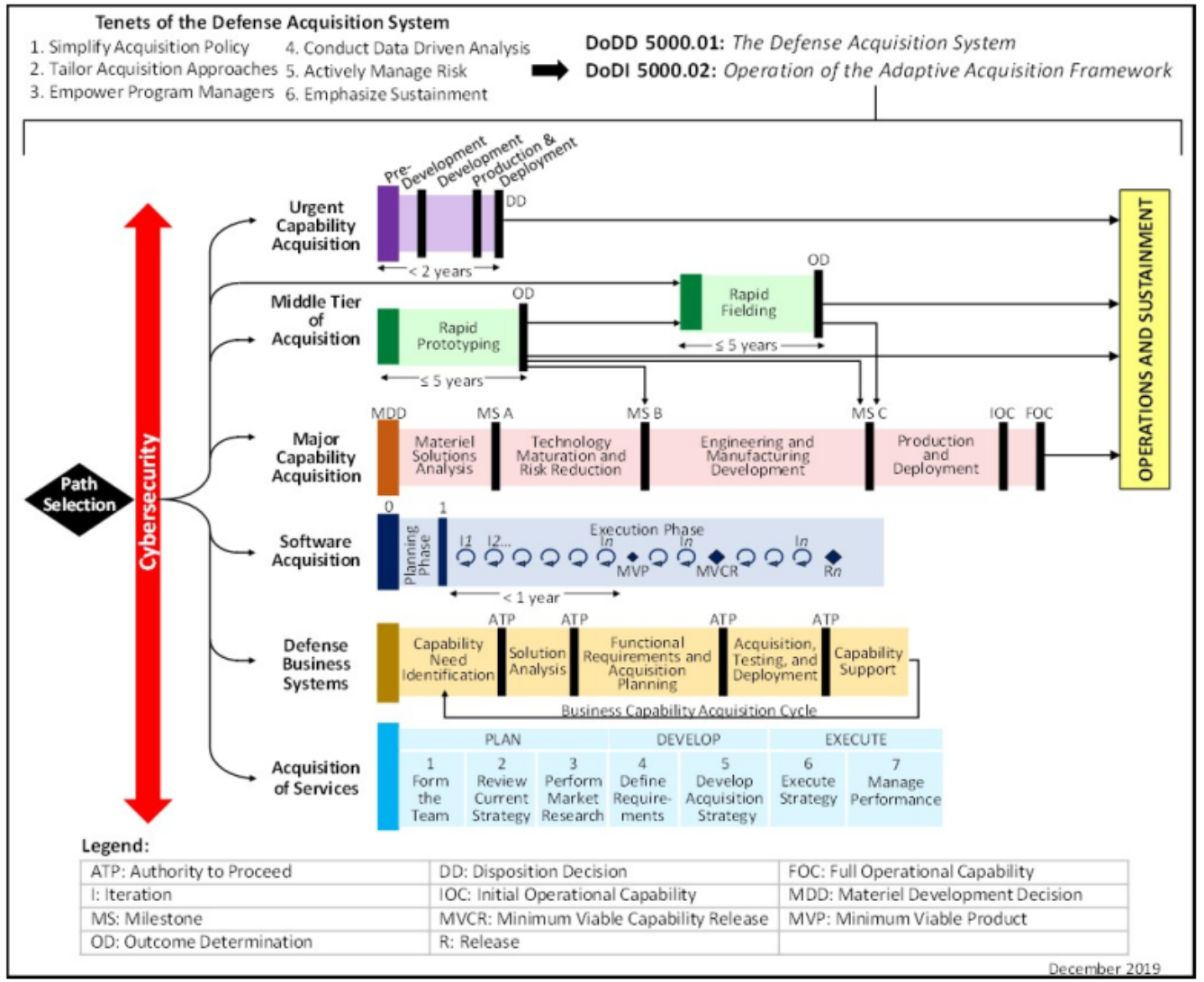
NATIONAL / FEDERAL

- Computer Fraud and Abuse Act Title 18 (§1030)
- Federal Wiretap Act Title 18 (§2510 et seq.)
- Stored Communications Act Title 18 (§2701 et seq.)
- Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
- Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
- Executive Order 13231 as Amended by EO 13286 - Critical Infrastructure Protection in the Info Age
- Executive Order 13526 Classified National Security Information
- Executive Order 13587 Structural Reforms To Improve Classified Nets
- Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing
- EO 13636: Improving Critical Infrastructure Cybersecurity
- EO 13800: Strengthening Cybersecurity of Fed Nets and CI
- NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
- EO 13873: Securing the Information and Communications Technology and Services Supply Chain
- EO 14028: Improving the Nation's Cybersecurity
- *NSPD 54 / HSPD 23 Computer Security and Monitoring*
- PPD 21: Critical Infrastructure Security and Resilience
- PPD 41: United States Cyber Incident Coordination
- PPD 28, Signals Intelligence Activities
- FAR Federal Acquisition Regulation
- A-130, Management of Fed Info Resources
- Ethics Regulations
- NIST Special Publication 800-Series
- NIST SP 800-63 series Digital Identity Guidelines
- NIST SP 800-88, R1,Guidelines for Media Sanitization
- NIST SP 800-101, R1 Guidelines on Mobile Device Forensics
- NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms
- NIST SP 800-137 Continuous Monitoring
- NIST SP 800-209 Security Guidelines for Storage Infrastructure
- NISTIR 7298, R3, Glossary of Key Information Security Terms
- CNSSD-502 National Directive On Security of National Security Systems
- CNSSD-900, Governing Procedures of the Committee on National Security Systems
- CNSSD-901 Nat'l Security Telecomm's and Info Sys Security (CNSS) Issuance System
- CNSSI-4009 Cmte on National Security Systems Glossary
- DoD Information Technology Environment Strategic Plan

OPERATIONAL/SUBORDINATE POLICY

- *CYBERCOM Orders*
- *JFHQ-DODIN Orders*
- Security Configuration Guides (SCGs)
- *Component-level Policy (Directives, Instructions, Publications, Memoranda)*
- NSA IA Guidance
- Security Technical Implementation Guides (STIGs)

