ARL-MR-1044 ● Oct 2021

Robotics Research Collaboration Campus: Operations for Industry Challenges

by Marshal Childers, Arnon Hurwitz, Jeffrey Westrich, and John Millemaci

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-MR-1044 ● OCT 2021

Robotics Research Collaboration Campus: Operations for Industry Challenges

Marshal Childers, Arnon Hurwitz, and Jeffrey Westrich
Computational and Information Sciences Directorate,
DEVCOM Army Research Laboratory

John Millemaci
Energetics Technology Center (ETC)

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
October 2021	Memorandum Report	September 2020–October 2021

4. TITLE AND SUBTITLE
Robotics Research Collaboration Campus: Operations for Industry Challenge

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Marshal Childers, Arnon Hurwitz, Jeffrey Westrich, and John Millemaci

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
DEVCOM Army Research Laboratory
ATTN: FCDD-RLC-I
APG, MD 21005

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-MR-1044

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
ORCID IDs: Marshal Childers, 0000-0002-8723-6977; Arnon Hurwitz, 0000-0002-0934-8359

14. ABSTRACT
The US Army Combat Capabilities Development Command Army Research Laboratory has established a facility for developing and proving autonomy and robotics technologies to meet the needs of the Army's modernization efforts. The Robotics Research Collaboration Campus (R2C2) will build a network of partnerships around the Open Campus model to perform collaborative research, stimulate local economy and act as technology incubator. This report describes the effort to plan a technology challenge that brings industry and academia researchers together with DEVCOM Army Research Laboratory researchers and government stakeholders to offer technology solutions to certain classes of problems and gain feedback on performance. The activity will inform and accelerate Army modernization through innovation discovery, demonstration, and experimentation. The challenge framework establishes the means and ability to regularly engage and leverage nontraditional and small businesses, as well as university business incubators, to address anticipated and emerging threats in order to accelerate the development of innovative solutions. These challenges are expected to be a series of events (1–2 per year) with topic areas that are expanded upon and which change based on needs and priorities.

15. SUBJECT TERMS
security, autonomy, technology challenge, robotics demonstration, industry challenge

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marshal Childers
Unclassified	Unclassified	Unclassified	UU	21	19b. TELEPHONE NUMBER (Include area code) 410-278-7996

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures

List of Tables

1. Introduction

The long-term goal of this effort is to inform and accelerate Army modernization through innovation discovery, demonstration, and experimentation. It will establish the means and ability to regularly engage and leverage nontraditional and small businesses, and university business incubators, to address anticipated and emerging threats in order to accelerate the development of innovative solutions. Our approach is to first conduct a technology challenge that brings industry and academia researchers together with US Army Combat Capabilities Development Command Army Research Laboratory researchers and government stakeholders to offer technology solutions to certain classes of problems and gain feedback on performance. This is expected to be a series of events (nominally 1–2 per year) with topic areas that are expanded upon and which change based on needs and priorities.

1.1 Value of the Industry Challenge

Value of holding the DEVCOM Army Research Laboratory Security Technology Challenge and potential follow-up efforts:

1) Supports modernization priorities and tech transition.
2) Engages industry and academia on problems and solutions relevant to Army.
3) Addresses stakeholder needs and creates a venue for user feedback and establishing capability goals.
4) Provides stakeholders the opportunity to evaluate new and emerging technologies in operationally relevant environments.
5) Provides a preview of possible collaboration opportunities between DEVCOM ARL researchers, stakeholders, and the participants from companies and universities.

1.2 Purpose of Report

The three phases used to establish the challenge are planning, preparation, and execution. The purpose of this report is to present the work and progress achieved during the planning phase. Planning took place between 1 January and 30 September 2021. The preparation phase is expected to begin 1 October 2021 and the execution of the challenge should take place mid-year 2022, and how this can be applied to future challenges at the Robotics Research Collaboration Campus (R2C2) at Graces Quarters, Middle River, Maryland.

2. Method

2.1 Necessary Elements

The elements that are necessary to be successful are based on the need for attaining the right information from proper sources. The following is a list of the elements required to plan, prepare, and conduct a successful challenge. This is an ongoing process and portions of the elements can, at times, be addressed in parallel.

1) **Requirements:** Identify the requirements and needs of stakeholders; obtain guidance to understand required capabilities and gaps; prioritize which needs will be addressed.

