Appendix E Case Study: Army Cyber Innovation Challenge Using OTA

E.1 Background

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.[77] 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, comprising offensive, defensive, and DoD Information Networks (DoDIN) capability areas. Army perspective points, or pillars, to achieving a future vision of Army Cyberspace Operations consist of:

- 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; and
- 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)) Systems 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.

E.1.1 Problem Set

The Army continually seeks to mature and operationalize the cyberspace domain. General Milley, U.S. Army Chief of Staff, when testifying before the Senate Armed Services Committee, stated that one of the Army's top priorities is "…to invest in the technologies, organization, and doctrine that will allow us to maintain overmatch against future adversaries while retaining the ability to adapt to unforeseen challenges." Army networks and information systems are large and complex, creating a large cyberspace "footprint" within the Department of Defense (DoD). The Army relies upon secure and resilient networks to support Army and joint forces at the tactical and strategic levels. The Army must continue to modernize its networks and information systems by applying a threat-informed defense model capable of reacting

[77] House Armed Services Subcommittee on Emerging Threats and Capabilities. 2015. Testimony of Lieutenant General Edward C. Cardon, Commanding General U.S. Army Cyber Command and Second Army.

to incidents and recovering and adapting in support of Unified Land Operations. The Army's portion of the DoDIN is the technical network that encompasses all Army information management and information systems that collect, process, store, display, disseminate, and protect information worldwide. In the pursuit of increasingly defensible networks, the Army must apply technical solutions that improve the overall security posture for creating a defensible cyber terrain that is resilient and adaptable in support of Army and Joint operations.

As an integral part of addressing this problem space, the Government has partnered with organizations such as the Consortium for Command, Control, and Communications in Cyberspace (C5) and Defense Innovation Unit Experimental (DIUx) to access leading edge technology and vendors with the collective expertise in the following technology areas specifically related to Army Cyberspace Operations:

Innovative technologies, processes, methods, facilities, and capabilities – These are sought to identify, develop, test, provide access to, and improve technologies resident in universities, private and federal labs, incubators, and industry that focus on Army cyberspace requirements (offensive, defensive, and DoDIN) related to weapons and weapons systems. At all levels, the Army seeks to build, operate, and secure defensible networks, defending them against specific threats to achieve mission assurance while denying the adversary freedom of action in the cyberspace domain.

Offensive Cyberspace Operations Objectives – Technologies supporting operations to project power by the application of force against enemies and adversaries in and through cyberspace.

Defensive Cyberspace Operations Objectives – Technologies supporting operations conducted to defend DoD or other friendly cyberspace and preserve the ability to utilize friendly cyberspace capabilities.

- Technologies to gain and maintain situational awareness through the visualization of key cyber terrain and an understanding of the actions occurring within that terrain;
- Technologies that actively predict and hunt for (search and discover) advanced internal cyber threats and vulnerabilities that do not trigger or generate warnings using routine detection measures;
- Technologies that allow friendly cyber forces to outmaneuver adversaries by performing preapproved, automated, agile, internal countermeasures that stop or mitigate cyber-attacks; and, when authorized, to conduct response actions external to friendly networks in order to create effects that deny the adversary use of offensive cyber capabilities;
- Technologies to conduct DCO mission planning and protection that identify and assure the availability of key cyber terrain and critical infrastructure for the Army, DoD, host nation, and civil authorities that support Army missions;
- Technologies that protect networks, information technology platforms, and data by controlling inbound/outbound traffic, dynamically managing locations of critical services, and hardening information systems;
- Technologies to conduct mission assurance actions that dynamically re-establish, re-secure, re-route, reconstitute, or isolate degraded or compromised networks;
- Technologies to conduct site exploitation and forensic analysis and determine technical and operational impacts of intrusions; and

- Technologies to evaluate the defensive posture of networks and information systems using vulnerability assessment methods and threat emulation in order to recommend or direct changes to ensure operational readiness.

DoDIN Operations Objectives – Technologies supporting operations to design, build, configure, secure, operate, maintain, and sustain networks.

- Technologies to build (plan, engineer, install) secure, resilient, and defensible networks;
- Technologies that support global, secure, adaptive, and rapid access across trusted and authenticated domains to authorized entities;
- Technologies that allow for the secure operation of networks (i.e., automated scanning and remediation of vulnerabilities);
- Technologies that support the integration with mission partners during garrison and deployed operations; and
- Technologies that support the discovery, delivery, and storage of data to provide awareness and access to information in a timely and efficient manner.

E.1.2 Acquisition Approach

To ensure the full scope of Army requirements and technology objectives would be accommodated through various consortium communities and associated models, ASA(ALT) engaged with the Army Armament Research, Development and Engineering Center (ARDEC) to adequately scope technology objectives and utilized an existing community, the Consortium for Command, Control, and Communications in Cyberspace, known as C5. Membership in the consortium is open (on a rolling basis) to all companies and academic institutions with associated capabilities, with annual dues of $500 annually. Academic institution fees are waived. 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. The Army's vision is to leverage various organizations such as C5, DIUx, and potentially others to help guide the development of next-generation defensive, offensive, and DoDIN cyberspace operations capability.

