Data Sharing is a Critical Capability

Ryan Schultz
Joint Staff J-6
Norfolk, VA
ryan.r.schultz.civ@mail.mil

LTC Karla Keelean
Joint Staff J-6
Norfolk, VA
karla.p.keelean.mil@mail.mil

James Jamison
Joint Staff J-6
Norfolk, VA
james.f.jamison2.civ@mail.mil

Ralph O'Connell
Joint Staff J-6
Norfolk, VA
ralph.m.oconnell.civ@mail.mil

ABSTRACT

Data sharing is a critical capability that enables the global integration of military forces to combat trans-regional, multi-domain, multi-functional threats. Interoperable command and control systems are prerequisite for a common strategic understanding which promotes unity of effort and effective mission execution. Enabling the warfighter to make decisions and take action at the speed of the problem requires a robust flow of information by accessing and processing authoritative data sources. Secure data sharing is essential to achieving interdependent joint/coalition forces. Due to its distributed nature, data sharing cannot be 'acquired' as a commodity, nor used as an individual weapon system. Unfortunately, there is no single DOD data sharing system, per se. Rather, using standardization and reuse, data sharing must be incorporated into the requirements development, acquisition, and sustainment phases of complex warfighting information system capabilities.

Joint Staff (JS) J-6 Deputy Directorate for Cyber and Command, Control, Communications and Computers (C4) Integration (DD C5I) Data and Services Division (DSD) operates within an established Joint Command and Control capability development framework that includes governance, standardized information exchange, and authoritative data source visibility and access. Disparate data producing and consuming systems develop their data service capabilities within a standardized framework to fulfill data sharing needs for decision makers. This paper will describe the DSD activities, challenges, and the way ahead to advance an interdependent joint force by evolving and horizontally integrating interdependent data services as critical joint/coalition data sharing capabilities.

ABOUT THE AUTHORS

Ryan R. Schultz is the Chief of the Data and Services Division on the Joint Staff of the Department of Defense (DOD). He manages a 25-person team responsible for working with DOD, interagency, and multi-national stakeholders to identify and resolve warfighter, combatant command and service operational data sharing and data interoperability issues. Mr. Schultz also is serving a 2 year term as the NIEM Business Architecture Committee (NBAC) Co-Chair where he works to set the business architecture and the requirements of NIEM, manage NIEM Core, and facilitate the processes for the regulation and support of NIEM domains. Following a 20-year career in the U.S. Navy, Mr. Schultz worked as both a contractor and civil servant on military database interoperability and information exchange issues, while earning various IT certifications. He also served as a senior information technology (IT) faculty instructor for Old Dominion University, leading a staff of 25 instructors and a 500-student training program. Mr. Schultz received his bachelor's degree in Ocean Engineering from the U.S. Naval Academy. He holds three master's degrees: Master of Business Administration with an IT focus, Old Dominion University; Master of Arts in National Security and Strategic Studies, U.S. Naval War College; and, Master of Science in Oceanography and Meteorology, U.S. Naval Postgraduate School.

LTC Karla P. Keelean is the Chief of the Data Exchange Standardization Section for the Joint Staff J-6, Data and Services Division in Norfolk, VA and serves as the National Information Exchange Model (NIEM) Military Operations (MilOps) Domain Steward Representative. LTC Keelean has over 17 years of experience of employing and managing tactical, operational and strategic level telecommunications and information technology solutions to support conventional, joint, multinational and special operations forces in garrison and during deployed military operations. LTC Keelean received her bachelor's degree in Exercise Science from Eastern Illinois University, her Masters of Arts in Public Policy Management from Georgetown University and earned a graduate certificate in Executive Data Science from Johns Hopkins University.

James F. Jamison is the Chief of Requirements and Implementation Support for the Joint Staff J-6, Data and Services Division in Norfolk, Virginia. In this capacity he advances the implementation of data standards, data sources and services to enable Joint, Coalition and Interagency information interoperability. He enlisted in the Marine Corps in 1974 and retired as a Colonel in 2009. A distinguished graduate of the US Naval War College, he has also earned four Masters Degrees including a 2014 Master of Strategic Foresight from Regent University.

