USW(R&E)

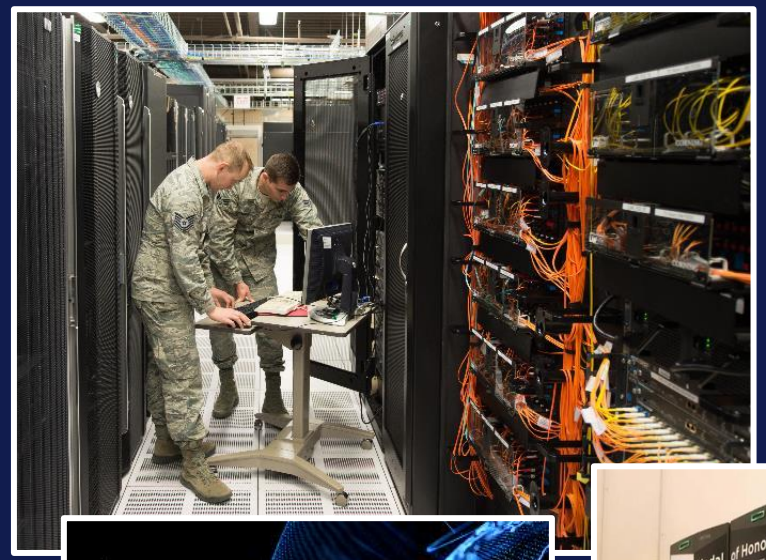
Provable Security: Operationalizing Formal Methods for National Defense

Developing a Strategy to Bridge the Transition Gap

Forrest Shull,
Principal Director, Advanced Computing and Software
Office of the Assistant Secretary of War for Critical Technologies

11 May 2026

Background: AC&S Strategic Landscape



SUPERCOMPUTER CARPENTER

The future is software-defined *everything.*

Software and computing are ubiquitous in the Department

- Critical to the performance of almost every weapons system.
- Underpins game-changing emerging technologies, including artificial intelligence and quantum computing.
- Provide communications, command and control.
- Used to create and improve new weapons systems.

Software allows transformation in warfighting capabilities without large platform re-investments.

Speed of developing and evolving software-enabled capabilities is a competitive advantage – Can make the difference between having a capability in the fight, or not.

Background: The Charge from Senate Armed Services Committee (SASC)

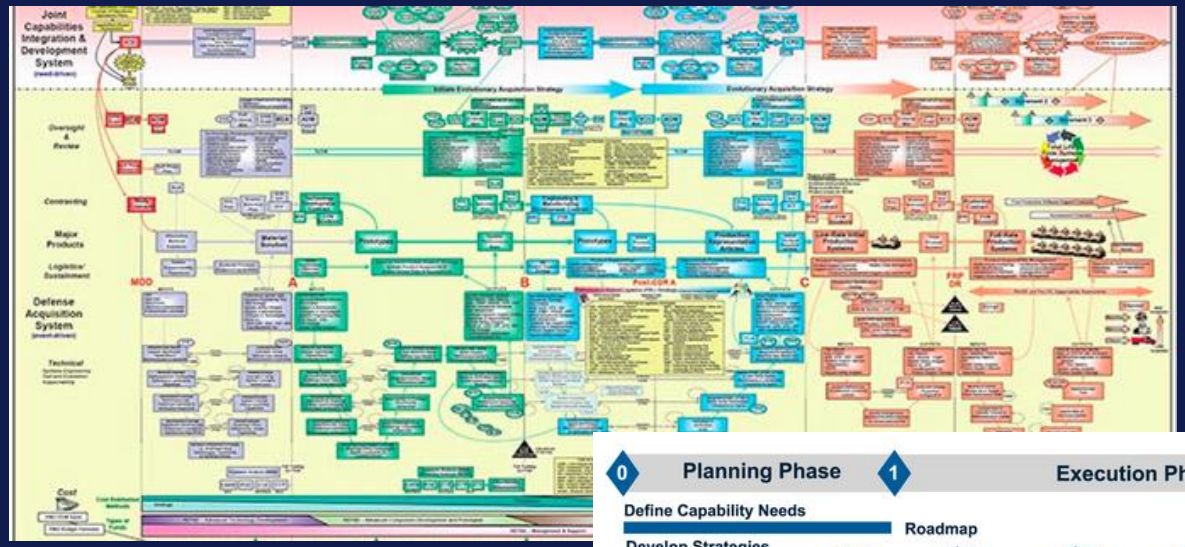
"The committee is concerned about the advancing sophistication, scale, and speed of cyber threats targeting Department of Defense (DOD) systems. The committee notes that formal methods and approaches for validation and verification, which establish mathematical guarantees in software code, can be used to prove the absence of exploitable vulnerabilities."