2) **Initial Challenge Design:** Develop an experimental design that takes into account the required capabilities and corresponding threats; take into account the site features and terrain to scope relevant challenges.

3) **Publicize Challenge:** Provide a request for information to the intended audience that describes the challenge and the details for participation; invite the submission of proposals for proposed technology solutions.

4) **Technology Selection:** Using criteria that emphasizes capability relevance, prioritize the proposals and select the maximum allowable given the constraints of budget, personnel, and site capacity. Selection is made by a panel that consists of the challenge architects, autonomy researchers, and stakeholders (as available and appropriate).

5) **Challenge Preparation:** Consists of two main activities – 1) Revise the initial challenge design as appropriate considering the pool of technologies represented by the selected proposals. Define the number of technologies that can be examined per day considering which technologies can be evaluated simultaneously and which should be separated by time and/or space to avoid competition and conflict between vendors. As required, consult the vendors to better understand the functionality and limits of their technologies; 2) address and communicate the logistics needs and requirements for site use and for participation by vendors and stakeholders; define and fund tasks that require support from partners and contractors; coordinate participation by users and others that can provide knowledgeable feedback; vendors sign non-disclosure agreements prior to the event.

6) **Challenge Execution:** Conduct the challenge according to the run schedule specified by the experimental design; apply a crawl (easy), walk (medium), run (difficult) approach to the challenge problems to foster meaningful data

collection and feedback; give as much accommodation to the vendors to perform as is reasonable given time and resource constraints.

7) **Documentation and Feedback:** Collate and assess performance observations and feedback; prepare and deliver reports to each vendor that summarize their participation and provide evaluations from users, autonomy researchers, and stakeholders.

2.2 Collaboration

To identify the requirements we consulted multiple stakeholders. Based on these interactions we formed the initial challenge design.

2.2.1 Army Stakeholders

To identify Army needs in the areas of security and protection, we consulted the Ignite Advancing Concepts Office, which introduced us to the Protection Branch of the Maneuver Support Capability Development and Integration Directorate (MSCDID). They pointed us to *Army Futures Command Concept for Protection* (AFC Pamphlet 71-20-7),[1] which we used to identify and confirm relevant challenge elements. We are continuing to discuss the challenge with this user community and attempting to secure participation from their users.

Futures and Concepts Center (FCC) Protection Required Capabilities (RC) that can be addressed in the DEVCOM ARL Security Technology Challenge and ideas for relevant challenge content for the current and future efforts:

- RC 3 "forces require the capability to augment Soldier performance and capacity to increase situational awareness"
  - Unmanned vehicles tasked to investigate areas/incidents to provide situational awareness
  - Automated area/perimeter security and initial contact with intruders
- RC 4 "forces require the capability to store and process large amounts of data from multiple sources, analyze, aid in decision making, reduce cognitive load of commanders and leaders, determine threat intent, develop friendly courses of action"
  - Processing to present the information from multiple agents, across timeframes to increase awareness and aid decision making
- RC 5 "forces require the capability to conduct, synchronize, and analyze ISR activities to identify, characterize, and deny all domain threats, obstacles, and hazards"

- Unmanned Ground Vehicle (UGV), Unmanned Aerial System (UAS), and Unattended Ground Sensor (UGS) performing autonomous surveillance
- Cueing from unmanned assets to presence of threats and obstacles

- RC 8 "forces require the capability to provide protection of installations, Lines of Communication (LOC), the organic industrial base, depots, arsenals, munitions factories, and stockpiles through a synchronized Army and other government agencies"
  - Represent the facility at Graces Quarters as an asset that requires protection
  - Scenario experimentation on techniques to leverage robotics and autonomy for protection tasks and approaches

- RC 10 "requires installations to be resilient against disruption and attack with robust capabilities to prevent, protect, mitigate, respond to, and recover from all threats and hazards"
  - Early detection of threats and hazards with UGS and cameras
  - Automated intervention by team of unmanned air and ground vehicles

- RC 12 "forces require the capability to protect individual Soldiers, platforms, and equipment from enemy attack and against environmental hazards to preserve life, enable freedom of action"
  - Unmanned assets used to look ahead of troops
  - Unmanned vehicles tasked with making first entry into potentially dangerous situations (e.g., fatal funnel)

