APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

OPERATIONALIZING EMERGING HARDWARE FOR AI APPLICATIONS: RECOMMENDATIONS FOR ESTABLISHING A DEFENSE APPLICATIONS CENTER

Version: 2022-09-28

Lead Author: William C Regli, UMD/ARLIS
regli@umd.edu

Contributors: David J Coombs, UMD/ARLIS

Read: "Here is why ARLIS should be the first DAC"

DISTRIBUTION RESTRICTED

Executive Summary

This report recommends establishing a flexible and adaptable Defense Applications Center (DAC). The Center will provide a shared resource in which the U.S. government (USG) and its designated performers can engage in active experimentation on how best to integrate advanced computing hardware with application needs from the Department of Defense (DoD) and the Intelligence Community (IC). The DAC would create, maintain, and sustain an operational capability for rapid testing and evaluation of advanced hardware and software solutions in the context of operational and defense-relevant problems.

The DAC would benefit from features that facilitate collaboration and work in a multi-level security environment. The DAC should be housed in a large TS/SCI-qualified Sensitive Compartmented Information Facility (SCIF) equipped with a conference facility as well as a variety of office hoteling space and laboratory workrooms that can be dedicated to the DAC. In addition to the physical spaces, the DAC should provide support for the transfer and stewardship of technical datasets required for experimentation. This includes the proper handling of classified data at a variety of levels, the creation of challenge (or proxy) problems from this data, and the capture of experimental design, concepts, processes, and results. As such, the DAC will become a shared scientific instrument for investigating the application of new hardware and software paradigms for autonomy and Artificial Intelligence (AI) and their insertion into operational use by the U.S. military and Intelligence Community.

Background

This report articulates and expands on one of the recommendations of companion report "OPERATIONALIZING EMERGING HARDWARE FOR AI APPLICATIONS: A SURVEY OF TRANSITION OPPORTUNITIES AND DATASETS".

That report summarizes the findings from an ongoing effort to document the computational workloads associated with applications from the Defense and Intelligence Communities that could benefit from hardware acceleration. In conducting the survey, the team worked to identify properties of the datasets being used, the nature of the queries being executed, and the computational pipeline associated with the execution of these queries. One of the recommendations is to establish an Applications Center to aid in transitioning candidate solutions to the defense and intelligence communities.

Testbeds and Experimentation will be key to supporting this need. Organizations would likely require extensive experimentation and evaluation before they could adopt even the most compelling hardware technologies and integrate them into operational use. Surveyed organizations lack such experimentation capacity. The team concluded that there may be a government-wide need for testing and experimentation support to enable potential users to explore new hardware technologies and make acquisition and engineering decisions.

Such an Applications Center would provide Testbeds that enable experimentation and the ability to evaluate tradeoffs. This would make it feasible for organizations to explore promising hardware technologies to realize revolutionary potential gains in meeting their mission-critical demands.

Key Considerations

Key technical and procedural considerations for establishing a successful DAC include characteristics of the host organization.

- The DAC host should be able to perform work as a trusted agent of the USG with a broad scope of core competencies relevant to the DAC.
- The DAC host should demonstrate exemplary past performance in a variety of test and evaluation (T&E) roles for the USG, and the investigator team should be well-qualified for the DAC. Past performance supporting testbed development, verification and validation, and integration should span many of the technical areas of expected operational relevance for the DAC.
- The DAC host's location and facilities should be within an hour's drive of most of the Intelligence Community and numerous DoD laboratories and integration centers in order to facilitate its effective and widespread use for testing emerging solutions.
- The DAC host should have transparent and responsive services for managing issues including security clearances, access controls, and collaboration agreements. Drawing on the host's extensive expertise in these areas, the DAC host should offer the quality of council and service needed across the wide variety of potential DAC projects.
- The DAC host should have an elastic and flexible approach to teaming and resourcing. With access to the full scope of the host institution and the broader host partner enterprise, the DAC team should be able to quickly pull together the right project-specific combination of faculty, student, and professional subject matter experts (SMEs) (informed by specific customer and project needs) to inform the design and execution of independent test and evaluation tasks.
- The DAC host would ideally provide unique access to technology end users from the IC and their mission sets, and thus a unique ability to connect innovative technologies to potential USG end users.
- Access to the full breadth and depth of computational resources at the host institution's disposal should be extended to DAC users.
- The DAC host should maintain flexible contracting mechanisms that will naturally support targeted task orders for each program/experiment supported.

Recommendations

The capacity to frame and provide a flexible Defense Application Center (DAC) is key to the recommended approach, adaptable to the needs of stakeholders and long-term transition efforts. The DAC will be a shared resource in which the USG and its designated performers can engage in active experimentation on how best to integrate candidate hardware and software solutions with application needs from the DoD and the Intelligence Community (IC). In doing so, the DAC promises to create, maintain, and sustain an operational capability for rapid testing and evaluation of advanced hardware and software solutions in the context of operational and defense-relevant problems.

