A Data Sharing Solution for a Coalition Common Operational Picture (CCOP)

National Information Exchange Model (NIEM)-based Approach to Coalition/Mission Partner Data Exchange

Lieutenant Colonel Karla J. Porch

U.S. Army

Joint Staff J-6

Mr. Frank W. Klucznik

Georgia Tech Research Institute (GTRI)

June 2016

Joint Staff J6, Deputy Directorate C5 Integration, Data and Services Division

1. Purpose.

This concept paper explains the need for a common approach to share Coalition Common Operational Picture (CCOP) information using the National Information Exchange Model (NIEM). NIEM was chosen because it solves certain data interoperability problems associated with establishing a CCOP in a Joint, Interagency and Coalition environment that other approaches have not been able to solve.

This document describes: (1) operational requirements for a CCOP; (2) how NIEM supports a shared COP used for dashboard display and decision-making in U.S. Mission Partner Environment (MPE) and Federated Mission Networking (FMN) environment implementation; and (3) a roadmap for developing, testing, evaluating and exercising this solution. The approach aligns with both the U.S. Department of Defense (DOD) Net-Centric Data Strategy and the emerging North Atlantic Treaty Organization (NATO) Core Data Framework Vision.

2. Problem Statement.

To-date there is no known comprehensive implementation of a CCOP that supports all U.S. and Coalition requirements. Consequently, the inability to establish a shared CCOP capability in both episodic and enduring environments is a significant obstacle to effective operational decision-making by warfighters at all echelons.

3. Operational Requirements.

The solution discussed in this concept paper uniquely supports a broad spectrum of COP requirements ranging from producing a static image on a digital map and battlefield objects for situational awareness, to collecting real-time data supporting decision making and the warfighter planning processes. The importance of a Coalition COP was recently summarized by the Director of the Joint Staff J6, LTG Bowman:

> "A COP is critical to effectively planning and successfully executing any operation. When it comes to a COP, everyone from the strategic to the tactical wants it and wants it now. COP capabilities allow your command to maintain situational awareness on mission critical activities (current ops, coalition interoperability, cyber, IT networks, logistics, etc.) in a Mission Partner Enduring or Episodic environment. A fully operational COP including mission partners and supported by JIE is key to the commanders' ability to make informed decisions. Sharing SA information across physical, logical and security domains is increasingly related to mission success, and the foundational capability in the Joint and Coalition environment."[1]

4. Current State.

The data required to support decision making across the full warfighting spectrum is resident in multiple NATO compliant information technology IT systems and shared in over 360+ messages developed over the past 20 years of information exchange requirements (IER)

[1] Remarks in the Joint Staff J6 published 'C5 Assessment to Combatant Commands', September, 2015.

analysis and consensus among nations. Even with this body of work completed, U.S. and Coalition partners currently lack the ability to exchange information between multiple diverse non-interoperable command and control (C2) systems.

Many national C2 systems use eXtensible Markup Language (XML) to define the message level architecture of their application program interfaces (APIs) for sharing information. Unfortunately, the use of XML is inconsistent among Coalition partners, which can result in a lack of information sharing among CCOPs.

5. What NIEM Offers.

NIEM is an approach to solving data interoperability problems that applies a standards-based approach which provides the building blocks national C2 systems need to develop agreed upon common interface specifications for the exchange of COP data. In fact, the benefits of NIEM are sufficiently compelling that the DoD Chief Information Officer (CIO) has directed the DOD-wide adoption of NIEM to help resolve interoperability problems caused by the inconsistent use of XML.[2,3] This guidance stipulates the use of NIEM for all XML information exchanges created or modernized as a part of a normal system's lifecycle management. Most recently, the NIEM technical specification was approved to be listed in the DoD Information Technology Standards Registry (DISR) as Information Guidance (the first step to being mandated for use).

NIEM technical specifications have been widely used and matured for over a decade. The family of NIEM specifications defines a common syntactical representation of XML, which is used to create a semantic model of reusable data components supporting military operations among other functional areas. In addition, NIEM provides a flexible and extensible technical framework for defining information exchange specifications supporting a broad range of warfighter mission areas. Of note, the NIEM approach can be used to define data exchange solutions that support the NATO APP-15 Information Exchange Requirement Specification Process.