The Government has established a Section 845 Prototype Other Transaction Agreement (OTA) with an existing consortium, the Consortium for Command, Control, and Communications in Cyberspace (C5) that has significant non-traditional contractor participants. The goal of this consortium community is to assist in maturing Army Cyberspace Operations through re-use, augmenting existing cyber technologies, and fostering relevant cyber weapons systems and awareness in the newly established Cyber domain. Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 1-02). Maturing the Army Cyberspace domain requires an effective understanding of the technology landscape as it relates to current and future cyberspace capability needs.

The mission of the consortium is to establish the Army as a leader in cyberspace operations, capability development, R&D, education and training programs, and policy development. Additional goals include:

- Be a thought and action leader across the cyberspace operations stakeholder community;

- Serve as proof-of-concept test bed and blueprint for requirements articulation and capability development;
- Facilitate the advancement of membership cyber maturity levels (as this domain knowledge grows, the probability of warfighter technological advantage increases);
- Create a cyber center of gravity as incubator and engine for a cyberspace capability; and
- Shape and enable cyberspace operations education.

E.1.3 Consortium Business Model and Other Transaction Authority (OTA)

To execute each Cyber Innovation Challenge, the Army works through a consortium, a voluntary organization with members from industry, academia, and Government, utilizing 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.

The C5 consortium acts as a conduit and marketplace linking the Army and industry (members of the consortium). The relationship between the Army and C5 is established through an OTA, while C5 translates the Army's requirements into commercial agreements with members of the consortium. Figure E-1 depicts the relationships and overarching process flow of the consortium business model[78] used by the Army and C5.

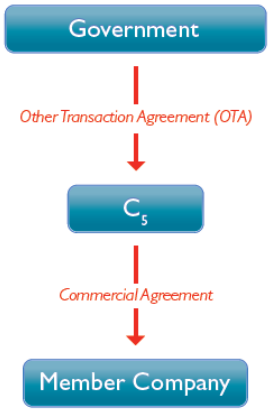

Figure E-1. Consortium Relationship Flow

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

[78] C5 Technologies. 2015. Consortium for Command, Control, Communications, and Computer Technologies. Available at: http://c5technologies.org/wp-content/uploads/2015/01/2015-C5-Brochure.pdf.

investments and innovation of all participating members to improve cyberspace operations return on investment.

Section 845(a)(2) of the National Defense Authorization Act (NDAA) for Fiscal Year 1994, Public Law (P.L.) 103-160, as amended (Title 10 United States Code (U.S.C.) Section 2371 note), authorizes the Secretary of the Army to carry out prototype projects that are directly relevant to weapons or weapon systems. In accordance with the above-referenced law, the Government must ensure that no official of an agency enters into an OTA for a prototype project under this authority unless there is significant non-traditional defense contractor(s) participation in the prototype project; or at least one-third of the total cost of the prototype project is to be paid out of funds provided by parties to the transaction other than the Federal Government. There have been several amendments to this authority over the years, specifically the FY16 NDAA, which includes additional guidance in Section 815 that is relevant to follow-on production contracts or transactions.

As part of continued development of a holistic approach to cyberspace operations capability, the use of OTA through the C5 consortium will improve Army acquisition innovation and responsiveness in the defense and countering of the emergence of dynamic cyber threats. The maturing and repeatable challenge-based model, utilizing OTA and a consortium, supports efficient and effective requirements analysis and evaluation of technology. Ultimately, the challenge-based model reduces the burden placed upon the commercial and non-traditional vendor community to engage the Government and vice versa.

Figure E-2 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. This repeatable process allows for both a traditional white paper response (to the synopsis, Request for Information, or Request for White Paper) from interested vendors in addition to a hands-on "challenge-based" technical exchange and demonstration event (typically held in a laboratory) with results evaluated for technical feasibility, raising the Government's confidence that the technology adequately addresses the requirement. After these assessments, other transaction awards are made to the most promising vendors, and the solutions (the prototypes) are provided to users for operational testing and feedback for further procurement and follow-on production and fielding decisions.