Ralph M. O'Connell is a systems engineer with the Joint Staff J-6 Deputy Director for Command, Control, Communications, Computers, and Cyber Integration (DD C5I) Data and Services Division (DSD). He has a BSEE from Virginia Tech, a Master in Systems Analysis from the Naval Postgraduate School, and certified DAWIA Level III Systems Planning, Research, Development and Engineering - Systems Engineering. Mr. O'Connell has over 30 years' experience supporting military system acquisition and fielding. He is currently working to extend Service developed data service capabilities and standards as DOD Enterprise solutions.

Data Sharing is a Critical Capability!

Ryan R. Schultz
Joint Staff J-6
Norfolk, VA
ryan.r.schultz.civ@mail.mil

LTC Karla P. Keelean
Joint Staff J-6
Norfolk, VA
karla.p.keelean.mil@mail.mil

James F. Jamison
Joint Staff J-6
Norfolk, VA
james.f.jamison2.civ@mail.mil

Ralph M. O'Connell
Joint Staff J-6
Norfolk, VA
ralph.m.oconnell.civ@mail.mil

DATA SHARING IS A CRITICAL CAPABILITY

The coordinated terrorist attacks on 11 September 2001 highlighted United States (U.S.) national security vulnerability to non-state actors using the internet and smart mobile devices as an effective low cost command and control capability. The 9/11 Commission Report (National Commission on Terrorist Attacks Upon the United States, 2004) identified multiple failures of information management, sharing, and coordination within and between layers of government agencies that exacerbated U.S. vulnerability to attack and inability to respond effectively. The report offers five major recommendations for combining resources and people more effectively to achieve unity of effort amongst the federal government. The Commission's recommendations for a National Counterterrorism Center and a Director of National Intelligence have been implemented; however, "unifying the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional governmental boundaries" requires significantly more work and coordination to address "the biggest impediment to all-source analysis – to a greater likelihood of connecting the dots – is the human or systemic resistance to sharing information." A foundational recommendation is that the President should lead the Government-wide effort to bring the major national security institutions into the information revolution.

In military terms, the desired outcome of achieving unity of effort in sharing information is called "Information Superiority." Information superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Publication 1-02, 2016) Current military planning anticipates adversary capabilities that are increasingly trans-regional, from multiple domains, and multi-functional (TMM). Understanding the historical lessons learned, the progressive nature of non-state actor threats, and our warfighters need for effective and agile data sharing between information systems in a complex operational environment (OE) drives the DOD to recognize that data sharing is a critical capability. A critical capability is defined as a crucial enabler for a center of gravity (COG) to function as such and is essential to the accomplishment of the specified or assumed objective(s). (Joint Publication 5-0, 2011) The warfighter COG within a TMM operating environment is a globally integrated and interoperable joint force. An interdependent joint force requires data interoperability that can only be accomplished by standardization with capability developers across the Navy, Army, Air Force, United States Marine Corps, Joint Staff, NATO and Coalition partners. Data sharing cannot be 'acquired' as if were a discrete commodity or individual weapon system. However, data sharing will be improved by incorporating standards and reuse requirements into the early capability development phases of each individual warfighting information system.

Historic lessons learned drive the need for U.S. and coalition partners to maintain an operational advantage over adversaries in a complex, information-laden operational environment. The DOD and Joint Staff Chief Information Officers (CIOs) are the Department advocates for promoting enterprise-wide information sharing; however, the CIOs are not responsible for developing information sharing material solutions. Data sharing is not developed as an independent capability within the DOD, and typically ends up as an "add on" requirement after the C2 systems have been developed by the Services and Agencies. The Data and Services Division (DSD) of the Joint Staff (JS) J-6 Deputy Directorate for Cyber and Command, Control, Communications and Computers (C4) Integration (DD C5I) is tasked to resolve this issue for the warfighter mission area. This paper will focus on the DSD role and functions in developing and implementing enterprise standards to improve information sharing capabilities for the joint and multinational force.

