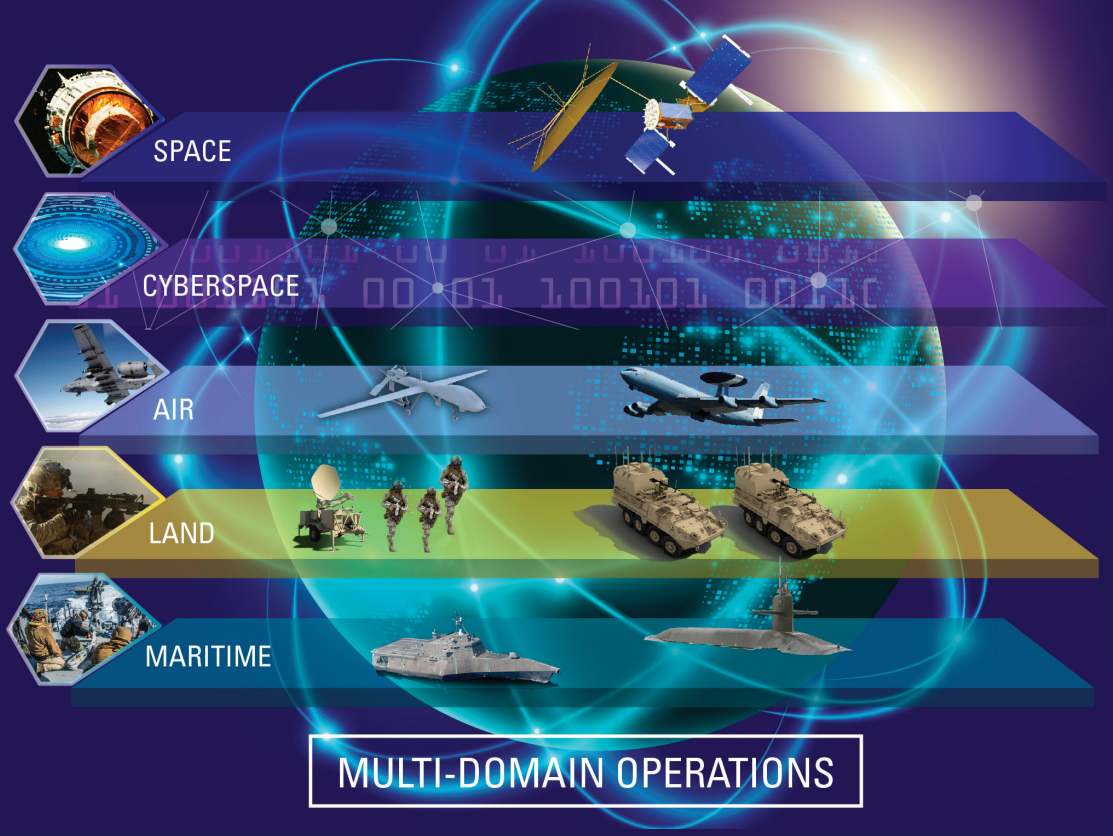
BREAKING DEFENSE / PATHFINDER

Cross Domain Solutions: Enabling All Domain Operations

Enabling the sharing of unclassified, Secret, and Top Secret mission critical data across warfighting domains and security boundaries at the tactical edge.

A BREAKING DEFENSE CUSTOM REPORT SPONSORED BY

GENERAL DYNAMICS Mission Systems



Defining the Multi-Domain Battle

SITREP

Preparing for future conflict with near peers is a key goal in the U.S. military's groundbreaking All Domain Operations (ADO) concept. ADO calls for all services to share data across multiple security domains in tactical vehicles, aircraft, vessels, and dismounted soldier systems, as well as cyber networks. Accomplishing this requires rapid and continuous integration of systems and networks to deter, compete, and prevail in conflicts short of actual armed hostility.

"In a new era of Great Power competition, our nation's adversaries seek to achieve their strategic aims, short of conflict, by the use of layered stand-off in the political, military and economic realms to separate the U.S. from our partners," wrote Army Gen. Stephen Townsend in a Training and Doctrine Command (TRADOC) report entitled, "The U.S. Army in Multi-Domain Operations, 2028."

"Should conflict come, they will employ multiple layers of stand-off in all domains—land, sea, air, space and cyberspace—to separate U.S. forces and our allies in time, space, and function in order to defeat us," wrote Townsend in 2018, when he was TRADOC commander (Townsend has subsequently been appointed commander of U.S. Africa Command).

