Carthage

A collaboration toolkit for cyberspace operators

Report Number: 9517-21-0004-HI
Prepared for USCYBERCOM under contract: FA701419FA209
Version: 2.0
Date: October 30, 2021

This page intentionally left blank.

Foreword

Every day, United States Cyber Command (USCYBERCOM) faces logistical hurdles working with systems and teams across our domain of responsibility. General Nakasone has written that "(m)ilitaries succeed when they embrace new technologies aimed at planning for the next war, not fighting the last one." In order to be an effective cyber force, we need powerful tooling that lets our staff build and manage systems with the speed, fluidity, and rigor of a global technology firm. The appropriate tools exist, and are available within private sector organizations. But they are foreign to the Federal space.

Units across USCYBERCOM continually seek effective mechanisms to access the systems they are defending, deploy diagnostic tools on affected networks, and share information with teammates. As long as these technical gaps remain, we will not keep pace in the Cyber Domain.

This document describes ***the solution to these technical gaps,*** *a DevSecOps product named Carthage, and its interoperability with an USAF-sponsored collaboration platform known as Advanced Collaboration Enterprise Services (ACES). HAF/A2Q developed ACES with the modern operations center and cyber domain in mind. ACES, Carthage, and their integration are now TRL 9 and have successfully undergone numerous structured evaluations.*

This paper describes the capabilities of ACES and Carthage, and explains how the two capabilities can serve cyber operators as a turnkey solution for professional systems management and collaboration.

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

BLUF

Carthage is a USAF-funded, Army-fielded cyber toolkit that gives operators the ability to rapidly and accurately deploy very large, complex infrastructure. Operators can use these environments for mission-specific requirements to replicate specific systems or embody specific TTPs. Carthage includes a built-in collaboration capability to provide non-colocated teams a shared real-time interface for cyber operations. It has successfully supported cyber training and operations for US Army, Air Force, Marine Corps customers. It should be adopted by USCYBERCOM and widely deployed to all cyber operators.

Executive Summary

The National Security Agency (NSA/CSS) and USCYBERCOM operate in cyberspace, both in defense of the Department of Defense Information Networks (DoDIN) and to counter our adversaries in gray and red cyberspace in support of national objectives. To that end, USCYBERCOM needs state-of-the-art, effective, efficient, and scalable cyber operations platforms and systems to achieve American superiority in cyberspace. Commanders need real-time and complete information to make informed, timely, and tactically-sound decisions, and operators at all levels must be able to seamlessly collaborate across both physical distance and network boundaries. Our systems managers' need modern DevSecOps, infrastructure-as-code services that will let them build, test, and deploy services with precision. Our offensive and defensive cyber forces need ready access to all of their tools in both their training and live environments, with the ability to share tools and targets with joint and coalition partners across geographical distance.

Such a capability was already developed by USAF's ISR Innovations (HAF/A2Q) in 2014, and it has recently been deployed operationally. We believe it is now ready for use within USCYBERCOM.

The capability has two components: Advanced Collaboration Enterprise Services (ACES), a HAF/A2Q program designed to improve information synthesis and situational awareness within operations centers; and Carthage, an USAF-funded DevSecOps system developed by the same systems integrator that developed ACES. In 2019, this team—a group of engineers who, individually, possess operational cyber as well as global Internet infrastructure management experience—integrated Carthage with ACES.

The results bring the cyber infrastructure management capabilities of a rigorous global technology firm to DoD's cyber teams, with special accommodations for large, distributed teams. This capability has since been deployed to the 91st Cyber Brigade and 960th Cyberspace Wing. It is ready to be deployed throughout USCYBERCOM as an Infrastructure-as-Code platform for remotely managing DoD mission systems, as well as for collaboratively planning and conducting offensive and defensive missions.