THE JOINT STAFF J-6 MISSION AND DD C5I ORGANIZATION

The JS J-6 assists the Chairman by providing the best military advice while advancing cyber defense, joint/coalition interoperability and command and control (C2) capabilities required by the Joint Force to preserve the Nation's

Security. The JS J-6 DD C5I is responsible for leading Joint C2 capability development, integration, architecture and engineering, C2 data and service standards, joint fires and combat identification, field assessments of joint fires capabilities, C4 system interoperability and technical integration assessments, and cyber capability development and assessments. The DD C5I maintains a persistent C4 environment to accomplish these responsibilities and is organized into six divisions and an analysis team as an end-to-end engagement construct from concept development through fielding and sustainment. This construct enables rapid, agile development and fielding of desired capabilities while providing the requirements traceability needed for mission effectiveness and long-term sustainability.

The DDC5I DSD advocates for data interoperability by facilitating and enabling warfighter access to authoritative data sources, establishing common C5 data and service standards, integrating these standards into capability requirements, and facilitating implementation within programs of record. Data standards describe the rules by which data are exchanged and recorded. In order to effectively share data, we must standardize the format as well as the meaning. (U.S. Geological Survey , n.d.)

The foundation for Joint C2 capability development is based on Standards, Principles, Rules, and Patterns that guide the development of necessary systems, services, data and information, and cybersecurity solutions to meet the warfighters' requirements. The outer oval represents Joint C2 community stakeholders who are considered mission partners. The inner section illustrates the shared context and understanding implicit between hierarchical and lateral echelons of command (i.e., Strategic, Operational, and Tactical levels), and is driven by doctrinal guidance for planning, conducting, and assessing operations. The dark blue oval-ring represents the DOD Information Network (DODIN) and encompasses net-centric capabilities such as Enterprise Services, Information Sharing, and Collaboration. These capabilities reflect key enablers to planning, conducting, and assessing operations, but are non-exhaustive. Figure 3 depicts the operational context for JC2 capabilities and includes key enablers.

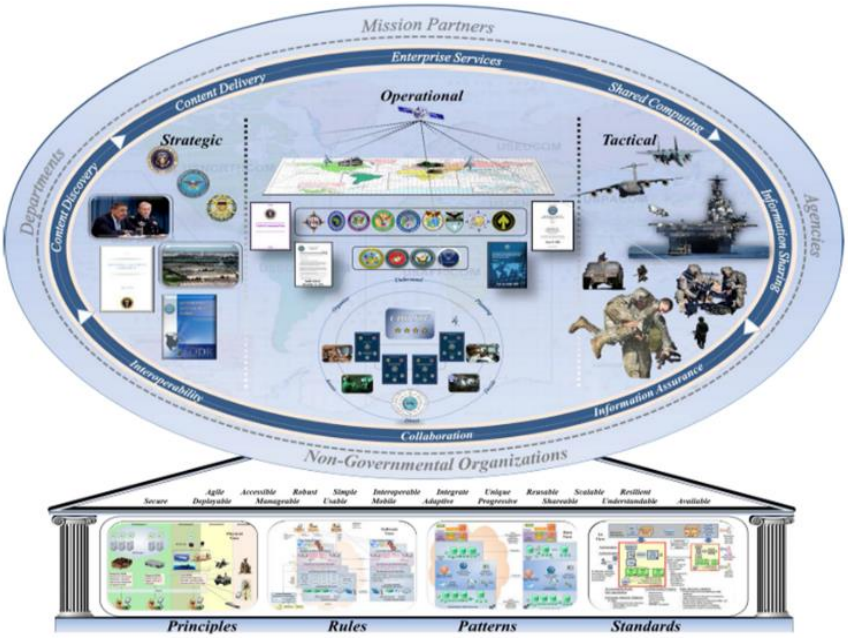

Figure 1 Joint C2 Operational Context and Enablers

Warfighter access to authoritative data that can be integrated into purposeful data sets is foundational to satisfying all JC2 capability needs. There are many different organizations working community-specific solutions for their unique mission. However, access to authoritative geospatial terrain, opposition and friendly force order of battle (OOB), and intelligence data is commonly needed across the JC2 warfighting, intelligence, training, test and evaluation, acquisition, experimentation, analysis, and planning communities. The JS J-6 DD C5I DSD is organized to horizontally integrate these distributed capabilities as enterprise solutions across Combatant Commands, Services, Agencies (CCMD/S/As), and multinational partners for the benefit of our joint and coalition warfighters.

