Why All NATO Members Need to Support CESMO Data

Read About

- CESMO
- Electronic support measures
- Tactical data links
- TDL Gateways
- Link 16 communications
- Single/multi-sensor geolocation
- Situational awareness

CESMO Plays a Critical Role in NATO Electronic Warfare Operations

Knowing the precise location of threats and friendly forces is essential to increase warfighter survivability. Cooperative Electronic Support Measure Operations (CESMO) data gives NATO coalition forces this visibility.

CESMO is the digital protocol NATO adopted in Standardization Agreement (STANAG) 4658 and Allied Engineering Documentation Publication (AEDP) 13 to support Electronic Warfare (EW) and Electromagnetic Operations (EMO). It involves platforms equipped with sensors capable of detecting radio frequency (RF) emissions from all types of ground, air, and sea platforms — hostile and friendly. Friendly platforms in the area can use the protocol and information exchange network CESMO provides to exchange collected data within seconds, allowing a real-time position fix of these signal sources.

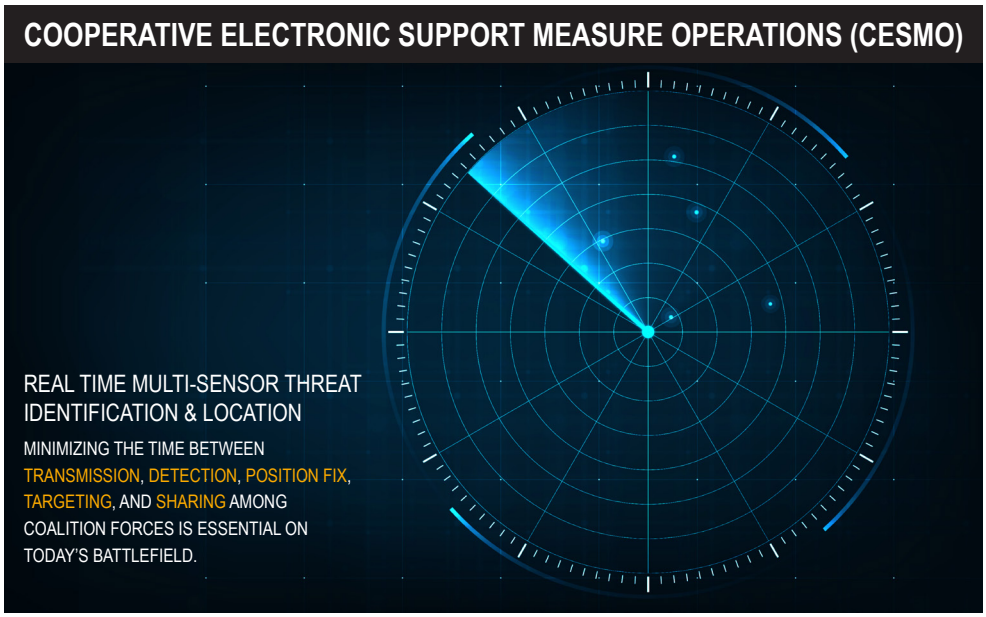

Figure 1: Cooperative Electronic Support Measure Operations (CESMO)

When CESMO is used on its own, all coalition forces on the CESMO network know exactly what types of threats they're facing and where they are. They also know the location of friendly forces they might not otherwise be aware of. When CESMO is used in combination with other tactical data link (TDL) types, this situational awareness is extended to the broader community of coalition forces and enhances time-sensitive targeting decisions.

In addition to improving tactical situational awareness and survivability, CESMO enables coalition forces to increase their exploitation of the electromagnetic spectrum by contributing to the Electronic Order of Battle (EOB) and NATO Joint Intelligence, Surveillance, and Reconnaissance (JISR). The CESMO data feed is also an integral part of Electronic Warfare Coordination Cells, and SIGINT and EW Operating Centers.

A Growing Number of NATO Member Countries Are Using CESMO

With the increasingly important role that CESMO plays in NATO electronic warfare and electromagnetic operations, the protocol is being continuously enhanced by NATO member countries. As a result, there's a growing community — including Germany, the United Kingdom, France, Spain, Italy, Norway, the Czech Republic, Greece, Turkey, and the Netherlands — already exchanging CESMO information. The protocol has been used in more than 20 trials and campaigns, most recently during Exercise Timber Express in Jagel, Germany.

As more NATO member countries recognize the value of CESMO communications, leading TDL solution providers are adding support for the protocol to their TDL solutions. However, developing solutions that support CESMO requires highly specialized knowledge and expertise that only a very limited number of solution vendors possess.