Current USCYBERCOM Challenges and Requirements

USCYBERCOM, like any military organization, is deeply hierarchical, with multiple layers of command and control (C2). In addition to its own chain, it must coordinate cyberspace operations with NSA, navigating an overlapping set of Title 10 and Title 50 authorities; coordinate defensive cyberspace operations (DCO) with several other USG agencies, some of which are outside the DoD; and work across the Intelligence Community (IC) in its offensive cyberspace operations (OCO) and signals intelligence (SIGINT) missions. This complexity is not necessarily a weakness and is expected for any combatant command. But to perform this work successfully, USCYBERCOM requires tools that allow staff and operators to communicate with these other stakeholders, and reach inside of the remote systems they are tasked with defending and/or exploiting. Such a systems environment is commonplace within private sector teams with similar (but often less critical) missions. But it remains out of reach for those protecting the nation's most critical military systems.

Key requirements for this capability are made clear by the Commander of USCYBERCOM's responsibilities in JP 3-12:

> *To establish and share comprehensive situational awareness of red and gray cyberspace, developing threats and anomalies.*
> ***JP 3-12 Chapter 3(e)(4,7)***
>
> *To coordinate with the IC, CCMDs, CO-IPE, Services, DOD agencies and activities, and multinational partners to facilitate development of improved cyberspace accesses to support planning and operations.*
> ***JP 3-12 Chapter 3(e)(5)***
>
> *To effectively integrate systems, networks, services, and EMS usage to ensure compliance with DOD-mandated DODIN configuration standards.*
> ***JP 3-12 Chapter 3(e)(7)***
>
> *To conduct operational planning, directing, coordinating, deconflicting, executing, and overseeing missions nationally and internationally across all CCMDs.*
> ***JP 3-12 Chapter 3(e)(9-13)***

We currently lack the technical ability to do these things effectively. Cyber units across *USCYBERCOM* find themselves without effective mechanisms for accessing the systems

they are defending, deploying basic diagnostic tools to affected networks, or sharing information with teammates. Our offensive teams, lacking a capable range environment for rigorously testing their weapons on adversary targets, are sometimes forced to do so on our own live infrastructure. The collaboration tools available to these teams come full of logistical hurdles to effective communication, making them insufficient for a domain in which adversary actions happen constantly and at lightspeed. As long as this technical gaps remain, we will never have superiority in cyberspace.

The status quo toolkit for DoD cyber training is dwarfed by the import of the mission. Left: Best Cyber Ranger competition, 2018. Right: Cyber Shield, 2018.

ACES Overview

ACES was developed by HAF/A2Q to provide the low-friction collaboration sought across many CCMDs: truly seamless, many-to-many collaboration and situational awareness to every screen, in every application, at any scale: single-user workstations, conference rooms, theater-scale operations centers, and mobile devices held by on-the-ground operators. ACES allows images, documents, videos, and arbitrary application windows to be moved and/or replicated seamlessly between any number of output devices and shared by any number of simultaneous users across devices, locations, and networks. It can securely integrate all systems, even legacy systems, and virtualize them to permit secure maintenance and defense activities, even across classification.

ACES is based on Debian Linux and was designed primarily with open source tools and open standards. It runs on commodity hardware and can support just about any existing network device and display.

ACES has been described by DoD as an "anytime solution": quickly deployable to meet 70% of a need, and easily tailored to meet remaining needs through an iterative development process. As an enterprise system, it is surprisingly lightweight. Its status as a Small Business Innovation Research (SBIR) Phase III product makes it easy to move forward quickly.

Carthage Overview

An effective cyber team should be able to rapidly provision enterprise-scale infrastructure, and manage that infrastructure as code. Carthage provides this capability. Carthage users deploy, attack, compromise, destroy, and redeploy full enterprise systems multiple times per day in a safe and isolated environment, allowing for continuous integration of both offensive and defensive tools and systems. Using an automated approach to building military and civilian cyber infrastructure, Carthage

quickly deploys fully populated and configured network ecosystems (including routing/firewalls, PKI/Active Directory, global network routing, and enterprise and tactical applications) with high accuracy and consistency. Carthage completely eliminates the concept of a "cyber range"; instead, complete infrastructure can be built and tested using a continuous deployment model, and used for live infrastructure just as it is for range-style training and testing.