- RC 14 "forces require the capability to mitigate chemical, biological, radiological, nuclear (CBRN) contamination using multiple, scalable means that reduce the hazard; reduce manpower, time and resources;"
  - Experimentation with CBRN detector onboard unmanned vehicles

- RC 15 "forces require the capability to conduct police operations to protect critical capabilities, assets, and activities (CCAA), facilitate and preserve the rule of law, and deny irregular threats across the battlefield"
  - Unmanned systems providing persistent surveillance and patrols of an area
  - Tasking unmanned vehicles to investigate pedestrians and vehicles that enter area
  - Cueing of video and imagery of suspects and activity to operators

- RC 17 "forces require the capability to conduct police intelligence operations to synchronize information from multiple sources and to analyze

and disseminate a clear understanding of criminal and security threats to commanders across the battlefield"
    - Combinations and teams of unmanned vehicles, unattended sensors, and humans gathering data on activity within an area
    - Representation of fused data for situational awareness

- RC 18 "forces require the capability to conduct battlefield forensics and biometrics activities to authenticate friendly forces and identify intelligence to target threat actors, explosives, CBRN hazards, and cyberspace-crimes"
    - Automated Blue Force ID challenge and verification
    - Approaches for using unmanned systems to detect explosives and CBRN

- RC 40 "forces require the capability to employ CBRN Reconnaissance and Surveillance (R&S) that informs commanders at all echelons via integrated early warning which provides real time understanding of CBRN threats and hazards by means of deployable platforms and novel sensors dispersed throughout the battlefield"
    - Experimentation of scenarios with unmanned vehicle technology coupled with hazard detection capabilities

- RC 43 "forces require the capability to conduct civil reconnaissance of the operational environment to provide situational understanding to assist in decision making, set the conditions to interact with the local civilian population, identify critical threats"
    - Collaborate to identify tasks that might be addressed with the use of autonomous systems for reconnaissance
    - Use intelligence gathered from unmanned systems as an additional source of situational awareness data

2.2.2 Public Safety Stakeholders

To provide context and relevance for the local and regional public safety community, we held a public safety roundtable meeting at the DEVCOM ARL Graces Quarters Facility. We presented the challenge concept to a large group of attendees from local and regional law enforcement personnel, emergency responders, and representatives from the Maryland Governor's Office on Crime Prevention and the Department of Homeland Security Office of Strategy and Policy, Science and Technology Directorate. This exchange yielded several relevant operational scenarios from which we identified requirements for the present challenges and which will be useful as a basis for further collaboration.

2.2.3 Government Organizations

Based on the interactions with stakeholders and the author's experience in experimental design for robotics and autonomy technologies, we created the initial challenge design, which is described in detail in the next section of this report. We shared this initial design with our colleagues at DEVCOM ARL including the DEVCOM ARL Essential Research Program (ERP) Program Managers (PM)—specifically Emerging Overmatch Technologies (EOT) and Artificial Intelligence for Maneuver and Mobility (AIMM).

As this is our first attempt at organizing and conducting such a challenge, we rely upon the experience and proven success of others in government who have planned and conducted challenges and competitions in the past. We consulted Mr. Zeke Topolosky of the DEVCOM ARL Strategic Partnerships Office who introduced us to Mr Matt Goodyear (Demonstration PM for the Office of Under Secretary of Defense for Research and Engineering [OUSD R&E]). We presented our challenge plans to Mr Goodyear who confirmed the relevance of the effort and offered to introduce us to Penn State researchers who have provided support for preparing and conducting the numerous OUSD Thunderstorm events. We hosted three researchers from the Applied Research Laboratory of Penn State at the DEVCOM ARL Graces Quarters Facility. During this exchange of presentations and detailed discussions about the activities surrounding past events, DEVCOM ARL was able to get a good picture of the logistics, preparation, and conduct required to hold a successful event. Furthermore, the Penn State researchers were generous with their knowledge and offered to provide any documentation and guidance that we would find useful. The authors were invited to participate in an upcoming Thunderstorm event that is focused on technologies for operations in contested environments. This will provide DEVCOM ARL with firsthand knowledge on the conduct of a large-scale technology demonstration and evaluation with multiple vendors and technologies.