Physical and compute infrastructure

The DAC primary objective is enabling collaborative research engagements between defense transition partners, government organizations, advanced hardware and software solutions, and other relevant science and technology organizations. Fundamental to enabling collaboration is the provision of infrastructure, to include facilities and personnel, upon which the collaboration can take place. A shared workspace for the test and evaluation of program-generated technologies against real world DoD and IC challenges requires a secure collaborative environment capable of hosting experiments driven by classified schema and storing outputs using often-classified operationally relevant data.

The DAC should be housed in dedicated office and laboratory space within a TS/SCI-qualified SCIF, with ample offices and a collaborative experimentation room to support visiting performer teams and on-site teams performing independent T&E of candidate technologies. This Center should provide hoteling and enable collaboration among stakeholder groups, all in a secure environment.

Managing legal agreements enabling teaming

To allow work in the secure DAC facility by outside groups, legal agreements establishing SCIF co-use authorization, memoranda of agreement and intellectual property agreements between parties, *etc*., must be generated and signed for each participating organization. The DAC needs the necessary expertise to do so. A designated DAC Agreement Coordinator should oversee the process to ensure agreements needed to create contractual relationships between collaborating parties are in place prior to teams arriving at the DAC.

Compute infrastructure and collaboration platform

The DAC or its host should procure both dedicated compute and core data storage infrastructure, both established on an isolated TS/SCI network within the DAC physical space. The DAC will need hardware configuration and a collaborative platform. Core data storage infrastructure should be provided, *e.g.,* object-storage capabilities software, to support researcher development and dataset access.

The platform will support process, tools, measurement, and evaluation for design, simulation, and emulation, tailored to the needs of each effort. As the platform evolves, the DAC will mirror the tools onto the classified implementation of the platform.

Security Infrastructure and Processes

The DAC should provide security services to all users of the Center and other partners at the sponsor's request. The Center should offer transparent and responsive services critical to facilitating collaborative hosting in the DAC, including the quality of council and service needed across the wide variety of potential DAC projects.

Clearances and Access

The DAC host should have infrastructure in place to manage security clearances, as will be critical in supporting a mass of performers and evaluators to be hosted at the DAC. With task order level DD-254s from sponsors in hand, DAC security staff will be enabled to create and hold security clearances for researchers and personnel from industry and academia, as required. To maintain SCIF accreditation, the DAC host should have formal processes in place to define and enforce access controls, ensuring that authenticated users can access the information they "need to know" (NTK).

The DAC Coordinator for Personnel Security will have primary responsibility for clearance processing/passing; visitor requests; maintaining any necessary insider threat, Operational Security (OPSEC), and security awareness programs; and managing the security support/access control staff.

System Assessment & Authorization (formerly Certification & Accreditation)

The Assessment & Authorization (A&A) processes for operating new hardware or networks in a SCIF can be onerous. The DAC should establish processes to allow for the assessment and authorization of new classified infrastructure in relatively short order. Steps within the A&A process include the development and submission of a System Security Plan and other accreditation paperwork (per applicable Risk Management Framework parameters) to the government authorizer, performing initial testing and assessment of system controls to demonstrate system performance as necessary, and developing and implementing an effective system Continuous Monitoring (CONMON) strategy.

A DAC Accreditation and Compliance Coordinator, an Information System Security Officer (ISSO) should: clear hardware and network systems for SCIF use; write and maintain security documentation; and implement and manage life-cycle technology and security activities including acquisition/software security, compliance reporting, audits, inventory, and secure disposal/destruction/sanitization of media, equipment, and information.

Data and Information Handling

The DAC team should provide support for the transfer and stewardship of technical datasets required for experimentation by candidate technology partners, providing technology teams access to government-held information as available and warranted. This includes the proper handling of classified data at a variety of levels along with the creation of data-informed challenge problems. In this way, the DAC would become a shared scientific instrument for investigating the application of new hardware and software paradigms for autonomy and A.I. and their insertion into operational use by the U.S. military and IC.

The DAC should operate under an overarching DD254 attached to an appropriate contract, *e.g.,* an Indefinite Delivery Indefinite Quantity (IDIQ) contract. The DAC should provide services for managing data, information, and computation at Unclassified, Secret, and TS/SCI levels, as appropriate. The Center should adhere to security guidelines specified in NIST publication SP 800-171 *Protecting Unclassified Information in Nonfederal Information Systems and Organizations* for unclassified infrastructure, and to the applicable approved System Security

Plan and associated security artifacts for classified systems and infrastructure. Processes should be available for the receipt of data, either digitally or by courier, and their storage in accordance with the regulations of the DSS National Industrial Security Program Operating Manual (NISPOM) and applicable Intelligence Community Directives (ICDs).

