Leveraging Industry Innovation

An Army Cyber Innovation Challenge

As cyberspace grows more complex and increasingly contested with sophisticated threats able to exploit known and unknown vulnerabilities, cyberspace operations and cybersecurity are exceptionally critical to national security.[1] The Army's portion of the cyberspace domain requires an effective understanding of the technology landscape as it relates to current and future cyberspace capability needs. At all levels, the Army seeks to build, operate, and maintain secure and defensible networks, protecting them against specific threats to achieve mission assurance, while denying the adversary freedom of action in the cyberspace domain. New and creative processes and models are required to mature holistic Army Cyberspace operations, comprised of offensive, defensive, and DoD Information Network (DoDIN) capability areas. Army perspective points, or pillars, to achieving a future vision of Army Cyberspace Operations consist of the following:

- Integrated ***Offensive Cyberspace Operations (OCO)*** providing degradation, disruption, or destruction effects.
- Transformed ***Defensive Cyberspace Operations (DCO)*** enabling maneuver, passive and active defense.
- Improved ***DoD Information Network (DoDIN)*** for a robust and assured defensive cyber posture.
- Integrated ***Cyberspace Situational Understanding*** capability providing analytics, storage, and correlation to reduce risk.

As a response to the operational community, the Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)) System of Systems Engineering & Integration (SoSE&I) Directorate developed the Army Cyber Innovation Challenge model. The model leverages existing authority, enabling an agile and flexible process to investigate priority Army cyberspace requirements. The challenge model provides a rapid prototyping capability to aid developmental acquisition strategies.

In structuring the challenge framework, ASA(ALT) collaborated with the operational and requirements communities, specifically Army Cyber Command (ARCYBER) and the U.S. Army Cyber Center of Excellence (CoE), to identify priority operational needs and align capabilities to formal gap analysis and requirements. To date, the Cyber Innovation Challenge has proven an effective mechanism to engage non-traditional vendors and quickly procure prototype technologies for operational evaluation.

---

[1] House Armed Services Subcommittee on Emerging Threats and Capabilities, Lieutenant General Edward C. Cardon, Commanding General U.S. Army Cyber Command and Second Army, First Session 114th Congress, March 4, 2015.

As the process continues to mature, it is important to note that this model is based on two "absolutes" or imperatives that are necessary for enduring success. First, the pace of change in this relatively new "Cyber" domain demands a culture of continual collaboration and information exchange to maintain a common understanding of perspective points supporting the future vision of Army Cyberspace Operations. These perspective points enable stakeholders to envision how investment decisions for priority requirements contribute to achieving the Army's vision for Cyberspace Operations. The second absolute speaks to building an enduring capability, which means prototyping efforts are not executed in a vacuum but are aligned with a requirements champion inside the acquisition community who will ultimately perform lifecycle management of the capability. This allows users to evaluate prototype solutions and provide critical feedback to the Cyber CoE and the lifecycle manager to mature the requirement, addressing the operational need.

The Consortium Business Model and Other Transaction Authority

To execute each Cyber Innovation Challenge, the Army works through a consortium, a voluntary organization with members from industry, academia and government, and uses a flexible acquisition mechanism known as Other Transaction Authority (OTA). This approach allows the Army to quickly solicit, evaluate and purchase limited quantity prototypes of equipment from a wide range of non-traditional sources, including small and micro companies who may lack the resources to engage in the traditional government contracting process.

To ensure the full scope of Army requirements and technology objectives would be accommodated within a single consortium community, ASA(ALT) engaged with Army Research, Development and Engineering Center (ARDEC) to adequately scope technology objectives and utilize an existing community, the Consortium for Command, Control, and Communications in Cyberspace, known as C5. The Army's vision is to leverage the C5 community to help guide the development of next-generation defensive, offensive, and DoDIN cyberspace operations capability. The consortium approach allows for cross-sector collaboration among industry, university, and government entities, offering diversity of subject matter expertise focused on addressing the most critical cyberspace operational challenges.

Historically, government has difficulty leveraging leading-edge technology and capability developed by small and mid-size businesses. The Cyber Innovation Challenge seeks to change that by using the OTA mechanism. By using OTA, which focuses on quickly delivering limited quantity prototypes, the Army eliminates barriers found in the typical federal contracting process that can diminish participation by non-traditional companies. In a fiscally constrained environment, the consortium community leverages the investments and innovation of all participating members to improve cyberspace operations return on investment.

As part of continued development of a holistic approach to cyberspace operations capability development, use of Other Transaction Authority through C5 will improve Army acquisition innovation and responsiveness to defend and counter emerging cyber threats. The maturing and repeatable challenge-based model supports efficient and effective requirements analysis and evaluation of technology. Ultimately, the challenge model reduces the burden placed upon the commercial and non-traditional vendor community to engage the government.

The model shown below provides a high level view of the two-phase down select process, illustrating how a well-articulated requirement initiates the process to efficiently investigate new and emerging requirements areas. The model allows for both a traditional white paper response from interested vendors in addition to a hands-on "challenge" based technical exchange event to raise the government's confidence that the technology adequately addresses the requirement.