The J-6 DD C5I DSD lines of effort are focused on solving current information sharing problems as enterprise solutions that will result in delivering a sustained information advantage to enable decision and action at the speed of the warfighting problem. Understanding that data sharing is a critical capability for system interoperability, DSD supports the derivation of system requirements from operational requirements and lessons learned to ensure data and service capabilities support our warfighter's mission needs for global integration and a common strategic understanding between mission partners.

J-6 DD C5I DATA AND SERVICES DIVISION (DSD)

The J-6 DD C5I DSD is efficiently organized to support Cyber and C4 capability development by improving data access and interoperability throughout the capability life cycle for the Joint Warfighter. Establishing and implementing common data and service standards within programs of record will improve warfighter access to mission relevant authoritative data. DSD activities that contribute toward implementing common data standards include: Joint, Multinational and Interagency Governance and Management; C2 Authoritative Data Source (ADS) Management; Data Exchange Standardization; Tactical Interoperability and Standards; Information Interoperability Capability Demonstrations; Cyber Symbology; Operational Environment (OE) Unified Data (UD) Alliance; and, the Future Concept Engagement. These activities are synchronized to support the Warfighter's ability to transform data into actionable information in an enterprise-wide information environment.

Joint, Multinational & Interagency Governance & Management

Implementing common data standards across the Joint, Multinational, and U.S. Interagency communities is foundational to interoperability and effective data sharing. DSD leverages multinational and interagency governance and management forums to collaboratively develop, adapt and adopt data standards that support interoperable capability implementation. Data and services stakeholders recognize the importance of converging on enterprise standards to promote successful interoperability between mission partner information systems. DSD seeks to horizontally integrate U.S. Army, Navy, Air Force, Marine Corps and DOD Agency developed data and services capabilities as Joint enterprise solutions that can be extended to interagency and multinational mission partners. The JS J-6, DD C5I and DSD Division Chief chair, co-chair, and support more than 20 enterprise level governance panels, committees, boards, and working groups to integrate Joint and Mission Partner data and services. Figure 4 illustrates some of the governance and management forums where DSD participates to synchronize community developed data frameworks and establish interoperable information exchange standard profiles. Taking a whole of government and coalition interoperability view, DSD seeks to establish common standards that promote enterprise-wide information sharing and reuse.

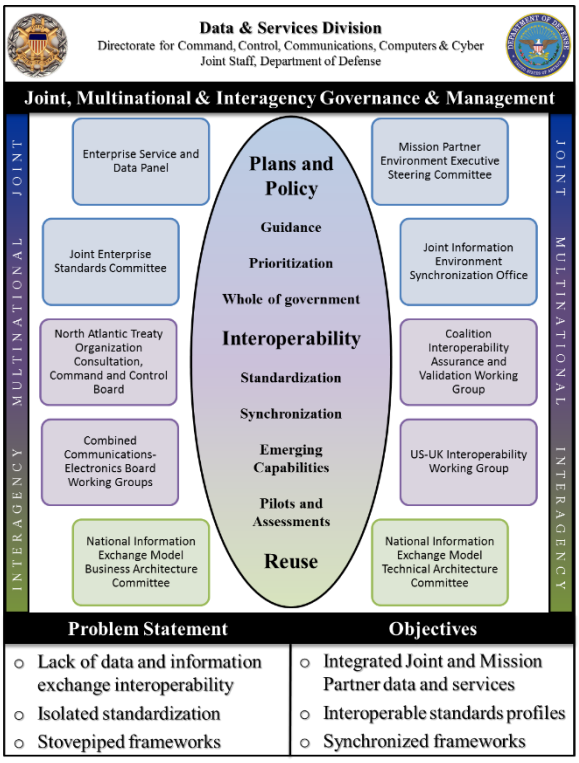

Figure 2 DSD Governance & Management

The J-6 DD C5I chairs the DOD CIO Enterprise Services and Data Panel (ESDP) enterprise-level governance forum to promote visible, accessible, understandable, trusted, and interoperable (VAUTI) enterprise services and data-related activities across the Department with an emphasis on re-use. The panel works to advance the DOD CIO's goals, policies, and strategies by tasking Tiger Teams to address specific data sharing issues in a specified amount of time. The ESDP synchronizes data service capability development activities across the Warfighting, Business, DOD portion of Intelligence, and Enterprise Information Environment (EIE) Mission Areas (MAs).