One of the best ways to counter that challenge—and bind coalition partners more tightly together—is the use of cross domain solutions (CDS). CDS govern information sharing so the right data is shared with the right people at the right time. It is one of the key enabling technologies for Joint All-Domain Command and Control (JADC2), the architecture by which the Department of Defense (DoD) plans to instantly connect mission leaders with mission data, not just across the five warfighting domains—air, land, sea, space, and cyber—but also among multiple security domains such as unclassified, controlled unclassified (formerly known as "For Official Use Only"), secret, and top secret.

An example of a mature, upgradable CDS product that is helping U.S. military and its partners execute ADO today is the Tactical Cross Domain Solution (TACDS) from General Dynamics Missions Systems. The newest version of TACDS meets the security requirements to connect networks at different classification levels across warfighting domains for simultaneous, synchronized, and sequential operations.

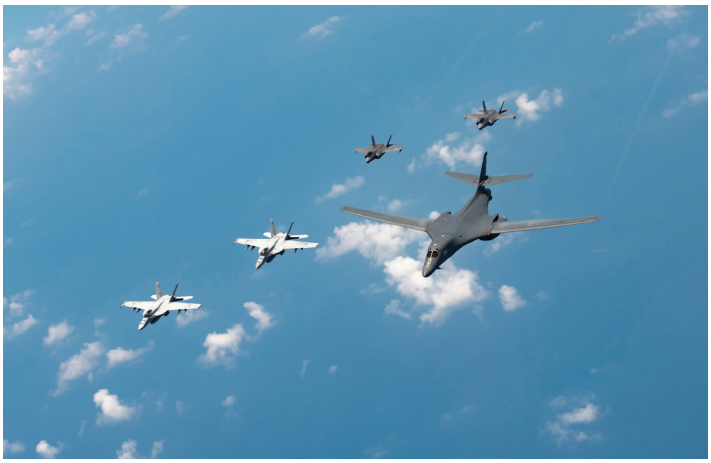
It's approved by the National Security Agency (NSA) and can securely share information such as high-definition full motion video (HD FMV), STANAG 4586, Variable message Format (VMF) and U.S. Message Text Format (USMTF) in harsh tactical conditions. TACDS is specifically designed to help the DoD transition to defend against more sophisticated threats.

– Barry Rosenberg, Contributing Editor
Technology & Special Projects

Fight and Work as a Coalition

Eliminating and replacing data/security silos with shared systems that let select data flow between domains, but which also have proper checks and controls, has been a DoD goal for years. The joint tactics, techniques, and procedures envisioned in ADO depend upon it, as do joint operations with allied nations. The U.S. and its partners depend upon significant cooperation ahead of operating jointly. All-domain coalition operations require a predetermined synergy versus a developing cooperation to stimulate a rapid response.

An illustration of why this is important is found in the F-35. Arguably the most important collaborative program in the world, the Lightning II includes eight international program partners—the U.S., United Kingdom, Italy, Netherlands, Australia, Norway, Denmark and Canada—and six Foreign Military Sales customers so far who are buying and operating the F-35—Israel, Japan, South Korea, Poland, Belgium and Singapore.



F/A-18 Super Hornets, F-35 Lightning IIs, and a B-1B Lancer conduct a large-scale joint and bilateral integration training exercise above the Indo-Pacific, Aug.18. 2020. Photo By: Air Force Staff Sgt. Peter Reft

When the American F-35s train together—the Air Force's F-35A conventional takeoff and landing variant, the Marine Corps' F-35B short takeoff/vertical landing variant, and the Navy's F-35C carrier variant—they are able to train via secure channels. The right CDS can facilitate the necessary data sharing amongst U.S. and its partners, allowing these forces and other joint campaigns to train as they fight.

In the case of data sharing across security domains, these challenges can be met with hardware and software of CDS.

Defining Cross Domain Solutions

CDS uses a controlled interface to secure information sharing among entities (agencies, countries, networks) with different security levels. For users, it gives military personnel granular control over data passing between network segments and various classifications of security.

This is done through the DoD's Risk Management Framework that follows principles established by the National Institute of Standards and Technology (NIST) to govern information systems on which CDSs are typically deployed.