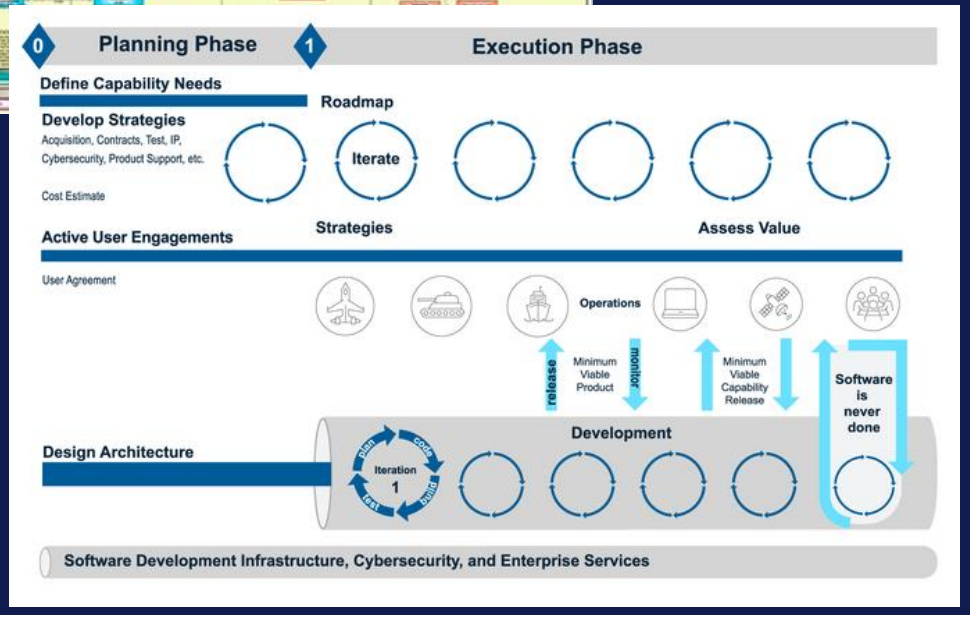
"The committee also notes that such approaches can and have also been used to secure hardware systems as well, demonstrating even broader application of formal methods."

"The committee directs the Secretary of Defense… to develop a comprehensive strategy for transitioning DARPA's formal methods research investments into production environments across the DOD."

-Senate Armed Services Committee,
National Defense Authorization Act, FY 2026, Senate Report 119-39

DoW Software Acquisition Modernization





Paradigm Shift: Software Acquisition Policy (DODI 5000.87) is radically different from traditional Department of War (DoW) approaches

- Built around best commercial practices
- Requires delivery of working software at least annually
- Adopted by 80+ programs
- Requires modern software practices and automation

Context: DoW Software and Computing

The … software development methodology will incorporate **continuous testing and evaluation, resiliency, and cybersecurity, with maximum possible automation**, as persistent requirements and include a risk-based lifecycle management approach to address software vulnerabilities, supply chain and development environment risk, and intelligence threats throughout the entire lifecycle.

- DoD Instruction 5000.87, "Operation of the Software Acquisition Pathway," 2020

The Department of Defense (DoD) has been slow to recognize that **software-defined warfare is not a future construct, but the reality we find ourselves operating in today**. Software is at the core of every weapon and supporting system we field to remain the strongest, most lethal fighting force in the world. …DoD has struggled to reframe our acquisition process from a hardware-centric to a software-centric approach.

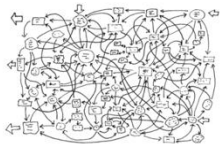
- Secretary of Defense Pete Hegseth, "Directing Modern Software Acquisition to Maximize Lethality," 2025

Software is a critical element of systems in the Department of Defense (DoD) and the ability to deliver **software at the speed of relevance** requires continued software modernization… DoD continues toward a future where artificial intelligence will help make common and complex software functions commodities.