Adaptive Acquisition Framework



DODI 5000.90, December 2020, pg 9, figure 1

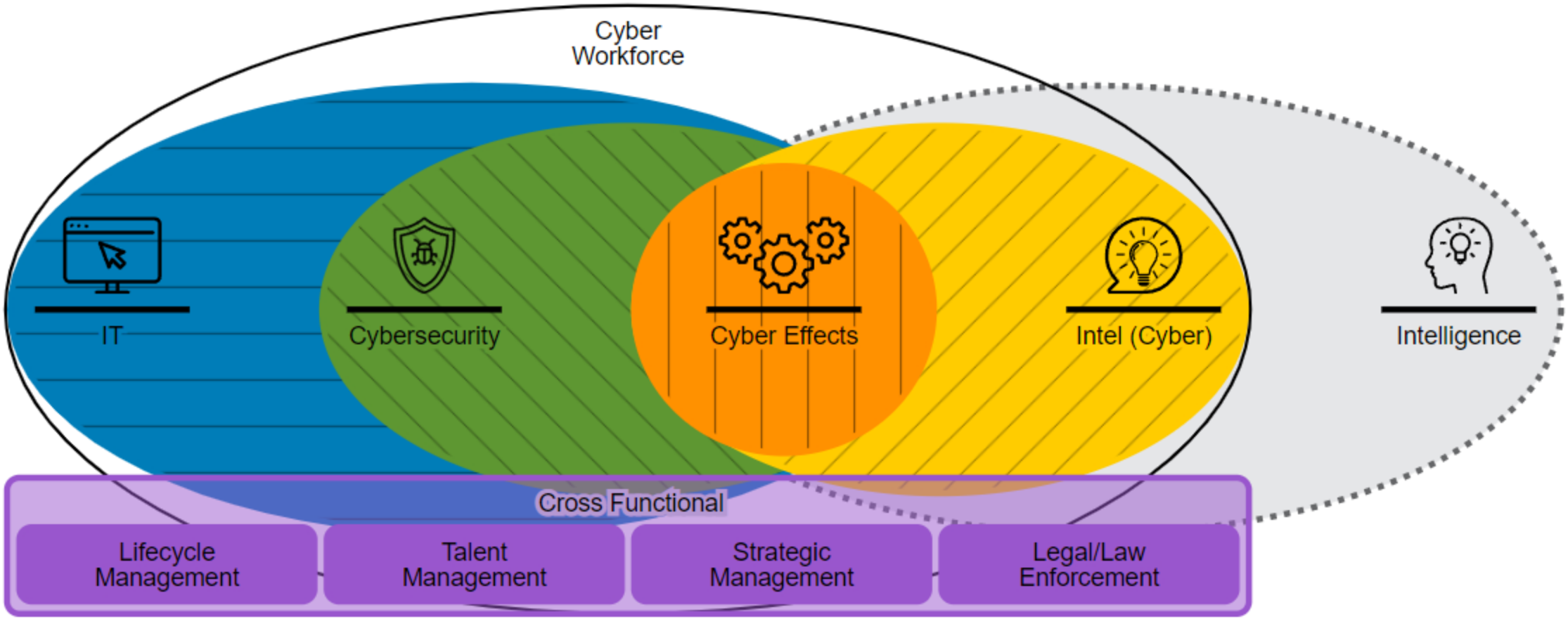
Developing People

- **National Initiative for Cybersecurity Education (NICE)**
  - https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/related-programs
  - Provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams.
- **NICE Tutorials:**
  - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-tutorials#NICE%20Cybersecurity%20Workforce%20Framework%20101
- **CISA Workforce Career Roadmap**
  - https://niccs.cisa.gov/workforce-development/career-pathway-roadmap
  - This digital tool offers an interactive way for working professionals (cyber and non-cyber), employers, students, and recent grads to explore and build their own career roadmap across the 52 different NICE Framework work roles.
- **CISA Training Course Search Tool – Find a training provider:**
  - https://niccs.cisa.gov/training/search
- **DAU CyberSecurity (Current Topics):**
  - https://media.dau.edu/channel/CyberSecurity/62925431
- **DAU Training**
  - ACQ 160: Program Protection Planning Awareness, Lesson 5.3
  - ENG 260: Program Protection for Practitioners
  - CLE 074: Cybersecurity Throughout DoD Acquisition
  - ISA 220: Risk Management Framework (RMF) for the Practitioner

Potential Talent Based Roles From The NICE Framework

Yellow Team	Blue Team	Red Team
• Enterprise Architect	• Network Operations Specialist	• Secure Software Assessor
• Software Developer	• Cyber Defense Forensics	• Info Sys Sec Developer
• Systems Developer	• Secure Software Assessor	• Sys Sec Analyst
• Systems Requirements Planner	• Info Sys Sec Developer	• Security Architect
• Data Analyst	• Sys Sec Analyst	• Cyber Operator
• System Administrator	• Security Architect	• Target Network Analyst
• Database Administrator	• Cyber Defense Infrastructure Support Spec	• Target Developer
• R&D Specialist	• Cyber Defense Analyst	• Cyber Ops Planner
• Network Operations Specialist	• Vulnerability Assessment Analyst	• Exploitation Analyst
	• Threat Warning Analyst	• Threat Warning Analyst
		• Cyber Intel Planner
		• All Source Collection Requirements Manager
		• All Source Analyst