This capability is based on modern DevSecOps tools and processes, ensuring all actions are tracked, reproducible, and revertible in a domain- and environment-agnostic way. It deploys fully functional environments to any cloud or on-premises network with a handful of commands or clicks. All components are stored by Carthage in industry-standard Git repositories, allowing complete auditability and reproducibility.

Some specific aspects of Carthage's approach bring unique value to USCYBERCOM's mission:

- *An open development environment for virtualizing mission systems.* Any system can be virtualized and integrated into an Carthage-based network environment. This lets Carthage users train and test tools in an environment that is an exact replica of the real-world system they are seeking to protect or attack. The development environment for these virtualizations uses an open API, so USCYBERCOM operators would be able to virtualize and configure these systems themselves instead of relying on a contractor. Carthage source code is available as an open source software project.
- *Support for large-scale orchestration.* The dominant orchestration tools (e.g., Ansible, Chef, Puppet, Salt, etc.) are good for creating and managing collections of hosts, but quickly become complex and fragile when used to manage large-scale architectures. For example, while each task in an Ansible playbook may be declarative and idempotent, the overall effect of running a collection of plays becomes highly iterative and time-consuming at scale. Carthage, by contrast, is designed to specify entire network ecosystems in a declarative fashion.
- *Support for legacy systems and architectures.* Tools like Kubernetes and Harbor have been developed with large enterprises in mind. But most of these systems were designed for microservice and container architectures. Carthage supports such architectures, but can also precisely emulate existing hardware-based systems just as well. This lets an enterprise smoothly manage its transition from

legacy systems to full infrastructure-as-code environments, or safely decide to remain a hybrid.

- *Automated dependency injection.* Other orchestration tools (such as Terraform or vRealize Automation) generally require explicit specification of every detail of the desired system, making configuration tedious for a large environment. Carthage allows the user to specify only the attributes of the system that they care about; after that, Carthage intuits the rest based on known properties of the system or the hosting environment. For example, if you ask Carthage to generate an Ubuntu-based environment that is isolated from the Internet, it will automatically download an Ubuntu update server and make it available in the environment, because it knows this is an implied requirement. This is true for Kali, Red Hat, or whatever other environments might be desired.

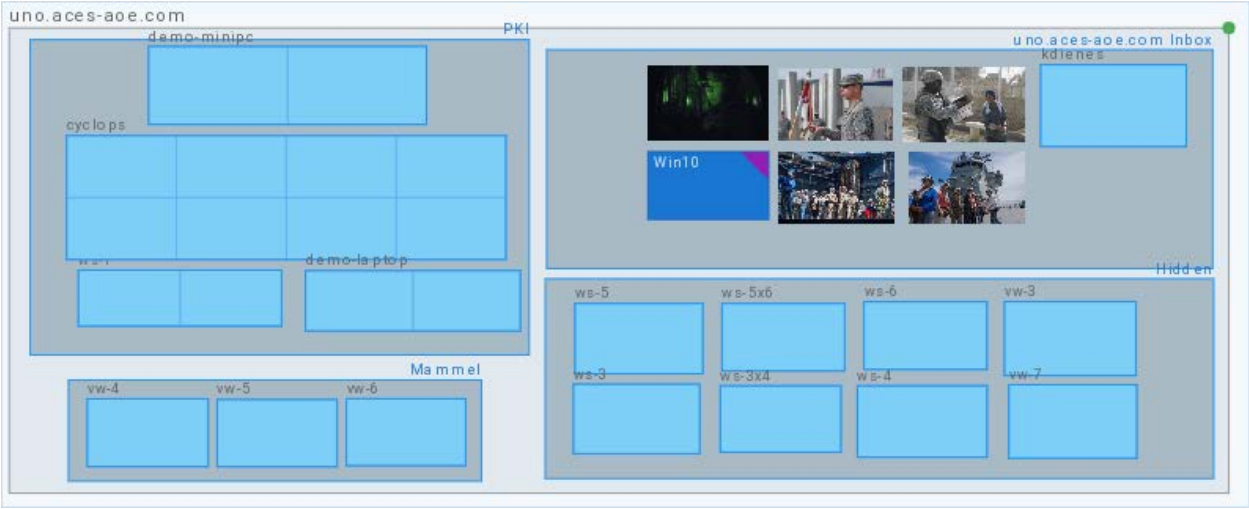
Cyber collaboration with Carthage and ACES