NIEM also provides a distributed and cost effective approach to governance that allows stakeholders to influence the levels of the NIEM architecture that are important to their information exchange. For example, the NIEM Program Management Office (PMO) governs the NIEM Core portion of the data model (i.e., those data components agreed upon by all NIEM domains) and the NIEM technical specifications. Any NIEM stakeholder can influence the NIEM Core or technical specifications through established NIEM architecture committees. Programs, existing standards bodies, and others who develop IESs using NIEM are responsible to configuration manage the IESs they create together.

This distributed approach to governance allows for independent versioning of artifacts across the NIEM architecture (.e.g., NIEM Core, domain models (like Military Operations-MilOps), technical specifications, data exchange specifications, etc.). As a result, if an IES is

[2] DOD CIO Memorandum, *Adoption of the National Information Exchange Model within the Department of Defense*, 28 March 2013.

[3] DOD Instruction 8320.07, *Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense*, 3 August 2015.

developed using NIEM v3.0, no changes are required when a future version of NIEM is released as long as there were no changes to the data sharing requirements supported by the exchange specification. If a C2 system that uses NIEM in their application interface updates its application software, the application interface does not need to change thereby ensuring interoperability continuity through technology refreshes.

The use and applicability of NIEM for sharing information and supporting identity and privilege management in a Coalition environment has been successfully demonstrated in Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) over the past three years through the Tactical Edge Data Solutions Coalition Warfare Program (TEDS CWP), and the Tactical Infrastructure Enterprise Services Coalition Warfare Program (TIES CWP).

6. Approach for Building a Coalition Common Operating Picture.

Currently, establishing a Combined Joint Task Force (CJTF) is the preferred method to organize coalition forces for managing military operations in an operational theater. The fundamental requirement for effectively operating a CJTF is establishing shared situational awareness.[4] Creating an agreed upon baseline set of IERs prior to the CJTF creation would reduce the time required to establish an operational CJTF CCOP. These baseline IERs would define the structure of what and how information is to be shared, with whom and for how long.

The Joining, Membership, and Exiting Instructions (JMEIs) for the U.S. MPE and FMN Joining Instructions (JIs) for FMN partner nations provide directions for establishing and organizing C2 System data and services requirements of a CJTF. Currently absent from these instructions are a predefined application interface and a protocol for exchanging the C2 System data required to establish a shared COP. JMEIs provide an ideal location to insert baseline IERs required to support a CJTF CCOP. This concept can also be used in a continental U.S. (CONUS) MPE situation between Federal, State, Local, Title 10 and 32 forces called upon to assist in emergency responses. NIEM has successfully been demonstrated in the Geospatial for NIEM (GEO4NIEM) Initiative. "Geospatial information technologies are increasingly a foundation for supporting homeland security, law enforcement, emergency management, and public safety missions in the U.S. While these technologies rely upon much of the same data, they are typically developed in silos within a specific mission area. As a result, data duplication and data exchange delays occur. However, mission partners could benefit from shared access to the common operating data and services used within these geospatial systems if they were exposed and exchanged in open standards. Hence the need for enhancing NIEM's geospatial exchange capabilities in order to significantly improve inter-government information sharing of this critical data source."[5]

[4] Joint Publication (JP) 3-33 "Joint Task Force Headquarters" 30 July 2012 http://www.dtic.mil/doctrine/new_pubs/jp3_33.pdf

[5] https://www.niem.gov/technical/Pages/Geo4NIEM.aspx

7. Technical approach.

In the context of this paper, an API defines a common system interface for sharing data in the establishment of a COP supporting warfighting operations across all echelons. NIEM's role in the API architecture is to define a syntactically consistent and semantically coherent data exchange payload. Once developed and implemented, these structures (i.e., API and NIEM payload) become the point of data interoperability across multiple disparate IT/C2 systems.

Having baseline IERs in MPE and FMN JMEIs support development of a consistent API by participating nations C2 systems and the priority they need to establish shared situational awareness for a CJTF. NIEM directly meets core tenants of MPE to identify who will be sharing information, what information will be shared, and how that information will be shared. Figure 1 illustrates a notional Coalition data sharing environment in which several nations contribute different capabilities to the operation. Each nation provides information about its resources and sources through a single predefined API.[6] International and Non-Governmental organizations