Five Major Disciplines in the NICE Framework



https://niccs.cisa.gov

Example Cybersecurity Working Group Roles	Chief Developmental Tester	Systems Security Engineer	Information System Security Manager	Lead Systems Engineer Representative	Lead Software Engineer/Architect	Lead DT&E Organization Representative	Operational Test Agency Representative	Cybersecurity DT&E Technical Experts	Cybersecurity OTA Technical Experts	Security Controls Assessor	Cybersecurity SMEs	Cyber-intelligence SME	CSSP/DCO Representative	System Maintainers/Logistics	Cyber Test Range Representative	Service T&E Policy Representative		
Major Cybersecurity Tasks	R=Responsible, A=Accountable, S=Supporting, C=Consulting, I=Informed																Comments	Source
Phase 1	**Understand Cybersecurity Requirements (and Plan for T&E)**																	
Compile List of Cybersecurity and Resiliency Requirements	A	S	S	C	C	R	C	S	C	S	S	C	C	C	C	I		
Prepare for Cybersecurity T&E Events	A	S	S	C	S	S	S	R	R	S	S	C	C	C	S	I		
Develop Cybersecurity T&E Strategy	A	S	S	C	C	R	R	S	S	S	C	C	C	C	C	I		
Phase 2	**Characterize the Cyber-Attack Surface**																	
Identify the Cyber-Attack Surface	A	S	S	C	S	C		R	S	S	S	S	S	S		I		
Analyze the Cyber-Attack Surface	A	S	S	C	S	C		R	S	S	S	S	S	S		I		
Document Analysis Results and Update Test Plans	A					C		R	S	S		I	I	I		I		
Prepare for Phase 3 and 4 Cybersecurity T&E Events	A		S			R		S		S		I	I	I	S	I		
Phase 3	**Cooperative Vulnerability Assessment (CVI)**																	
Plan CVI Test Activities	A		S			R		S		S	C	S	I	I	S	I		
Conduct CVI Events	A		S			R		S		S	C	S	I	I	S	I		
Document CVI Test Results	A		S			S		R		S	C	I	I	I		I		
Prepare for Phase 4 Cybersecurity T&E events	A		S			R		S		C	C	S	I	I	S	I		
Phase 4	**Adversarial Cybersecurity DT&E (ACD)**																	
Update Cyber Threat Assessment	A	S	S	S	S	R		S			S	S				I		
Update Kill Chain Analysis	A	S	S	S	S	C		R		S	S	S				I		
Plan Adversarial DT&E	A		S			C		R			S	S			S	I		
Conduct ACD	A		S			S		R			S	S	S	S	S	I		
Document ACD Test Results	A	I	S	I	I	S		R	I	I	S	S	S	S	S	I		
Phase 5	**Cooperative Vunerability and Penetration Assessment (CVPA)**																	
Plan CVPA			S				A		R		S	S	S	C	S	I		
Coordinate with Cybersecurity Vulnerability Assessment Team			S				A		R		S	S	S	C	S	I		
Execute CVPA and Document Results			S				A		R		S	S	S	C	S	I		
Phase 6	**Adversarial Assessment**																	
Plan Adversarial Assessment			S				A		R		S	S	S	C	S	I		
Coordinate with Cybersecurity Vulnerability Assessment Team			S				A		R		S	S	S	C	S	I		
Execute AA and Document Results			S				A		R		S	S	S	C	S	I		