Facilitating Experiments in the Defense Applications Center

The DAC should be designed to support experimentation and evaluation to facilitate integrating emerging technologies into defense systems. Doing so will require an appropriately configured and flexible testbed with usable interfaces, defined performance objectives, and a robust coordination and resource allocation system.

Most DAC technology integration efforts should likely begin in an unclassified collaborative environment, allowing teams to maximize the number and diversity of contributing researchers and candidate solutions. Following promising early integration results and given a clear rationale for additional integration and testing in a classified environment, designated experiments should then transition.

The Center Coordinator (CC) should lead DAC activity coordination, interfacing with customers and overseeing space management, resource utilization, and scheduling. For a designated experiment, the CC should serve as the liaison between DAC and stakeholder program management, USG transition customers, and the relevant technology solution team. The CC should identify data infrastructure requirements, information security requirements, and stewardship requirements. The CC should clarify and capture stakeholder baselines and offered metrics, determine how the DAC can best support that experiment to achieve program goals, and use those findings to inform DAC resource scheduling and allocation. The role of the CC is a critical component of ensuring the transition of ideas coming into the DAC and for the creation of a long-term repository of approaches, experiments, and metrics to accelerate innovation for future users.

The DAC should provide hoteling for two primary user types: Integration Teams (ITs) and Assessment Teams (ATs). Integration Teams would be working to integrate advanced technologies with DoD and IC application needs. Independent Assessment Teams would be conducting test and evaluation of the technologies developed by Integration Teams. The ATs should have their own coordinator. The CC should remain the focal point to coordinate a hosting schedule to ensure all groups nominated to work in the DAC would be afforded adequate space, time, and compute resources to get the job done.

DAC Testbed Engineers (TEs) should construct and maintain the DAC testbed and oversee technical implementation of embedding advances technologies in scenarios, prototypes, or evaluation pilots as part of a testbed. Following testbed network accreditation, TE engagements are envisioned to last weeks-to-months for each experiment coming into the DAC. Depending on the workload, complexity, and amount of parallelism in the design of experiments populating the DAC, it is expected that the DAC should provide a pool of research engineers who can perform the role of TEs, matrixed across disciplines. Performance objectives for the testbed should be established in consultation with the DAC sponsor, and regularly assessed by the CC and TEs through central logging functions. If any failures are encountered, TEs should work closely with the testbed platform developer to replicate and fix the issue on the unclassified instantiation before mirroring software updates to the classified testbed. TEs and the DAC would then continue to monitor logs to ensure issue resolution.

Composing Assessment Teams

The DAC should design agile processes to compose, assemble, manage, and eventually decommission an Assessment Team (AT) tailored to each project. Each AT may augment core members with subject matter experts (SMEs), from leading faculty and engineers to advanced students. Each AT should establish appropriate metrics and perform independent test and evaluation of advanced technologies and other evaluation tasks as determined by the government sponsors and stakeholders.

Each assessment task may vary in complexity, security requirements, and technical scope. The DAC should design a process to assemble outside experts to join each Assessment Teams (AT) as needed. These experts should focus on evaluating specialized or esoteric defense applications, *e.g.,* sensors (bio or otherwise), or domains outside the expertise of the core team.

The DAC should establish an Assessment Manager (AM). The AM should capture assessment needs, and compose, manage, and decommission an AT for each experiment. The AM should coordinate with USG sponsors and stakeholders to develop and maintain a schedule of evaluations and requirements. For each individual assessment task, AM activities should include managing the following:

- AT Scoping: The AM should work with sponsor and government customer(s) to capture support requirements; design evaluation goals, scope, and metrics; translate needs into challenge problems; develop experimental methodology (*i.e.*, type of AT needed and likely T&E construct), cost estimate, process model, and timeline; and gather and package the data sets and problem specifications for the evaluation task.
- AT Build: The AM should identify and recruit SMEs, investigators, and students to constitute the AT for the given task; ensure all AT members hold suitable clearances and need-to-know for the work required and are clear of any OCI concerns; oversee the provisioning of space, basic computational infrastructure, and data and document security requirements.
- AT Capture and Closeout: The AM should ensure reproducibility and lessons learned by capturing experiment processes and outcomes, including data; and capture final assessment materials and organize results in coordination USG sponsors.

The DAC should develop an AT approach that offers an agile methodology that can be customized to serve a variety of possible evaluation needs. Such needs may range from benchmark design and independent T&E execution to assisting teams without appropriate clearances to integrate their technologies with USG customer needs. Such an agile approach should enable the DAC to compose each AT from a broad resource pool with a minimal technical management core.