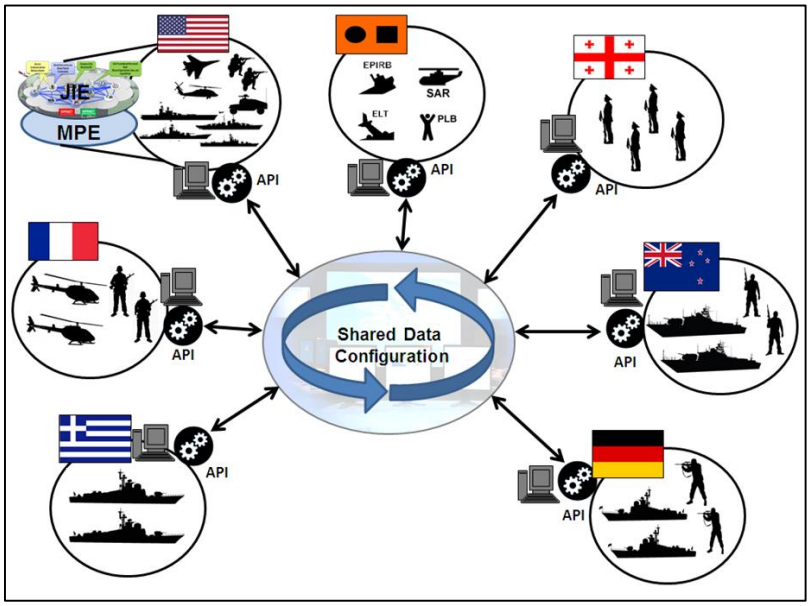


Figure 1: Notional Shared Data Configuration Environment

may also be called upon to assist the CJTF during international distress incidents and they may choose to share their data with the Coalition through the same common API. A NIEM-based solution provides a common syntax and semantics for structuring and defining data level interfaces at all echelons of Joint and Coalition environments across the enterprise. Having an agreed upon API specification provides consistency of information sharing beyond the data level by providing the additional building blocks a programmer needs to build the software interface, and thereby makes it easier to develop a software application or web service.

An API expresses a software component in terms of its operations, inputs, outputs, and underlying types. The API infers a common set of routines, protocols, and tools for accessing

[6] For the purpose of this paper the concept of an API applies to computer software applications, as well as web and mobile applications that leverage capabilities inherent to web browsers and Internet servers.

and sharing information housed in a software application's data store. APIs can be implemented rapidly if pre-defined technical specifications are available for reuse by anyone within the Coalition. The existing NATO exercise program (Allied Spirit, Saber Junction, Combined Resolve and Swift Response) provide the venues for developing and demonstrating a NIEM-based CCOP API.

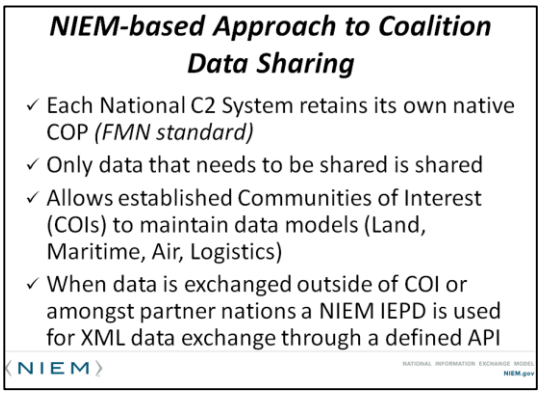
7. Summary and Way Ahead.

The information content required to support decision making across the full warfighting spectrum is resident in multiple NATO compliant IT systems and previously agreed messages. To date, there is no known comprehensive implementation of a CCOP that supports all U.S. and Coalition requirements. Data sharing within a Coalition environment needs an efficient standards-based approach to exploit new and emerging technologies. The requirements and driving need for an effective CCOP, as well as the current data sharing and interoperability problems associated with establishing a CCOP are well documented.

A NIEM-based CCOP API is a proven approach that supports new and emerging technologies, as well as the federated networking environment. The NIEM approach also allows for the independent configuration management of existing C2 systems, data standards, and other data sharing capabilities. This approach will improve data sharing and interoperability while reducing the overall cost and time to establish a federated networking environment. Use of this approach will increase U.S. and mission partner operational situational awareness.

This solution also has the potential to influence and support other data sharing initiatives across DOD such as: GCCS-J modernization, Global Force Management Data Initiative, National and Joint Robotics and Autonomous Systems efforts, NGB's JIEE and WebEOC, etc.

This paper provides the framework in Appendixes A-C to develop a predefined CCOP API to better support the broad array of shared situational awareness requirements at all echelons of mission partners during both episodic and enduring events. Joint Staff J6 plans to leverage CWIX 16 and Bold Quest (BQ) 2016 as opportunities to develop and incrementally mature this capability. After BQ, JS J6 will evaluate the resulting artifacts and consider incorporating them into the MPE JMEIs to establish a base level of data sharing in coalition warfighting environments.