The focal point for DoD/government cross-domain capabilities and mission needs is the NSA's National Cross Domain Strategy & Management Office (NCDSMO), which governs requirements and testing for CDSs manufactured by all commercial companies.

NCDSMO is responsible for developing the "Raise the Bar" (RTB) protocols for improving CDS from a design, development, assessment, implementation, use, and security perspective. To have products certified, CDS manufacturers must meet RTB requirements in areas like system architecture, software development, management, and monitoring systems.

RTB is specifically targeted at improving the cybersecurity and addressing emerging threats of all CDS equipment used to protect U.S. government classified information and data integrity. It focuses particularly on preventing cyberattacks against or through the CDS system. RTB controls are designed to catch errors made by software developers that can be exploited by adversaries.

Applications for CDS

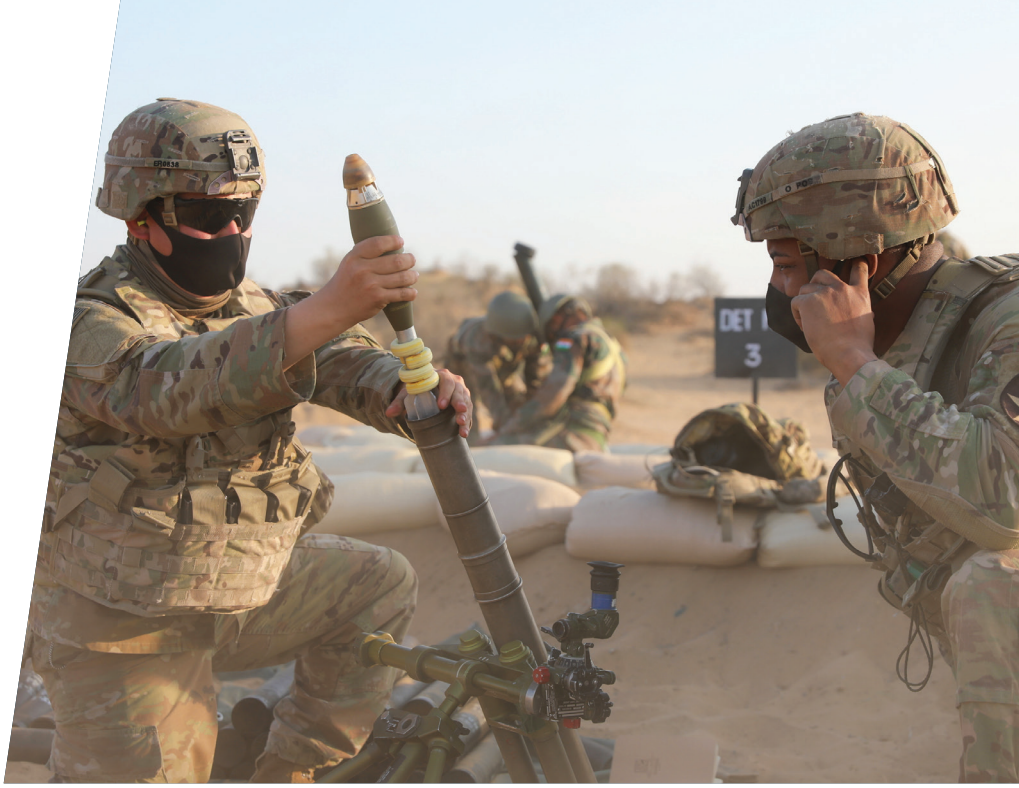
CDS typically support a wide variety of tactical deployments and systems. General Dynamics Mission Systems' TACDS can process numerous tactical data and message formats to provide instant, secure access to real-time information for warfighters in today's tactical environment. With broad capabilities, TACDS is specifically designed for diverse applications on the modern battlefield, such as:

Situational Awareness (SA) and Command & Control (C2): Exchanging SA/C2 data (position/location information [PLI], Link 16) in real-time across security domains and between combatants and commanders; medical evacuation (MEDEVAC).

Real-Time Condition Based Maintenance: Vehicle health and status monitoring; remote maintenance and vehicle diagnostics; fuel and ammunition level monitoring.

Real-Time ISR Data Collection & Dissemination: Unmanned aerial system video; unmanned ground sensors; remote sensor video; "Every Soldier as a Sensor"; and vehicle-mounted and soldier-carried cameras.

Unmanned Vehicle Control: Protecting classified data and preventing spills of targeting information, ISR data, air reconnaissance request/task form; text-based sensor cueing messages.