3. Design of the Challenge

3.1 Site Features

The DEVCOM ARL R2C2 facility at Graces Quarters Facility in Middle River, Maryland offers terrain and infrastructure that represents an ideal setting for evaluating technologies related to security and protection from threats that are relevant to the Army and public safety stakeholders. It provides a proving ground for research and development of autonomy, robotics, and artificial intelligence. Figure 1 shows the Mounted Operations on Urban Terrain (MOUT) features, the

rich, vegetated terrain that changes with seasons, and the onsite maintenance and repair facilities.

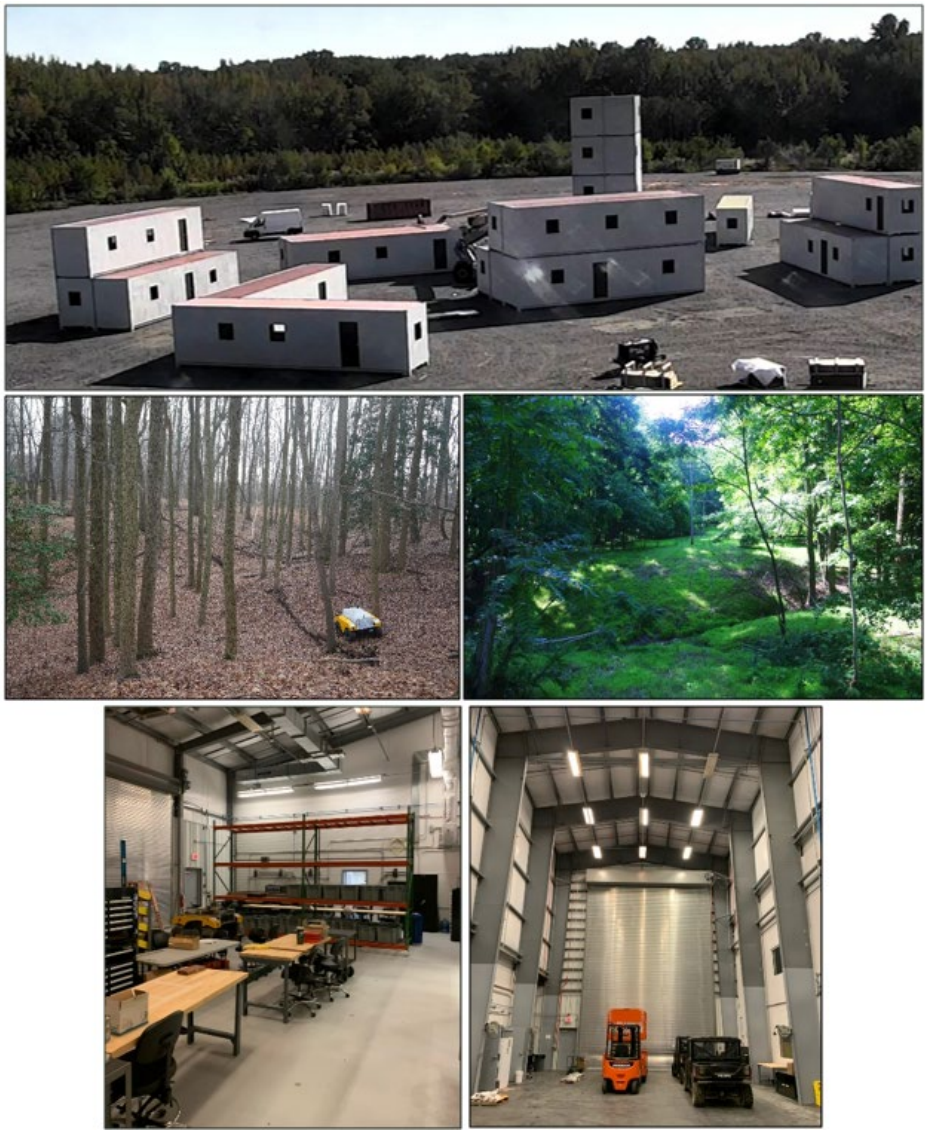

Fig. 1 Robotics Research Collaboration Campus

3.2 Challenge Scope

Upon considering the breadth of required capabilities that are applicable across stakeholder needs, we opted to shape this first challenge to present fundamental threats that have many implications and opportunities for application of technology. These also offer the opportunity for companies of all sizes and maturity to offer solutions to part or multiple parts of the scenarios.