When responding to a cyber incident, the entire response force is seldom collocated: the network team at the entity being attacked—another DoD agency, a deployed unit, etc.—may be far from the *USCYBERCOM* team assigned to support it, which itself may be distributed across multiple on-premises and telework sites. The organizations have network permissions regimes that often do not play well together: it is not unusual for a senior security engineer to provide command line instructions over the phone to a less-skilled user with greater access rights. The responding team itself may be working over multiple networks at different classifications. Likewise, in the OCO realm, teams often work together across various Joint Mission Operations Centers (JMOCs) and various T10 and T50 infrastructures. Due to these challenges, in addition to strong DevSecOps tools for managing systems, we also need a secure yet low-friction means of communicating within teams and with other organizations.

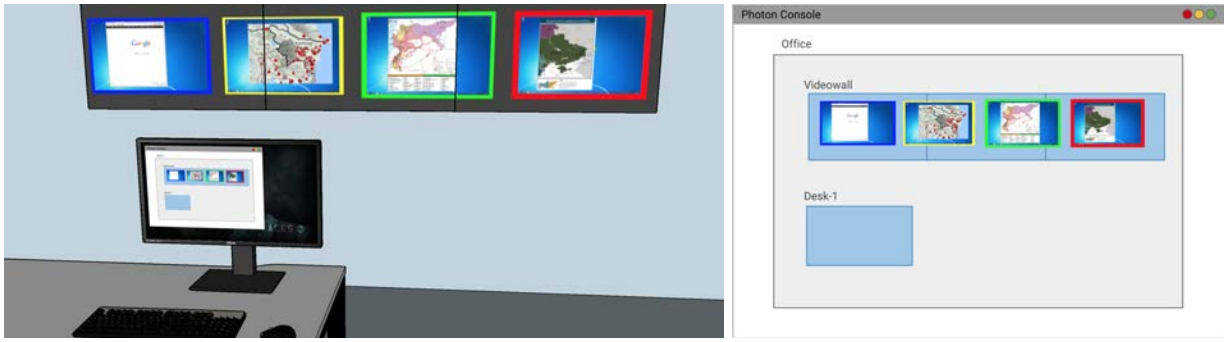
HAF/A2Q's original requirement for ACES was an immersive "I see what you see, and you see what I see" experience across desktops and devices, allowing the many workstations and video walls within an Air Operations Center to seamlessly share information with each other and with deployed teams.

Using ACES, any user on any device can share the contents of their screen in real time with any number of other users and devices. Permissions can be adjusted to allow any user, or a subset of users, to send keyboard and mouse inputs to any other device in the ACES network.

The user interface for this collaboration experience is simple. Content on ACES-powered displays is coordinated via a web console that depicts your enterprise's displays as they appear in real life. By clicking and dragging on the console, windows on any display can be moved around the display and to other displays; resized; duplicated; and destroyed. Administrators can create custom views that automatically revert a display environment to a standard layout, so that a team's preferred tools and views can be automatically loaded, sized, and placed in the right location on a video wall or desktop. These views can span any number of displays from one to several dozen.



An ACES console for a smaller video wall configuration, blank and ready to organize content. Light-blue rectangles represent individual displays. Conjoined displays represent video walls.



Example 1: A small ACES installation and associated JMOC console interface.