The DAC should design experiments to evaluate new technologies using government partner provided data when available. This should ensure that the technologies are hardened against real world DoD and IC implementation challenges. The AT should test technology designs against similar designs and baseline technology (*e.g.,* non-accelerated algorithms). The AT should consider concluding experiments with problems that are unsolved or underspecified with respect to data and existing performance benchmarks. Challenge problems should be initially based on open and unclassified data. These data sets should be provided free of cost to each project's research performers and USG partners.

The DAC should design agile approaches to supporting experiments with USG classified data and information needed to test advanced technologies developed by uncleared teams. The AT process should develop partnerships and collaborations to potentially compose cleared integration teams. Potential partners include the US Naval Research Laboratory, National Institute of Standards and Technology, National Intelligence University and other DoD and DoE facilities.

Data Repositories: Toward a Science of Applied Autonomy

The DAC could feed into a persistent learning environment able to accelerate discovery and innovation. Capturing experiments, reusing datasets, and developing transferable engineering principles will have a multiplying effect on the development of AI and autonomous technologies, for future uses, reproducibility, and verification of results. Repositories of experimental design, process data, reusable techniques and designs, research outcomes, and lessons learned could be created and maintained, and shared across DoD and IC transition partners.

Key elements could be captured and stored in the classified repository:

- Requirements: Goals as defined by the sponsor and transition agents as well as those defined by the performers and technical community, through a combination of customer problem ingest and direct guidance.
- Experiment design: Specification and capture of the experimental hypothesis, metrics and measurement fabric, and assessment methodology.
- Data configuration and management: Capture of the hardware/software configuration, versions and operating systems, libraries, as well as state of experimental data, its provenance, and management requirements.
- Post-experiment data stewardship: Define what to do with configuration information post-experiment; capture lessons learned; create a repository of reusable techniques and designs; provide for future uses, reproducibility, and verification of results.

Technology Transition

The DAC would be in a unique position to foster transfer of the know-how and approaches developed by the DAC and its users to critical programs across the national security landscape. In addition to the transition customers identified by the DAC user community, the DAC should work to identify other possible beneficiaries of the DAC's work from the IC and DoD communities. As allowed by program classification guidelines, the team could work with international partners, including the FVEY ("Five Eyes") intelligence community as well as NATO and other international partnerships, to create a transition clearing house for allied nations in our collective effort to adapt our military and intelligence communities to the application and use of AI and autonomy.

Results and Technology Transfer

The DAC should make no proprietary claims on intellectual property or systems developed by those working in the testbed during DAC research. Where appropriate, intellectual property generated by DAC host staff who are performers should be documented. Innovations from the DAC host team would include processes and methods for system test and evaluation. Such methods should be transitioned to the broader community, defense or public as appropriate, via publications and reports.

Conclusions and Summary Recommendations

This report recommends establishing a flexible and adaptable Defense Applications Center (DAC) to provide a shared resource in which the U.S. government (USG) and its designated performers can engage in active experimentation on how best to integrate advanced computing hardware with application needs from the Department of Defense (DoD) and the Intelligence Community (IC). The DAC would create, maintain, and sustain an operational capability to rapidly test and evaluate advanced hardware and software solutions to address operational and defense-relevant problems.

This recommendation articulates and expands on one of the recommendations of companion report "OPERATIONALIZING EMERGING HARDWARE FOR AI APPLICATIONS: A SURVEY OF TRANSITION OPPORTUNITIES AND DATASETS". That report found that organizations would likely require extensive experimentation and evaluation before they could adopt even the most compelling hardware technologies and integrate them into operational use. Yet there exists no such experimentation capacity. One of the recommendations is to establish an Applications Center to aid in transitioning candidate solutions to the defense and intelligence communities. Such an Applications Center would provide Testbeds that enable experimentation and the ability to evaluate tradeoffs. This would make it feasible for organizations to explore promising hardware technologies to realize revolutionary potential gains in meeting their mission-critical demands.

The recommended DAC would benefit from features that facilitate collaboration and work in a multi-level security environment. The DAC should be housed in a large TS/SCI-qualified Sensitive Compartmented Information Facility (SCIF) equipped with a conference facility as well as a variety of office hoteling space and laboratory workrooms that can be dedicated to the DAC. In addition to the physical spaces, the DAC should provide support for the transfer and stewardship of technical datasets required for experimentation. This includes the proper handling of classified data at a variety of levels, the creation of challenge (or proxy) problems from this data, and the capture of experimental design, concepts, processes, and results. As such, the DAC will become a shared scientific instrument for investigating the application of new hardware and software paradigms for autonomy and Artificial Intelligence (AI) and their insertion into operational use by the U.S. military and Intelligence Community.