As NATO member countries evaluate CESMO solutions, they must ensure they understand the full value CESMO provides and how that value is enhanced and extended with an intelligent gateway that can translate between CESMO and other TDL types.

Fast, Coordinated Information Sharing Increases Survivability

Previously, surveillance aircraft flew over battlefields to capture RF signals to determine threat locations and types. Warfighters in the field received details about the threats, such as missile launchers and radar systems, in a spreadsheet, often hours or even days, after the signals were collected.

Since then, technology and tactical data networks have evolved considerably to offer new battlefield tactics. Today, adversaries rely on communications equipment and weapons that are smaller, more sophisticated, and more mobile than previous versions. As a result, threats are constantly moving and RF emissions often occur in very short bursts. To be effective on today's battlefield, the time between transmission, detection, position fix, and targeting must be shared among coalition forces in as near to real-time as possible.

While every NATO member country has its own threat detection and geolocation technologies, it is a challenge for a single country to gather enough information to put the complete picture together to cover large areas. Fast exchange of standardized information about emissions on the battlefield is the only way to resolve the challenge.

Many NATO members already use TDLs, such as Link 16, to securely share information across platforms and EW assets. However, many platforms and EW assets used in NATO ESM operations don't support Link 16 communications. Link 16 is simply too time-consuming, complex, and expensive to implement across all EW assets used by all NATO member countries.

CESMO is Designed for Widespread Adoption

In contrast to other data links, CESMO is IP-based and can be exchanged between coalition platforms using commonly available UHF/VHF radios. This is an easy criterion to meet. Even ground troops already carry radios that can send and receive encrypted data.

To encourage widespread adoption, the CESMO protocol is designed from the ground up for ease of integration, ease of use, low cost, and broad applicability across a wide range of electromagnetic operations.

+ CESMO procedures are developed in a way that ensures minimal disruption of the warfighters' normal mode of operation.
+ CESMO is able to operate on low-bandwidth, bearer-agnostic radio networks by employing the same variable message principles as the Variable Message Format (VMF) protocol to minimize message size.

+ CESMO is easy to implement on existing (in service) ground, air, and sea platform using existing radios in a peer-to-peer architecture.

Multi-Sensor Geolocation Increases Accuracy

Here's a very high-level look at the sequence of activities that occur from the time an RF emission is detected until the moment the CESMO Fusion and Coordination (CFC) operator shares details about the threat location and type:

+ The CFC operator periodically sends a "request list" to every CESMO Collector Asset (CCA) on the network containing emitters of interest on which to report when detected.
+ When a CCA detects an RF signal, it sends a message to the CFC indicating the identification, line of bearing, and parameters of the signal.
+ The CFC fuses the signal information, determines a location, and then shares that information with everyone on the CESMO network.
+ If a CCA detects a signal not "requested" by the CFC, the CCA can send the signal information to the CFC. The CFC may update the request list, if the signal is of interest.

Figure 2 illustrates the accuracy difference between single-sensor geolocation based on triangulation and the multi-sensor geolocation based on cross bearings that CESMO uses.

Sharing CESMO Information Enhances the Common Operating Picture

TDL gateways that translate CESMO information to the other TDL formats used by coalition forces such as Link 16, Link 11, Link 22, VMF, or Cursor-On-Target (CoT), dramatically improve situational awareness among mission participants.

Sharing CESMO information gives warfighters a consistent and cohesive view of threats and friendly forces, resulting in a more complete and accurate common operating picture (COP). This knowledge increases cooperative opportunities among coalition forces to make time-sensitive targeting decisions, and helps to avoid accidental targeting of friendly forces.

Without a cohesive COP, each participant has a different, and far smaller, window into the overall battlefield situation, increasing risks for all.