Coalition Interoperability: Compliance with standards and protocols for the use of command, control, communications, and computers (C4) in dismounted soldier systems; real-time SA and C2; ISR video collaboration.

Mature, Upgradeable CDS System

Getting to a state of true ADO with a capable force by 2028 and a ready force by 2035 is an aggressive timeframe that requires DoD to employ mature, upgradable CDS products.

The General Dynamics Mission Systems-built TACDS is just such a product. It enables digital messages and information such as FMV to be shared and transmitted across different security domains in austere tactical environments out to the edge.

FMV, for example, is a critical filter component that'll become increasingly more necessary to achieve ADO. Having multiple streams of HD FMV provides a huge advantage to the warfighter.

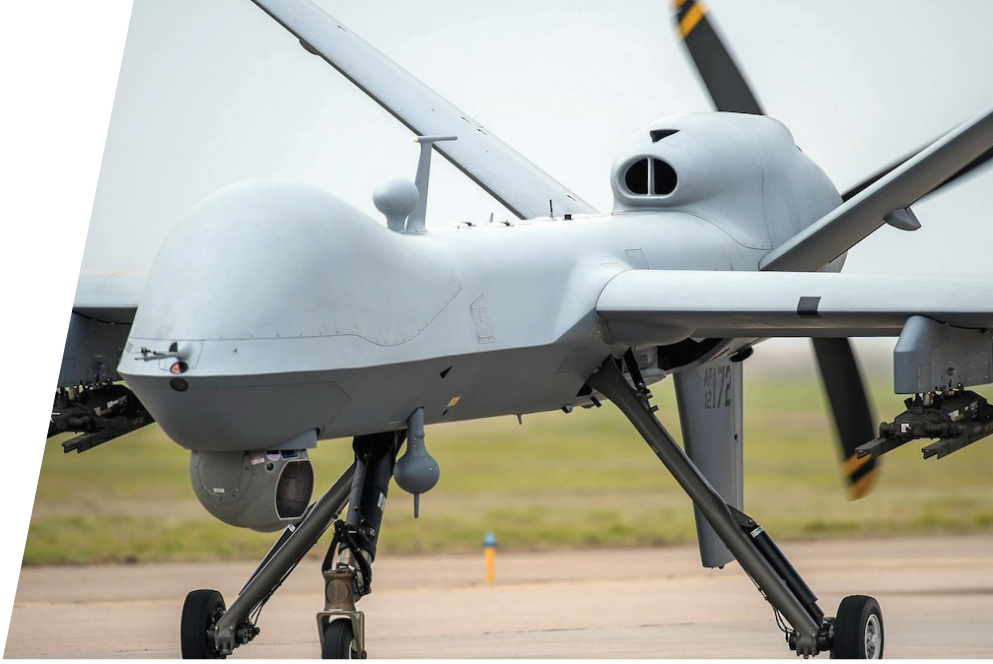
Certified by the NSA in 2012 and currently in use in ground vehicles, mobile shelters, ground sensor systems, ships, aircraft, and unmanned aerial systems, TACDS is a low SWaP-C, rugged, tamper-resistant CDS that comes in two form factors: TACDS-Vehicle Mount (VM) and TACDS-Low Profile (LP), both offering the flexibility and configurability needed to support a variety of missions.

The newest TACDS product is in use by the Army's Capability Set 21 (CS21) testing/deployment program. A major component of CS21 is the Integrated Tactical Network (ITN). This approach injects new commercial components and network transport capabilities into the Army's tactical network environment, providing maneuver brigades and below with smaller, lighter, faster, and more flexible communications systems. This mix of commercial capabilities integrated with programs of record systems offers resilient communications as part of a command's primary, alternate, contingency, and emergency communications plan.

The approved ITN components for CS21 include tactical CDS—including TACDS, as well as single-channel commercial radios with advanced networking waveforms, high-capacity line-of-sight radios, voice and data gateways, small aperture satellite terminals, expeditionary servers, variable height antennas (via a quadcopter drone), and 4G commercial technology.

TACDS is also being installed on the U.S. Air Force's new combat search and rescue helicopter, the HH-60W "Jolly Green II". MEDEVAC is one of the important maintenance and support applications for CDS, and the HH-60W is a namesake of the Vietnam War-era HH-3E Jolly Green Giant that flew hundreds of search and rescue missions in Southeast Asia. The HH-60W specification drives more capable defensive systems, vulnerability reduction, weapons, cybersecurity, expanded adverse weather sensor capabilities, and more comprehensive net-centric requirements. The Air Force plans to buy 113 HH-60W helicopters.