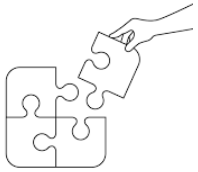
- 2025-26 US DOD Software Modernization Implementation Plan

The Shared Challenge: Broad Transition

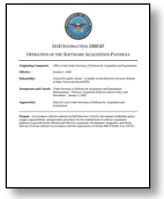
Some reasons why Formal Methods have been difficult to transition:



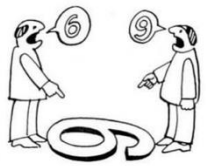
Integration Complexity: Requires specialized subject matter experts, unique software tooling integration, and deliberate coordination between verification experts and development teams.



Workforce Gaps: Limited availability in both government and industry of needed expertise.



Policy Gaps: Absence of clear guidance that recognizes and incentivizes adoption.



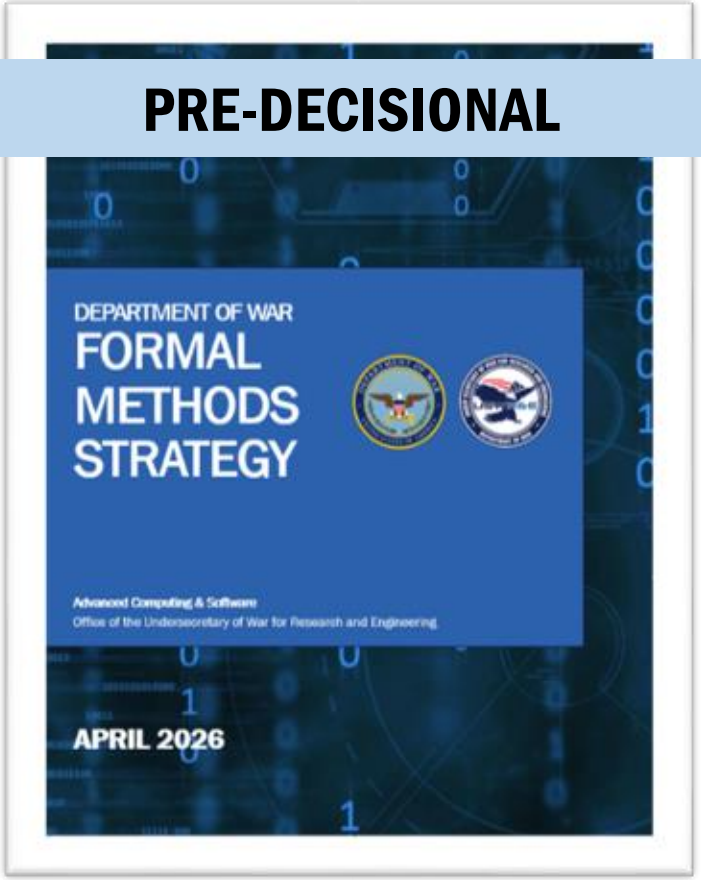
Perception Barriers: Misconception that application requires prohibitive costs and implementation timelines.

Strategy: A Three-Pillar Approach to Transition

Major Areas of work:

1. Characterize Costs & Benefits for DoW
2. Integrate into the Ecosystem
3. Engage with Industry

PRE-DECISIONAL



Collaboration among stakeholders in:

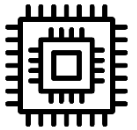
- Office of the Under Secretary of War (OUSW) for Research and Engineering (R&E)
- OUSW(Acquisition and Sustainment)
- Defense Advanced Research Projects Agency (DARPA)
- Director Operational Test and Evaluation
- Department of War Chief Information Officer

1. Costs & Benefits in Defense

Challenge: Provide clear expectations for the Department in terms of what to expect in terms of pricing, benefits, and deliverables under realistic acquisition conditions.

What We Are Doing / Have Done:

Multiple years: DARPA technology development
Over 20 successful transitions to DoW acquisition programs



2025: OUSW(A&S) assessment
Conducted assessment of operationally relevant product acquisition applying formal methods; identified positive impacts to cost, quality, and schedule

2025-2028: DARPA Capstones
Executing targeted pilot projects to collect additional longitudinal data and evidence in high-priority contexts.

2025: DARPA Industry Accelerator
Funding a select group of innovative industry proposals, enabling them to validate the commercial viability of advanced formal methods integration in commercial applications.

1. Costs & Benefits in Defense

What's next?