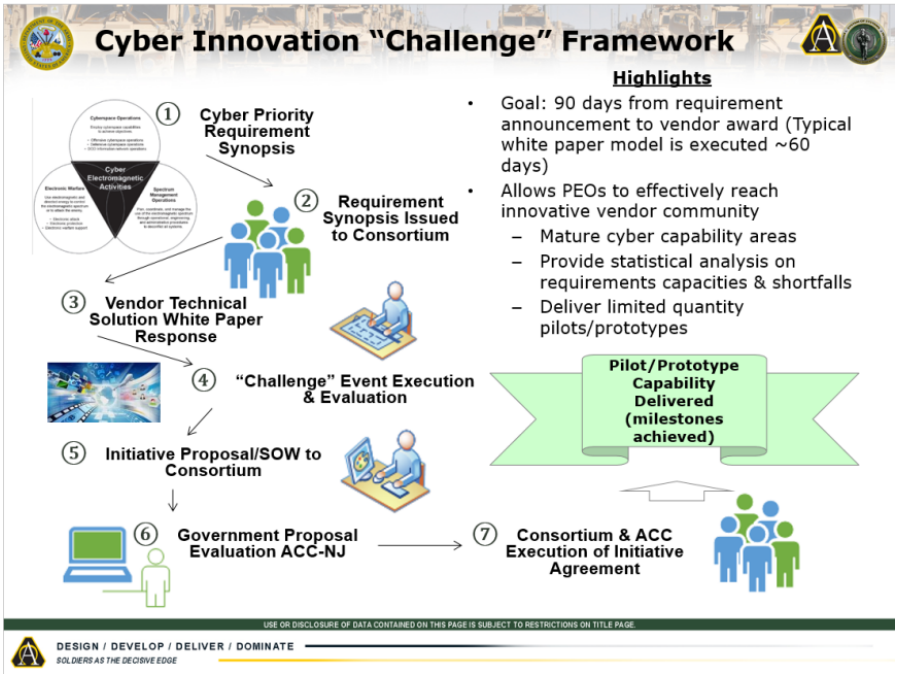

Figure 1: Cyber Innovation Challenge Framework

The model is designed to be flexible for both the government and vendors, while maintaining enough due diligence and rigor to maintain confidence that the investment in prototype solutions is providing leading edge technology and innovation in the requirements space. The entire process is designed to go from requirement to vendor award in approximately 90 days.

(R) Requirement	Requirements Synopsis Advertised to Community
(R) + 14 Days	Vendor White Paper down-select and invitation to challenge demonstration
(R) + 35 Days	Conduct Technical Exchange and/or Demonstrations
(R) + 60 Days	Vendor(s) Proposal Requests
(R) + 90 Days	Vendor Awards Issued

Figure 2: Typical Army Cyber Innovation Challenge Timeline

Roles/Responsibilities

Success of the Cyber Innovation Challenge depends on an enduring partnership and ongoing collaboration between ARCYBER (the operational element), the Cyber CoE (the requirements element), and ASA(ALT) (the acquisition element). A mix of personnel from each of the stakeholder organizations comprise a technical team that works together throughout the entire process to develop challenge requirements, identify evaluation criteria, evaluate vendor white paper proposals, conduct vendor technical exchange and demonstrations, and ultimately provide a recommendation to the requirement champion for vendor awards.

ASA(ALT) engages the ARDEC and C5 early in the planning process to develop the challenge execution framework, which involves the issuing of high level solicitations; identification and alignment of a life cycle manager, typically a Program Executive Office (PEO) Project Manager (PM); and identification of a resourcing profile for each specific challenge. ASA(ALT) provides personnel to the technical team in addition to the program manager, to facilitate the execution of the whitepaper evaluation and ultimately providing the vendor recommendations for selected prototype capabilities.

The Cyber CoE is responsible for analyzing, determining, and championing cyberspace operations requirements influenced by Army concepts, strategies, analyses, and lessons learned; to be investigated through the Innovation Challenge framework. TRADOC support involves additional resources related to experimentation, assessments, and data collection; which includes, but not limited to hosting evaluations events of candidate technologies.

ARCYBER is responsible for articulating cyber needs from the operational perspective, through Operational Needs Statements (ONS) framing early requirements language as a bridge to the enduring Joint Capabilities Integration and Development System (JCIDS) requirements documents. As part of the planning process, ARCYBER also assists in identifying appropriate cyber units to evaluate the delivered prototypes in an operational environment.

With these organizations and other partners working in tandem, the Innovation Challenge will continue to provide the means for agility and cross-sector collaboration to address priority requirement gap areas in the cyberspace domain.

Innovation Challenge Status

The Army has conducted three (3) formal Innovation Challenge events starting in May 2015 and most recently hosted an event in March 2016. The status of each challenge is as follows.

Innovation Challenge #1 (Deployable Defensive Cyberspace Operations [DCO] Infrastructure [DDI]): The winning vendors from Challenge #1 are delivering prototype solutions to Army cyber forces in April 2016 (10 months after formal release of the requirement), totaling ~$4.5M in awards.

Innovation Challenge #2 (Cyberspace Analytics): The updated requirement was formally released through C5 on 5 April 2016. A 10 day extension was requested to allow additional vendors time to join C5 to participate, with vendor whitepaper responses now due 29 April.

Innovation Challenge #3 (Micro-cloud Management Solutions): The requirement is targeted for release through C5 in April 2016.

For additional information please contact Mr. Larry Jennings at 703-692-2438, larry.l.jennings8.ctr@mail.mil or Ms. Elizabeth Bledsoe, 703-571-1177, Elizabeth.e.bledsoe.ctr@mail.mil.