As TACDS meets the security requirements to connect networks at different classification levels across varying domains, it is an ideal solution for DoD and the Intelligence Community. The system completed its Lab Based Security Assessment (LBSA), a government assessment for verification of vendor claims, and was assessed to meet RTB requirements by the NCDSMO in October of 2019.



Special Forces need real-time surveillance and full-motion video that requires an information interchange at different classifications between them and surveillance platforms such an Army MQ-9 Reaper.

Case Studies for CDS

The 2018 National Defense Strategy specifically notes the importance of operations across both physical warfare and classification domains of data security.

"Some competitors and adversaries seek to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends (e.g., information warfare, ambiguous or denied proxy operations, and subversion)," the strategy states. "These trends, if unaddressed, will challenge our ability to deter aggression."

The fabled Chinese military strategist Sun Tzu wrote, "the supreme art of war is to subdue the enemy without fighting." The following examples show how the U.S. and its allies can utilize CDS to help protect against adversaries.

Maintenance and Support

A rotorcraft mission system operates at a high-security classification level to provide aviators with the situational awareness data they need to safely conduct missions. That includes health usage and monitoring system (HUMS) data that not only provides the crew with real-time status of critical systems on the high side of security but also valuable data that maintenance personnel can use for predictive maintenance on the low side.

That can only happen, however, if the data that the maintainers and logistics analysts need for an active, predictive maintenance program is downgraded for use in unclassified systems. That lets the data be brought directly into the hangar on rugged laptops and accessed by the technicians.

CDS makes it possible for technicians and analysts holding different levels of security clearance than the operators of the aircraft itself to access vital data that improves operational performance for both rotorcraft and fixed-wing fleets while reducing costs for military operators.

Special Forces

Special Operations Forces tend to operate at a high-level security classification, including operations in austere, edge environments. They are prodigious consumers of FMV and real-time surveillance, which necessitates an information interchange at different classifications between special forces and surveillance platforms such an Army MQ-9 Reaper.

While Special Forces operate at a high classification level, the unmanned aerial systems they work with may not be operating at that same level. CDS systems make it possible to take data and information from a lower level and transfer it to the higher level for special operations forces to consume. CDS can accomplish that footwork in real time so that special operators don't have to wait for the data to be sent back to enterprise military networks, reclassified to a higher enclave, and then sent back to them. Eliminating that time delay means that FMV, for example, can be immediately actionable.

Real-Time Video

Sharing live video among all levels of a combat force is a force multiplier. TACDS, with its support for FMV, mitigates security concerns for its effective and cyber secure distribution of video at the forward edge of the battlefield. Sensors and other ISR assets can be remotely controlled and accessed in real-time while maintaining a strong cyber defense against the introduction of malware or zero day attacks. This results in more timely assessment of intelligence to affect the outcome of an engagement or more secure force protection posture for a perimeter.

CDS govern information sharing to connect mission leaders with mission data across air, land, sea, space and cyber.

Situational Awareness

Ground forces, in particular, rely on GPS-enabled Blue Force Tracking for essential data on the positioning of friendly forces. ADO will be dependent on that and on the ability to share position location information between different forces that are operating in the same area.

Today, the ability to exchange data from, say, a national secret network to a secret releasable network may involve redaction of certain information. Maybe you don't want to expose where your elite fighting forces are or reveal certain information about the capabilities of your aerial platforms. On the other hand, there's value in exposing other elements of your fighting force to partner forces.

A CDS bridges the gap between the national secret network and any coalition network, enabling decision makers to lead diverse forces and also have the ability to turn sharing on and off automatically.

The Takeaway

TACDS provides a low SWaP-C, purpose-built CDS to solve mission needs at the tactical edge. General Dynamics Mission Systems continually invests in TACDS to ensure alignment with NCDSMO mandates and provide peace of mind to customers that their investment in TACDS will keep their mission going for years to come. The company's team of experts can help design rulesets for your filters, install TACDS in your labs, train to self-administer TACDS, and provide support for your Site Based Security Assessment mandated by NCDSMO.

For more information, contact TACDS@gd-ms.com, or visit www.GDMissionSystems.com.