- Define / refine **Key Performance Indicators** to help DoW:
  1. Set clear expectations for impact and cost-effectiveness of formal methods applications, relative to alternative security approaches.
  2. Use lightweight, periodic performance reviews to adjust strategies, update implementation approaches, and provide a continuous learning and adaptation cycle across programs.
  3. Leverage data from ongoing pilots to understand which metrics can be insightful across multiple programs.

2. Integrate into the Ecosystem

Challenge: How to embed formal methods into iterative approaches such as continuous integration / continuous development (CI/CD) pipelines so they are compatible (technically, time-horizon-wise, etc.) with the rest of our ecosystem.

How do we make the technology intelligible to developers and decision-makers, not just to PhDs?

What We Are Doing / Have Done:

Ongoing: "Ratcheting Levels" proposal

Provide a useful pathway showing how formal methods adoption can start with lighter weight approaches and progress to more formality, with assurance results commensurate with need and increasing costs.

Lightweight formal methods envelope suitable for most projects/programs

L1	Automatically extracted description of system architecture	**Get the true-to-life building plans:** Tools to assure description is faithful to code Tools to recover architecture from code bases
L2	Automated descriptions of all valid / expected inputs at all system interfaces	**Lock the front door, and all doors:** Tools to automatically generate input-handling code Tools to automatically generate validity filters Tools to automatically generate input tests at scale
L3	Memory safety certificate (per-module and globally)	**No data corruption, no data leakage:** Tools to assure memory safety across complete code bases, including glue code and ABIs
L4	Models and proofs of stated properties	**Mission-relevant models:** Automated tools to assure models Tools to recover models & validate faithfulness to code
L5+	Functional correctness specifications, with proofs of security against well-defined threat models	**Proven security against threat models:** (Semi-automatic) tools to produce and validate proofs

Ongoing: Industry SMEs

Attract experts experienced in making formal methods viable in commercial environments to share their best practices in government contexts.

Sidebar: Communicating a Framework for Adoption

Gradual Assurance & Understanding Framework: Demonstrate that "ratcheting up" resilience is possible, and technologies can be matched to different program needs.

- Rely on (semi-)automated tools and concrete artifacts that can be required from contractors.

	Deliverable	Informal Goal Statement	DARPA tech
L1	Automatically extracted description of system architecture	Get the true-to-life building plans	ARCOS, V-SPELLS
L2	Automated descriptions of all valid / expected inputs at all system interfaces	Lock the front door, and all doors	SafeDocs, V-SPELLS, HARDEN
L3	Memory safety certificate (per-module and globally)	No data corruption, no data leakage	Rust; V-SPELLS
L4	Models and proofs of stated properties	Mission-relevant models	(varied)
L5	Functional correctness specifications, with proofs of security against well-defined threat models	Proven security against threat models	ARCOS, SafeDocs, AMP, others

Natural boundary for lightweight formal methods – Many programs could benefit from these practices.

2. Integrate into the Ecosystem

- **What's Next / Where We Need You:**
  1. Feedback on the "**Ratcheting Levels**" proposal – To reflect broad experience
  2. Engaging with DoW Software Factories - Transitioning into these **enterprise resources** would affect improvements for many programs; need to understand their unique needs and transition opportunities
  3. Best Practices Guide – Help set **incentives and expectations** for more programs
  4. Best practices for application to **both software and hardware** – Ensure we are answering the SASC call for broad application, and addressing mission level needs

3. Engaging with Industry

Challenge: Create the right incentives for performers to bring these technologies into their work for DoW. Ensure we are able to articulate concrete, verifiable, and valuable deliverables that can be written into a contract.

What evidence is needed to be provided to the government for confidence in the outcome and what are the blockers from industry performers?

What We Are Doing / Have Done:

2024-25: DARPA / R&E Defense Chief Technology Officer (CTO) Round Tables and other industry events

- Invited participation from industry (traditional Defense Industrial Base, new entrants, small nontraditional providers…) and DoW (up to the Under Secretary level)
- Assessed current activities and perceptions and gather recommendations
- All participating CTOs expressed support for:
  - Enhanced Cyber Resiliency Standards
  - Cyber Resiliency Block Upgrade Demonstrations

3. Engaging with Industry

- **What's Next / Where We Need You:**
  1. Policy feedback – Make us aware of existing policies or guidance that are getting in the way.
  2. Product offerings that reduce barriers to use and show impact in realistic contexts with other practices
  3. Continued dialog

Call for Feedback

Help us articulate the value proposition of Formal Methods for DoW.