The primary sources of threats are pedestrians and vehicles that enter the area of operations in each of three scenarios. The scenarios consist of site infrastructure protection at the MOUT area, inner perimeter security along improved routes, and outer perimeter security in unstructured environments. The derived relevant capabilities emphasized across these scenarios are maneuver with purpose, persistent security, and information for shared situational awareness.

For each scenario we consider two main thrusts that on the whole facilitate the application of the easy, medium, difficult paradigm. Thrust 1 concerns autonomous mobility capabilities to ensure that the systems and technologies can operate in the relevant and challenging environments of the R2C2 facility. Thrust 2 stresses autonomy for security capabilities by presenting security breaches of various degree and the need to detect, report, and respond. Figure 2 shows the operating areas and possible routes that are available (availability of certain routes is dependent on seasonal maintenance such as mowing and clearing).

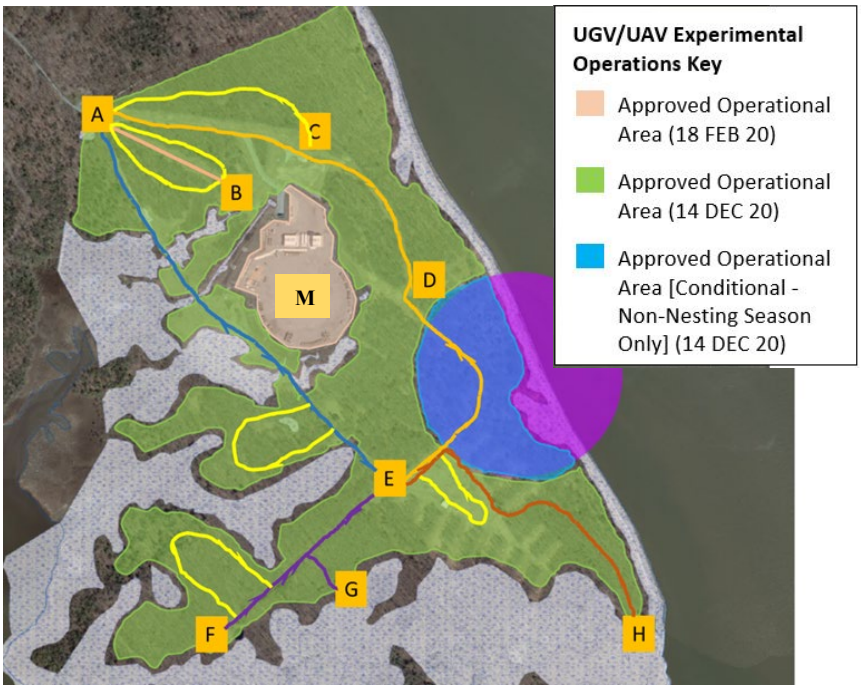

Fig. 2 Possible operating areas and routes

In consideration of the terrain complexity at the various locations within the operating area with respect to autonomous mobility thrust and the challenges to perception in this environment for the autonomy for security thrust, we estimated degrees of difficulty for each thrust. Table 1 provides estimated difficulty for specific routes between the labeled areas and mobility in the vicinity of Area M, which represents the MOUT feature and surrounding gravel pad. Response area

indicates the requirement for technology to maneuver to a designated area when directed.

Table 1 Autonomous mobility thrust degrees of difficulty

Area	Difficulty
Area M	Easy
Routes A-E, A-B, A-C, I-D	Medium
Routes C-D, D-E	Difficult
Response Areas	**Difficulty**
Area M	Easy
I, A, C	Medium
D	Difficult

Table 2 provides estimated difficulty for the designated areas and routes when technology is required to detect, report, and respond to activity therein.

Table 2 Autonomy for security thrust degrees of difficulty

Area	Difficulty
Area M	Easy
Areas I, A, C	Medium
Area D	Difficult
Area along route C-D	Difficult

3.3 Challenge Scenarios

The details of challenges for each thrust are presented in the form of the following scenarios. For the Autonomous Mobility thrust, the three main scenarios are patrol a pre-determined route, maneuver to and within an area when cued, and execute modified routes based on user input. Metrics and estimated levels of difficulty for these scenarios are provided in Table 3.