Platform flexibility. ACES powers video walls as well as physical and virtual workstations. Any window currently displayed on a workstation can be duplicated and displayed on any video wall alongside a common operating picture (COP) for all to see (a wall-based window can be duplicated to a user's desktop display as well). As the user updates the window from their own workstation, the duplicate on the video wall updates in real time. ACES-powered video walls run on commodity TVs and mini PCs, and can be assembled in about as long as it takes to mount the TVs and connect the mini PCs to the network.

ACES can seamlessly integrate visual content from any screen using hardware or software video capture. This enables computers and other devices to be shared within the operating environment without being an explicit part of the system's design. While software video capture enables integration of network-connected devices (through a web browser), hardware video devices capture live video over HDMI. This does not require the source to be connected to the system network in any way. This allows a team to safely view the contents of external devices that could introduce malware to a trusted network. ACES is designed to be flexible, so that it can integrate with many third party cross-domain solutions (CDS).

Network performance. Another A2Q requirement for ACES was performance over disadvantaged networks. Many commercial collaboration solutions assume their users will be using reliable broadband connections; the moment the signal degrades, the collaboration experience collapses; NSAnet Skype users know this well. But tactical environments work under inherently unreliable network conditions, and any real-time collaboration tool must degrade gracefully as network latency increases. Entanglement, the synchronization engine that keeps ACES sites connected and working in tandem, ensures operational resilience over disadvantaged networks through efficient bandwidth management.

System concept & design. Many collaboration products assume a world in which users only collaborate at pre-designated times, and with a concrete list of collaborators. ACES is always on. Rather than asking users to reserve a seat and schedule an appointment for a VTC or screen-sharing session, ACES systems are built from the bottom-up to communicate seamlessly with one another.

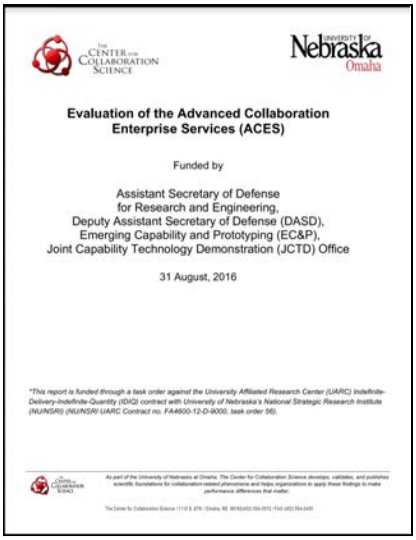
Users & Reviews

ACES and Carthage have been used by thousands of cyber personnel, giving USCYBERCOM a glimpse into how the product would perform for our teams:

- ACES is currently deployed operationally at the 513th Air Control Group, Tinker AFB (POC: Capt. Caleb Wanzer, DSN: 884-7171, caleb.wanzer@us.af.mil). The 513th is currently working with the ACES team to prototype an airborne ACES system for the E-3 Sentry AWACS platform.

- ACES and Carthage are deployed together as a primary DevSecOps platform being used to train National Guard and Reserves Cyber forces. This integration has been used by numerous cyber security warfighters to conduct national level training exercises. It is deployed to ShadowNet, a cyber defense training cloud managed by the 91st Cyber Brigade. In 2020, Carthage supported Cyber Yankee, Wooly Knit, Cyber Shield, and the 960th Cyberspace Wing's annual training. Operators with the 960th submitted written feedback stating Carthage was "great," "fantastic," "super helpful," and "amazing." Further Carthage development is currently being requested by the 960th CW where the capability is being used to develop cyber defensive tools (POC: MSgt. Tyler Watkins, Cyber Training Manager, DCO, tyler.watkins.4@us.af.mil, 210-925-6555).

- ACES was recently installed at three locations of particular interest to cyber stakeholders: AFLCMC's Kessel Run Experimentation Lab in Boston; Air Combat Command's experimental operations center at Joint Base Langley-Eustis; and Fort Belvoir's Defensive Cyberspace Operations "Forge" development center.