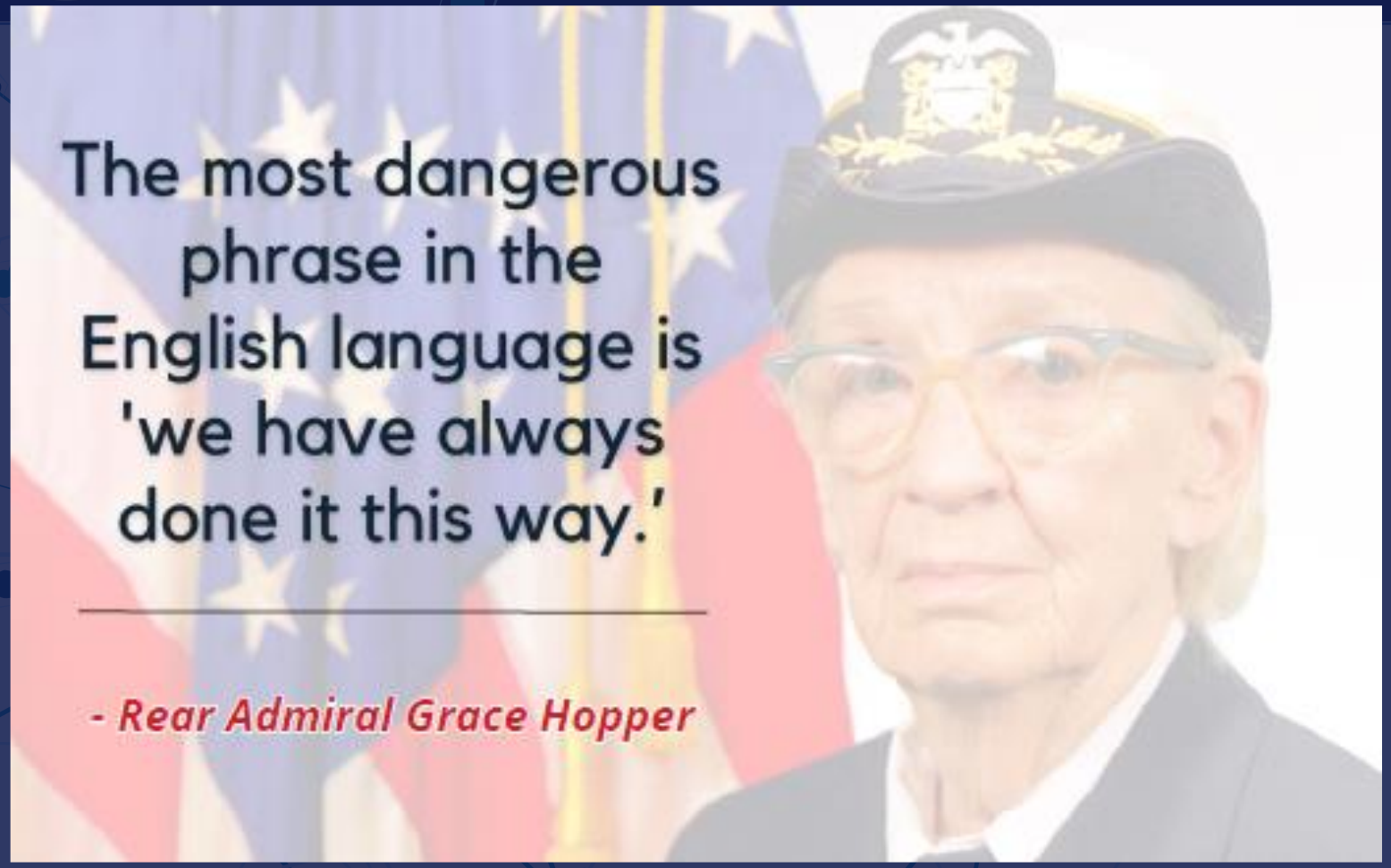
Challenge: What would a hypothetical **"cyber resiliency block upgrade"** look like for a system?

- **How would the government describe the requirements, monitor progress, and know if the work is successful?**

Challenge: Feedback on the strategy.

- **What are we missing? What else is needed to support transition into production environments across the department?**

Call for Feedback



Maruan Barakat,
Advanced Computing & Software Action Officer

maruan.m.barakat.ctr@mail.mil