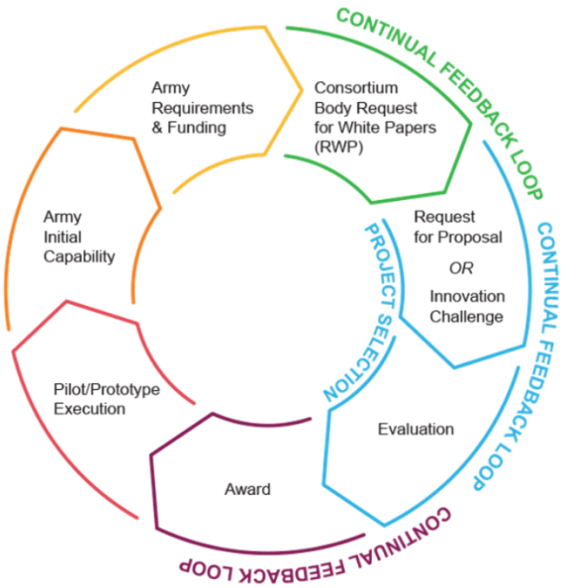

Figure E-2. Down-Select Process

Some of the highlights of this process, shown in Figure E-3, include a goal of 90 days from the identification of the requirements and funding profile to Army Contracting Command (ACC)-NJ's execution of the initiative. The typical white paper model is executed in approximately 60 days. This allows Program Executive Offices (PEOs) to effectively reach the innovative vendor community, mature cyber capability areas, provide statistical analysis on requirement capacity shortfalls, and deliver limited-quantity pilots or prototypes.

Figure E-3. OTA Process Highlights

The model is designed to be flexible for both the Government and vendors while maintaining enough due diligence and rigor to ensure confidence that the investment in prototype solutions is providing leading-edge technology and innovation in the requirements space. As shown in Table E-1, the entire process is designed to go from requirement to vendor award in approximately 90 days.

Table E-1. Estimated Process Timeline

(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

E.1.4 Cyber Innovation Challenge Evaluation Framework

The typical evaluation framework is tailored for each specific requirement and consists of an integrated assessment of the factors below:

- Ability to develop, demonstrate, implement, and transition a solution based on adequacy, reliability, and relevance of the proposed technological solution in meeting the minimum requirements and objectives as outlined within the requirements synopsis.
- Scientific and/or technical benefits of the approach described in the white paper and/or technical benefits of the proposed technological solution. Soundness of the technical approach, including complete and clear processes to deliver a comprehensive software solution. Evaluation of proposed software necessary to meet the requirements of the proposed technological solution.
- Resources required and level of expertise of the proposed personnel to meet the requirements of the proposed technological solution. This also involves the availability of facilities necessary to ensure related people, processes, and technologies can operate at appropriate classification level commensurate with applicable information or capabilities.

E.1.5 Acquisition Team Approach

Success of the Cyber Innovation Challenge depends on an enduring partnership and on-going collaboration between Army Cyber Command (ARCYBER) (the operational element), the Cyber Center of Excellence (CoE) (the requirements element), and ASA(ALT) (the acquisition element). A mix of personnel from each of the stakeholder organizations comprises 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 issuing of high-level solicitations; identifying and aligning a lifecycle manager, typically a PEO Project Manager (PM); and identifying a resourcing profile for each specific challenge. ASA(ALT) provides personnel to the technical team and the PM to facilitate the execution of the white paper evaluation and recommend the vendor 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 that are investigated through the Cyber Innovation Challenge framework. Support by the Army's Training and Doctrine Command (TRADOC) involves additional resources related to experimentation, assessments, and data collection that include, but are not limited to, hosting events to evaluate candidate technologies.

ARCYBER is responsible for articulating cyber needs from the operational perspective in an Operational Needs Statement (ONS) that frames 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 Cyber Innovation Challenge will continue to provide the means for agility and cross-sector collaboration in addressing priority requirement areas in the cyberspace domain.

E.1.6 Results and Outcomes

In structuring the challenge framework, ASA(ALT) collaborated with the operational and requirements communities, specifically ARCYBER and the U.S. Army Cyber 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.

The Army has initiated several Innovation Challenge events designed to investigate new and emerging priority requirements. The first requirement effort was kicked off in May 2015 with several follow-on requirements focused across a broad scope of Cyberspace Operations. The status of each challenge is as follows:

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

Innovation Challenge - Cyberspace Analytics: The updated requirement was formally released through C5 on April 5, 2016. The solicitation generated 47 vendor white papers, and technical evaluations were completed.[79]

Innovation Challenge - Persistent Cyber Training Environment: The requirement was released through C5 early 2nd quarter FY17. The Government technical team reviewed vendor white papers and conducted the technical evaluations, ultimately recommending seven vendors for follow-on technical exchange and final recommendation of award.[80]

Innovation Challenge - Use Activity Monitoring (UAM) as a Service: The request for white papers was closed by C5 in July 2017.

---

[79] United States Army. 2015. Army Innovation Challenge Industry Day. Available at: https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=2624a821003e97ba368836f697e533f7&_cview=0

[80] United States Army. 2016. Persistent Cyber Training Environment Challenge Article. Available at: https://www.army.mil/article/178005/

E.1.7 Lessons Learned / Best Practices

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 the relatively new cyber domain demands a culture of continual collaboration and information exchange in order 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.