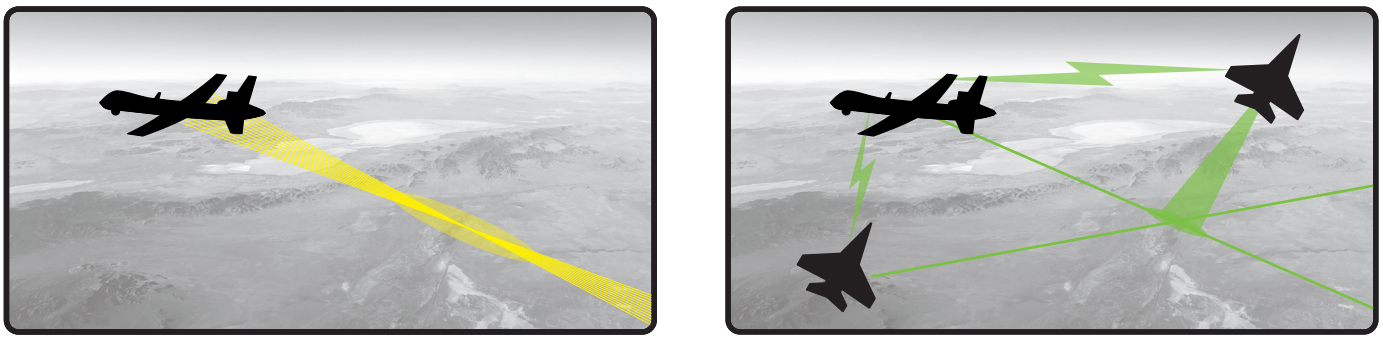

Figure 2: Single-Sensor Geolocation Versus Multi-Sensor Geolocation

TDL Gateways Must Bridge Networks in a Transparent Way

With its ability to almost instantly geolocate RF-emitting assets, the CESMO protocol can be used to detect a variety of EW threats, including:

+ Radar: geolocating surface-to-air missile sites
+ Navigational warfare: geolocating GPS jammers
+ Communications: geolocating VHF and UHF radio signals
+ Electro-optical and infrared (EO/IR): geolocating infrared target illuminators

Because Link 16 is also often used to enhance situational awareness in NATO missions, it's particularly important to share the CESMO information about these threats on the Link 16 network.

Figure 3 illustrates how CESMO and Link 16 can be used together to increase situational awareness. The platforms receiving both message types now have precise geolocation information from the CESMO network as well as EW product information, parameters, and land point or track information from the Link 16 network.

With the complexity involved in translating information to and from Link 16 networks, most legacy TDL gateways are correspondingly complex to connect, configure, and use.

Some gateways can take at least half a day to connect and configure, and require expert assistance from the gateway vendor to set up. Other gateways take the opposite approach and implement only certain aspects of the Link 16 standard. However, these partial implementations severely limit interoperability. For a cohesive COP, the gateway must provide full interoperability with Link 16 networks and devices.

All Complexity Must Be Hidden From Warfighters

To meet warfighters' needs on the battlefield, TDL gateways must be designed much like an appliance would be, hiding the complexity of TDLs and data translation behind the scenes.

The gateway must provide push-button startup so the system is operational within a few seconds and automatically connects to all TDL types. Radios must be automatically configured with no expert input. Even error messages must be easy to understand. This ease of use must carry through all aspects of TDL gateway operation

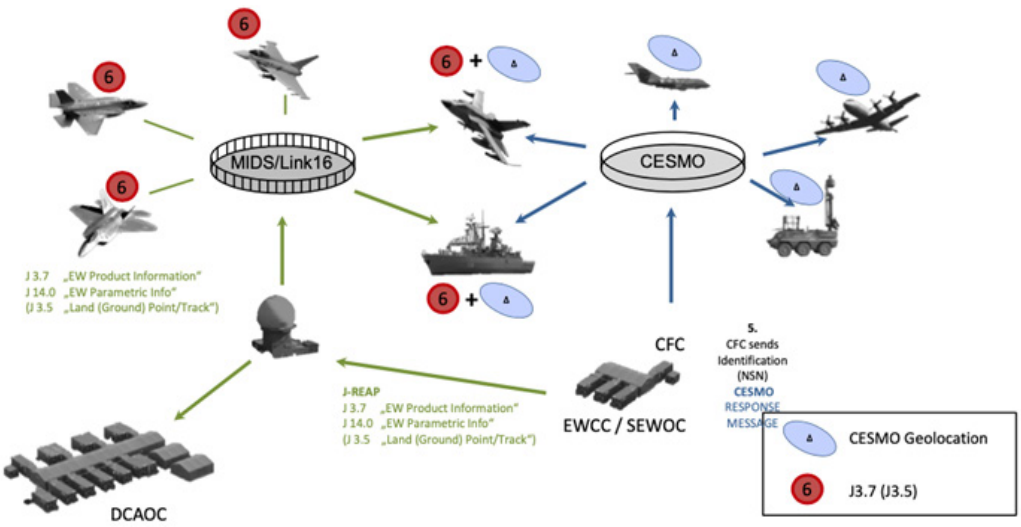

Figure 3: Bridging CESMO and Link 16 Networks to Improve Situational Awareness

to ensure warfighters can focus on mission tasks rather than the enabling technologies. The way data translations are presented to warfighters is extremely important. Warfighters don't care that communications equipment is sending a CESMO message to a device that communicates using Link 16. They care that the information exchange is successful, fast, and gives them the information they need in an easy-to-understand format.