Appendix A: NIEM's Role in API Development

NIEM's role in the API architecture is to provide the technical standards and repeatable engineering processes necessary to develop syntactically consistent and semantically coherent data exchange payloads. Once developed and implemented, these structures become the point of data interoperability across multiple disparate IT/C2 systems. The API defines a common system interface for sharing data in the establishment of a COP supporting warfighting operations across all echelons.

As shown in Figure 2, the API Specification block refers to documentation that provides technical details describing processes, routines, data structures, object classes, and variables associated with a *particular interface.*

The *Descriptions* block employs NIEM XML in conjunction with the NATO Information Exchange Requirement Specification Process (APP-15), DoD Architecture Framework (DODAF), or other IER process to describe and define the structure of the message. The message instance is referred to as an Information Exchange Package (IEP). This block can also include other artifacts necessary to support requirements such as metadata tagging, security markings, identity access management, or payload within a larger message (i.e., Intelligence Community Trusted Data Framework).

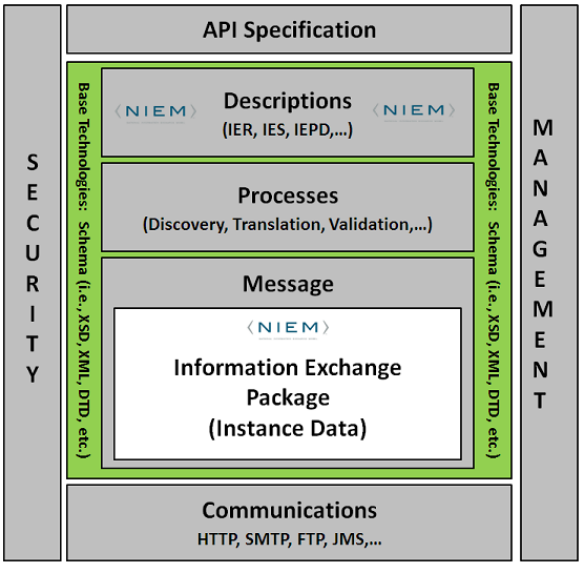


Figure 2: Generic API Architecture

The Communications block refers to all of the necessary hardware, software and protocols needed to connect the API to the network.

The Security and Management blocks extend vertically through all API blocks. Security and Management were intentionally illustrated in this manner to convey that each API block may have its own independent security and management characteristics, requirements and processes.

An API defines its functionalities in a way that they are independent of their respective implementations. For example, a particular API may be implemented using Java in one software application/system and implemented using C++ in another. This allows system specific software implementations to vary without negatively affecting data sharing and interoperability. Each National C2 System is able to retain its own native COP (FMN standard). Only data that needs to be shared is shared as delineated in the CCOP guidance. As a result, an API can take on many forms (e.g., Google Maps Application, Banking Apps on Smartphones, etc.), and share information across the enterprise through remote calls from data consumers (e.g., smartphone users, web services).

Appendix B: CCOP API Design Considerations.

A listing of all possible requirements for Coalition COP is beyond the scope of this paper. To date, there is no known comprehensive implementation of a CCOP that supports all US and Coalition requirements. The design considerations that follow represent high level guiding principles for consideration in developing a NIEM-based CCOP API.

Concepts in this paper postulate an effective CCOP API would be designed to exchange data about any entity (e.g., any noun) in a single location (e.g., position) or multiple locations if moving (e.g., track). It would contain sufficient data components to generate a static dashboard display as well as provide sufficient data to support decision makers at all echelons.

The DOD Net-Centric Data Strategy requires that data, information and information technology services should be visible, accessible, understandable, trusted and interoperable (VAUTI). These tenets when incorporated in a CCOP solution will support:

- *Robustness:* An effective CCOP solution must be able to provide the underlying data (e.g., data source, time added, added by whom, associated data, etc.) of geospatial visualization available in the COP. Underlying data about CCOP resources needs to be made accessible through an interactive (i.e., click-through) CCOP feature.

- *Flexibility:* Resource information is made available in a wide variety of formats (e.g., binary, text, enumerations, etc.) and communicated through national and Coalition messaging standards (e.g., USMTF, Variable Message Format (VMF), Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM), NIEM etc.). These data standards are implemented in unique and incompatible syntax and semantic representations. It is therefore necessary to map and translate data from existing data standards to a commonly defined API supporting a CCOP.