Figure F- 2. Example RASCI Table

Table A-2. Quick-Look Summary of DT&E Cybersecurity Phases 1 through 4

	Phase 1 Understand Cybersecurity Requirements	Phase 2 Characterize Cyber Attack Surface	Phase 3 Cooperative Vulnerability Identification	Phase 4 Adversarial Cybersecurity DT&E
Inputs	• Program Office Requirements Documentation • Cyber Survivability Risk Category (from CSEIG) • DBS System Functional Requirements • PPP, Cybersecurity Strategy • System Engineering Plan • DoDAF System Views • DBS Design specifications • DBS Capability Implementation Plan • System Requirements Documents • VOLT Report/STAR, Cyber Threat Modules • RMF Security Plan, RMF Security Assessment Plan • MBCRA	• List of cybersecurity and resilience requirements assembled in Phase 1 • CONOPS, CONEMP, User manuals • DBS Capability Implementation Plan • DBS Capability Support Plan • CSSP Support Plan • ISP • DoDAF operational views and system views • DBS Design Specifications • System Design Documents • System Interface Control Document • RMF Security Plan and Security Assessment Plan • Authorization boundary diagrams • Program Protection Plan • System Threat Assessment • System Engineering Plan • TEMP and MBCRA	• Cybersecurity portion of the DEF • Attack Surface Analysis Report from Phase 2 • Test results from contactor T&E activities • Test results from component level testing • Software Requirement Specification • Software Test Plan • DBS Capability Implementation Plan • DBS Capability Support Plan • Test Strategy for Phase 3 • Updated TEMP • RMF Security Assessment Plan • RMF Security Plan • MBCRA results	• Cyber threat assessment • Kill chain analysis • Cyber-attack surface analysis • VOLT Report, CTMs, DITL, or service/component threat assessment • Verification of cybersecurity T&E infrastructure requirements from Phase 3 • All cybersecurity test results to date • Mature and stable system baseline • MBCRA
Major Tasks	• Compile list of cybersecurity and resiliency requirements • Prepare for cybersecurity T&E Events – Develop the initial DEF – Identify supporting cybersecurity T&E resources – Develop the initial OT evaluation framework – Align RMF activities with the TEMP – Plan and schedule an MBCRA • Plan for cybersecurity T&E – Develop cybersecurity T&E strategy	• Identify the cyber-attack surface – Examine system architecture, components, and data flows – Analyze and decompose system mission – Map mission dependencies • Analyze the attack surface – Characterize the cyber threat – Examine cyber effects on the system and mission – Develop cyber kill chain – Perform or update MBCRA • Document results and update test planning and artifacts – Document results of cyber-attack surface analysis in a cyber-attack surface analysis report • Prepare for Phase 3 and Phase 4 cybersecurity DT&E events – Formulate test strategy	• Plan CVI Test Activities – Develop cybersecurity test objectives – Contractor testing – Plan test events – Document test plans – Plan cyber test infrastructure – Integrate system testing • Conduct CVI events and document results – Obtain reports – Cybersecurity evaluation – Update mission-based cyber risk assessment • Prepare for Phase 4 adversarial cybersecurity DT&E event	• Update cyber threat assessment and kill chain analysis • Plan adversarial DT&E – Develop test objectives – Define metrics – Identify resources – Develop rules of engagement – Define process and test cases – Plan integrated tests – Document test plans – Finalize preparation of test infrastructure – Conduct TRR • Conduct adversarial cybersecurity DT&E – Perform ACD events – Obtain reports – Cybersecurity evaluation – Exit criteria for cybersecurity DT&E
Outputs	• Cybersecurity and resilience requirements • Inclusion of T&E items within the system Development RFP • Updates to MBCRA	• Attack surface analysis report • Identified attack-surface protection responsibilities • Updates to MBCRA	• CVI reports • Evidence of tracking or remediation of known system vulnerabilities • Planning for at least one future ACD event • Verification of T&E infrastructure requirements for Phase 4, ACD • Updates to MBCRA	• ACD event assessment reports • Updated RMF POA&M • Cybersecurity evaluation • Updates to MBCRA

Table A-3. Quick-Look Summary of OT&E Cybersecurity Phases 5 and 6

	Phase 5 Cooperative Vulnerability and Penetration Assessment	Phase 6 Adversarial Assessment
Inputs	• Phase 1 and 2 artifacts • Authorization to Operate • Test results from contactor DT&E • Identification of mission-impacting deficiencies • Resolutions to identified mission impacting deficiencies • Completion of residual DT&E • Updated cybersecurity evaluation • Operational Test Readiness Review • Approval of operational test plan by appropriate authority • Updated MBCRA	• Authorization to Operate • Test results suggestive that system is capable of operation in intended environment • Remediation (verified fix, or documentation) of all mission-impacting deficiencies previously identified • Approval of operational test plan by appropriate authority • Verification, validation, and accreditation for all ranges and simulations to be involved in the event • Training completion for operators, system administrators, and network administrator • Recent MBCRA results
Major Tasks	• Plan CVPA • Coordinate with OTA • Execute CVPA • Document results	• Plan adversarial assessment • Coordinate with the OTA team • Execute the adversarial assessment • Document results
Outputs	• DOT&E Memorandum identifies the minimum expected data • CVPA report with discovered vulnerabilities • POA&M for remediating all major vulnerabilities • Documented operational implications of non-correctable vulnerabilities • Updated MBCRA	• DOT&E Memorandum identifies the minimum expected data • Operational evaluation • Updated MBCRA