To provide translated information that's easy for warfighters to understand, TDL gateways must translate the concepts being communicated rather than the individual words. These conceptual translations must be automated, supported across multiple TDL types, and provided in context. That means the TDL gateway must fuse information from all data links with previously received information and then send the appropriate information, in context, to the other TDLs.

Finally, TDL gateways must be provided in a form factor that is suitable for any location on the tactical edge of the battlefield. For example, a warfighter in the field should be able to run the software on a standard laptop or remotely operate it without a user interface; on an unmanned aerial vehicle (UAV) that can be put in an advantageous position in line-of-sight of the participants for an extended period.

CESMO and Link 16 EW Assets Can Be Connected Today

Thanks to close partnerships between leading industry and military organizations, user-friendly TDL gateways that translate between CESMO, Link 16, and other TDL types in a transparent way, are available today and are being used in real-world trials and exercises.

When CESMO information is translated and provided to EW systems on airborne platforms that use Link 16, those systems automatically display the details of the detected tracks including identity and positions of hostile and friendly forces the air crew did not know about. The crew can now quickly and precisely evade threats, make more informed decisions, and more effectively interoperate with coalition forces on the CESMO network. Similarly, warfighters from ground vehicles are also now aware of friendly and hostile threat positions they could not see or detect due to topography or other physical barriers.

Warfighters can see information that comes in on all communications networks so that all networks behave like one. The warfighter does not need to know that some of the assets and information may not be native to their employed data link.

Without the gateway, someone has to manually share the critical CESMO information with these warfighters, delaying the data, creating unnecessary distractions, and introducing the risk of errors on each end of the communications.

For more insight into a real-world example, read our case study Bringing Near Real-Time Threat Identification and Location Information to the Entire Coalition.

Curtiss-Wright is One of Only a Few CESMO Experts Globally

Every organization that needs to interoperate with NATO EW assets that communicate using CESMO must support the current protocol.

However, the CESMO standard is rapidly evolving making it very challenging for newcomers to build in-house expertise. In fact, much of the standard's evolution occurs during week-long events where participants discuss requirements and make the associated software updates on the spot. Unless organizations are involved in developing the standard, their knowledge will likely be out-of-date within just a few months.

Partnering with proven CESMO experts is the most efficient and effective way to access the specialized knowledge.

Curtiss-Wright is one of only a few CESMO experts globally. While the CESMO standard is written by NATO member countries and government agencies, Curtiss-Wright was asked to be an expert contributor to the standard. As a result, we are heavily involved in testing hypotheses and different aspects of the protocol to ensure they function as defined.

We were asked to take this role because we are widely recognized as a world-leading expert in TDLs.

Authors

Peter Ellis
Principal Engineer
Curtiss-Wright Defense Solutions

Steve Horsburgh
Director, Product Management
Curtiss-Wright Defense Solutions

René Raden
Captain, German Air Force
CESMO SME & Project Team Lead
NATO SEWWG

Marco Mehling
LtCol, German Air Force (retired)
Airbus Operational Requirements Manager

We Understand How to Share CESMO Information Across Networks

Curtiss-Wright's TCG HUNTR™ TDL Hub and Network Translator is an intelligent translation gateway for multiple TDLs, including CESMO, Link 16, VMF, CoT, GPS, Situational Awareness Data Link (SADL), and Joint Range Extension Applications Protocol (JREAP). It took years of extensive research and effort to develop, and it leverages over two decades of knowledge and expertise in TDL technologies and messages.

TCG HUNTR eliminates the many challenges associated with legacy TDL gateways. It is extremely fast and easy to set up and use at the tactical edge of the battlefield and other military environments with minimal personnel and training, and almost no expertise. This simplicity allows warfighters to communicate and access data in a natural and intuitive way across CESMO, Link 16, and other networks with no need for expert knowledge of the technologies or complexity behind the scenes. Every participant has instant access to critical information at their fingertips, that helps to increase survivability.

Through close partnerships that ensure TCG HUNTR meets the most urgent TDL translation requirements today and tomorrow, we continue to cement our role as the trusted, proven leader in defense and aerospace.

Learn More

Products

- TCG HUNTR - TDL Hub and Network Translator
- TCG BOSS - Battlefield Operations Support System
- TCG LinkPRO - Tactical Data Link Processing Software
- TCG GTS - Ground Tactical Data Link System

More Resources

- Tactical Data Link Translation Made Easy – What it takes to Get it Right
- Advanced Tactical Data Link Gateway for the Modern Warfighter
- 5 Fundamentals to Simplify TDL Translation