The Center for Collaboration Science
University of Nebraska Omaha

Evaluation of the Advanced Collaboration Enterprise Services (ACES)

Funded by

Assistant Secretary of Defense
for Research and Engineering,
Deputy Assistant Secretary of Defense (DASD),
Emerging Capability and Prototyping (EC&P),
Joint Capability Technology Demonstration (JCTD) Office

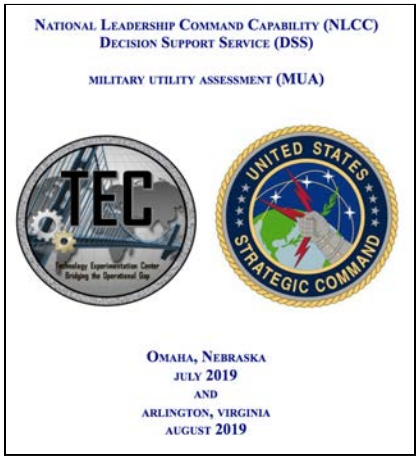
31 August, 2016

This report is funded through a task order against the University Affiliated Research Center (UARC) Indefinite-Delivery-Indefinite-Quantity (IDIQ) contract with University of Nebraska's National Strategic Research Institute (NUNSRI) (NUNSRI UARC Contract no. FA4600-12-D-9000, task order 56).

- In 2016, a USSTRATCOM-sponsored test of ACES was conducted at the University of Nebraska-Omaha (UNO). It has been used at various scales to support live exercises for JSOC and USSTRATCOM. The results of these and other Photon test cases (primarily scenarios in which a team of analysts was asked to collaborate on tasks and attain convergent situational awareness) were gathered by UNO into a report ("Evaluation of the Advanced Collaboration Enterprise Services (ACES)", August 31, 2016). Users in this study were overwhelmingly positive about ACES's capabilities, calling them "unprecedented" and "superb."

The ease and utility of ACES is perhaps best illustrated by an incident on the morning of a 2016 JSOC exercise: as plans were being coordinated across sites prior to exercise kick-off, various event support systems, ACES included, were being configured and participants were receiving training in their operation. Soon after ACES was made available to the remote participants, they began using it to collaborate on the exercise setup process itself in advance of the actual test, having received mere minutes of training. In the words of one evaluator: "I have never seen a capability like this. We literally solved a real issue in our room before the exercise even started. We completed that using the technology."

- In 2019, ACES was the subject of a Military Utility Assessment conducted by USSTRATCOM J81 (POC: Philip L. Hezeltine, Chief, Advanced Warfare Solutions Development Branch USSTRATCOM/J81, 402-912-8238, Philip.l.hezeltine.civ@mail.mil, Philip.l.hezeltine.civ@mail.smil.mil). "The overall assessment conclusion recommends USSTRATCOM use the ACES solution during a larger-scale, multi-day exercise to better validate its military utility for the Global Operations Center (GOC)."



Given the level of success ACES and Carthage have had with other cyber units, we believe deployment to USCYBERCOM is a low-risk action with high potential payoff. We recommend rapid adoption of ACES across the NSA/CSS and USCYBERCOM enterprise as part of an enterprise modernization strategy.

Vendor & Strategic Integrator

In early 2014, HAF/A2Q began working with Hadron Industries, Inc. (CAGE: 67NM8), a small business based in New Hampshire, as the lead developer and systems integrator of the ACES program. A2Q staff who worked with Hadron at the time have continued to engage Hadron through multiple reassignments, noting the advanced technical abilities and responsiveness of Hadron's engineers.

These engineers have experience as both uniformed cyber officers, and as key members of critical software projects such as iOS and Debian Linux. They know the

state of the art, and they also speak our language. This team is readily available for highly technical, engineering-focused discussions about the needs of USCYBERCOM. Please contact the authors of this white paper to facilitate such a discussion.