Page A-4

An Approach to Assessing Your Team

Quadrant I, II, IV:

Needs Vectoring, Resources, and Top Cover

- Future Team
- Dream Team
- Action Team
- Ad-hoc Collaborators
- The Newbies
- Working Group

Quadrant III:

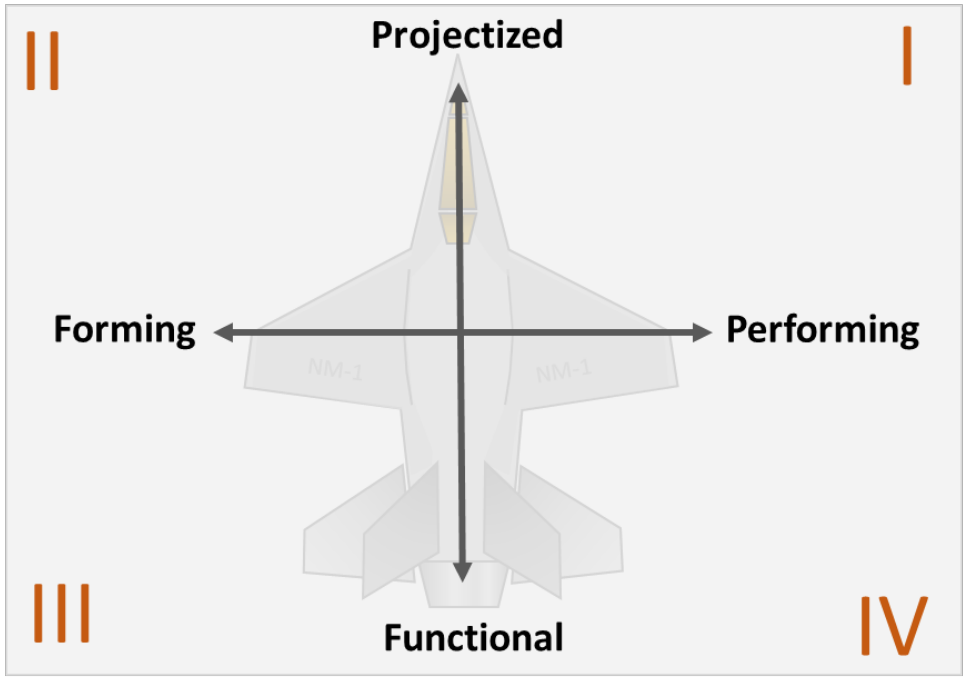
Needs Instructing, Coaching, and Mentoring

- The Cats
- The Lost Ones

- Aggressors Feed Forward Vulnerabilities to Defenders Continually
- Defenders Hunt Bad Guys, Removes Them, Patches Vulnerabilities
- Aggressor Acts Like Bad Guys to Find Vulnerabilities

Factors:

- Team Dynamic: Tuckman's Stages of Group Development
- Team Autonomy: Organizational Structures from Functional to Projectized



Driving Forces:

- National Security Pivot to Strategic Competition
- National Cyber Strategy
- DOD Cyber Strategy
- Response to Advanced Persistent Threats Obtaining DOD Weapons Program Data through Cyberattacks

Threshold of Competency:

- Acq Level 1
- 3 Level on AF Cyber Weapons Systems

Single Team Lead:

Single source of prioritization, direction, and workplace culture

- RDT&E Members
- Range Members
- MDT Members

Fully Trained:

- Acq Level 3
- 7 Level on all AF Cyber Weapon Systems

Functional Managers:

Multiple priorities, visions, and workplace cultures

- Certified Cyber Teams
- RDT&E Members
- Range Members
- MDT Members

Example of Ranking Teams

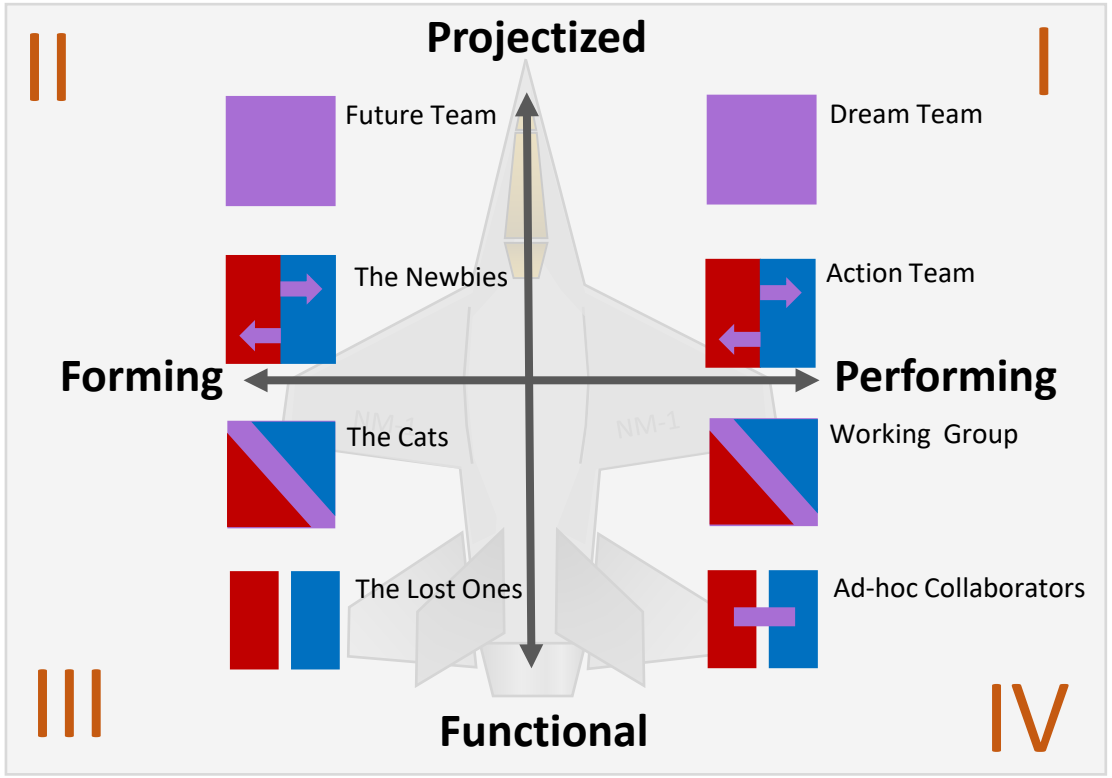
Single Team Lead:

Single source of prioritization, direction, and workplace culture

- RDT&E Members
- Range Members
- MDT Members

Driving Forces:

- National Security Pivot to Great Power Competition
- National Cyber Strategy
- DOD Cyber Strategy
- Response to China and Russia Obtaining DOD Weapons Program Data through Cyberattacks



Factors:

- Costs and time to move from Junior to Senior team
- Ability to move from Functionally Aligned to Projectized

Threshold of Competency:

- Acq Level 1
- 3 Level - Cyber Tools, Tactics, and Procedures

Fully Trained and Engaged:

- Acq Level 3
- 7 Level - Cyber Tools, Tactics, and Procedures

Aggressors Feed Forward Vulnerabilities to Defenders Continually

Defenders Hunt Bad Guys, Removes Them, Patches Vulnerabilities

Aggressor Acts Like Bad Guys to Find Vulnerabilities

Functional Managers:

Multiple priorities, visions, and workplace cultures

- RDT&E Members
- Range Members
- MDT Members