Table 3 Autonomous mobility thrust scenarios with metrics and estimated levels of difficulty

A. Patrol a predetermined route (maneuver to support perimeter security, area security)

Metrics: % on track, coverage per minute, # operator interventions

Maneuver	Difficulty
X to Y	w/map Easy; w/waypoints Medium
X-Y-X continuous	w/map Medium; w/waypoints Difficult
Continuous long-term	Difficult

B. Maneuver to activity within an area (cue from operator or sensor)

Metrics: time to arrival, accuracy

Maneuver	Difficulty
To designated area	Single robot Easy; Team Difficult
Patrol in/near area	Medium
Return to base/rally point	Medium

C. Permit pre-mission route modifications

Metric: time from plan request to start

Planning	Difficulty
Sub-portion of pre-defined route	Easy
Custom route definable by non-expert	Medium

The Autonomy for Security thrust has three main scenarios: activity detection, identification of foreign agents, and response measures. Metrics and estimated levels of difficulty for these scenarios are provided in Table 4.

Table 4 Autonomy for security thrust scenarios with metrics and estimated levels of difficulty

A. Activity detection

Metrics: true positive, false positive, false negative

Behavior	Difficulty
Scan area for activity	Easy
Detect moving agents/vehicles	Medium
Report detected activity (operator configurable)	(Images) Medium, (location/trajectory) Difficult

B. Identification of foreign agents

Metric: Classification rate

Agent	Difficulty
Moving pedestrian	Medium
Moving vehicle	Medium

C. Response measures

Metric: Time in vicinity

Behavior	Difficulty
Follow pedestrian	Difficult
Approach pedestrian/vehicle	Medium
Contain/head-off pedestrian	Difficult

3.4 Initial Security Challenge Design

Using the selected areas of operation, the determined scope and specified scenarios, there is enough information to publish the request for information for participation in the challenge. The design of the challenge will not be finalized until the pool of participating technologies is known and the functionality of each technology is understood.

4. Conclusion

4.1 Summary of Plans and Progress

DEVCOM ARL is supporting the Army's Modernization Priorities and accelerating technology discovery through the development of a technology challenge. This event will bring industry and academia researchers together with DEVCOM ARL researchers and government stakeholders to offer technology solutions to certain classes of problems and gain feedback on performance. The first challenge addresses required capabilities in security and protection and will lay the groundwork for subsequent, periodic challenges in other subject areas that

are relevant to the Army. In this first phase of the process we collaborated with stakeholders to identify required capabilities and consulted other government experts with experience in conducting technology challenges to create an initial challenge design.

4.2 Way Forward

The preparation phase will consist of securing funding and attaining necessary support for the logistics of participation by vendors and stakeholders; publishing the request for participation, selection of the participating vendors, and interaction with the vendors for finalizing the challenge design. The final, execution phase will consist of conducting the challenge, documenting and evaluating results, and providing feedback to the participants.

5. References

1. AFC Pamphlet 71-20-7. Army Futures Command concept for maneuver in multi-domain operations 2028. Army Futures Command; 2020 July 7.

List of Symbols, Abbreviations, and Acronyms

AIMM	Artificial Intelligence for Maneuver and Mobility
AFC	Army Futures Command
ARL	Army Research Laboratory
CBRN	Chemical, Biological, Radiological, Nuclear
CCAA	Critical Capabilities, Assets, and Activities
DEVCOM	US Army Combat Capabilities Development Command
EOT	Emerging Overmatch Technologies
ERP	Essential Research Program
FCC	Futures and Concepts Center
LOC	Lines of Communication
MOUT	Military Operations on Urbanized Terrain
MS CDID	Maneuver Support Capability Development Integration Directorate
OUSD R&E	Office of Under Secretary of Defense for Research and Engineering
PM	Program Manager
RC	Required Capability
R2C2	Robotics Research Collaboration Campus
UAS	Unmanned Aerial System
UGS	Unattended Ground Sensor
UGV	Unmanned Ground Vehicle

1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
1 (PDF)	DEVCOM ARL FCDD RLD DCI TECH LIB
12 (PDF)	DEVCOM ARL FCDD RLC B PIEKARSKI J FOSSACECA C BEDELL FCDD RLC I B MACCALL M CHILDERS A HURWITZ J WESTRICH K SCHAEFER-LAY FCDD RLC V M KWEON FCDD RLH FD A MARATHE FCDD RLL DA F THOMPSON FCDD RLW C D LYON
5 (PDF)	ENERGETICS TECHNOLOGY CENTER J MILLEMACI T LUCIUS R KAVETSKY C NIETUBICZ J MICHEL