- Security: A CCOP API must support multiple security standards used by prospective mission partners. Any CCOP API must support multiple security marking standards (e.g., UNCLASSIFIED, SECRET, Coalition Specific classification etc.).

- *Redaction*: Aggregated U.S. COP data from the operational theater is classified (SECRET and TOP SECRET) at the operational and strategic echelons. Information will also need to be shared at an unclassified level to other mission partners (e.g., U.S. Government, International Organizations and Multinational Partners).

- *Accessibility:* Optimally, a CCOP is a net-centric, open standard, web-based solution. Proprietary solutions are expensive, require a specific hardware/software configuration to implement, require extensive/expensive certification and accreditation (C&A) and are not inherently interoperable. Conversely, web-based solutions are found across the operational environment, provide scalability throughput to support user requirements across all echelons, require less expensive C&A, and offer configurable componentized solutions.

Appendix C: High Level CCOP Technical Overview

The figure below shows the initial state of the use case where three partners decide to form a warfighting coalition. In the image below, colors (i.e., red, orange, green, yellow and blue) represent common semantic data, shapes (i.e., circle, square, etc.) represent syntactical representation, and the blue cylinders are varied data stores. As a notional example, the color RED represents unit information; however it is represented differently in each of the four databases depicted below. In this use case, all of the C4I systems, including the Combined Joint Task Force (CJTF), receive similar data from different sources and store it uniquely in their own unique databases. In this use case, each C4I system has the capability to generate a COP display.

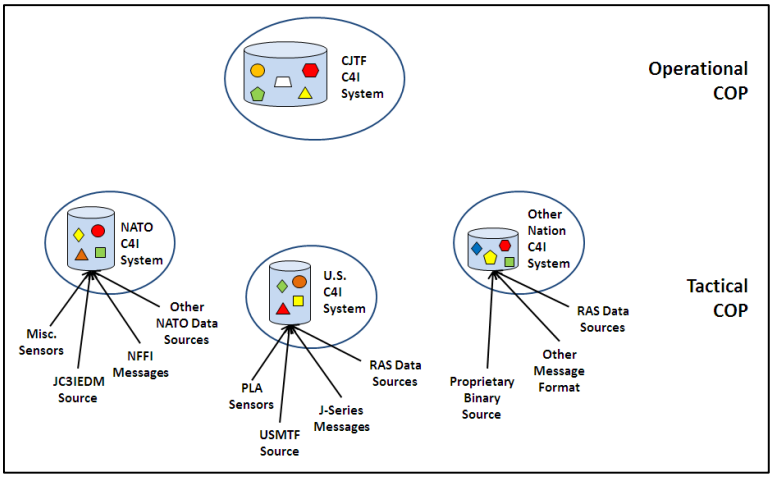


Figure 3: Notional Coalition Environment Initial State

A NIEM based API defines a common system interface supporting the establishment of a CCOP via existing C4I system. NIEM facilitates information sharing by providing a standard syntax and reusable semantic components for defining XML based API interfaces. Furthermore, NIEM does not affect the C4I data store or transport methodologies.

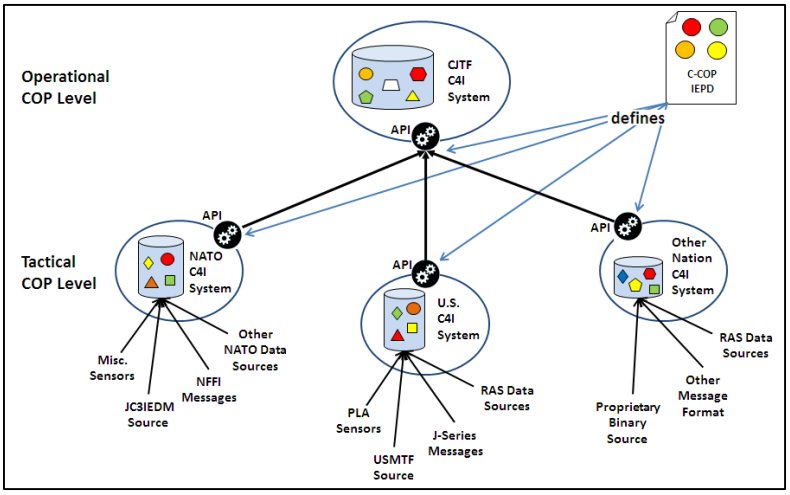


Figure 4: Notional Coalition COP Solution Technical Approach