On behalf of the DOD CIO, DSD co-chairs the Data Technical WG (TWG) with the Intelligence Community (IC) CIO representative to provide IT standard recommendations to the Joint Enterprise Standards Committee (JESC) who advocates to the DOD CIO Enterprise Architecture Services Board (EASB) for the establishment and maintenance of mandatory standards in the DOD Information Technology Standards Registry (DISR).

In an effort to align the DOD information enterprise and DOD Warfighter mission area with NATO and mission partners, DSD serves as the U.S. Head of Delegation to the NATO Information Exchange Requirements Harmonization Working Group (IERHWG) to promote interoperable solutions developed with the NATO staff and allies. The IERHWG harmonizes requirements across all domains (air, land, sea, intelligence, medical, etc.) to translate operator Information Exchange Requirements (IERs) into Information Exchange Specifications (IES) that can be implemented in accordance with a standardized NATO Core Data Framework (NCDF) process. This U.S. and NATO coordination provides a deliberate opportunity to horizontally integrate delivered data and services capabilities.

To advance data sharing as a critical capability for the Joint Warfighter, the JS J-6, DDC5I, and DSD leadership will coordinate with data and services governance and management stakeholders to incorporate enterprise IT standards in the requirements and acquisition process that rewards program managers for the successful delivery of interoperable IT services resulting in a data-sharing combat capability. DSD is preparing enterprise IT services, data and data exchange standards, and data reuse language for inclusion in DOD Acquisition Guidebook that emphasizes implementation during materiel development. Without explicit and standardized acquisition data guidance, DOD developers will continue to develop programs in a vacuum that inhibits enterprise data sharing and can led to sub-optimized warfighter capabilities.

C2 Authoritative Data Source Management

DSD chairs the C2 Data Working Group to manage the registry of C2 Authoritative Data Sources (ADS) and data services. In today's data-dense and austere budget environment, providing access to C2 data and promoting reuse of data services is extremely important. DSD supports and tracks the C2 ADS planning and execution of conforming to the Department's Net-Centric Data Strategy goals of making data visible, accessible, understandable, trustworthy, interoperable, and responsive to user needs on a continuing basis. For C2 ADSs the first three of these goals are tracked, verified and reported by the Division using an ADS exposure metric up through the C4/Cyber Functional Capability Board secretariat and underlies the C2 Combat Capacity Developer's annual Operational Priority process. Approximately 75% of the 200 plus C2 ADS are exposed. Exposure is considered complete when an ADS is: 1) visible -fully registered in the Data Services Environment (DSE); 2) accessible - an operational endpoint or URL is identified; and 3) understandable –an ADS's Web Services Description Language (WSDL) or other schema is published in the DSE. Importantly, the Division works with the Combat Capability Developer to link C2 ADSs with requirements and C2 Operational Priorities through the Joint C2 Decision Support Tool-kit. The linking allows the Joint C2 Family of Programs visibility to if and when ADSs that support their capability are exposed and promotes reuse of authoritative sources across the JC2 community.

Data Exchange Standardization

The CCMD/S/As have historically developed C2 system capabilities without regard for data interoperability with other C2 systems. Rather than addressing standardized information sharing frameworks from the beginning, point-to-point information exchanges are often "bolted-on" after systems are deployed. To provide commanders with a holistic Common Operating Picture for situational awareness, operational C2 systems must share data (interoperate) with logistics, transportation, intelligence and cyber systems. Many C2 systems within DOD use extensible markup language (XML) to exchange data. Unfortunately, without a standardized framework, use of XML does not in-and-of itself guarantee cross-system interoperability. If there are inconsistencies in the XML, a 'translation or mediation' service is required to support data exchanges between multiple C2 systems. A translation mechanism does not ensure an effective information sharing because C2 systems and associated data standards (e.g., United States Message Text Format (USMTF), Cursor on Target (CoT), etc.) may use different term representations for the same information. Point-to-point information exchanges, or gateways, are only useful to the two specified mission partners for that specific exchange. This gateway approach inhibits reuse, as the gateways rapidly become unwieldy in number and expensive for achieving information interoperability. Enabling multiple users to exchange data using a common interface specification is needed to ensure that all authorized users have access to all mission-relevant authoritative data.

The DOD CIO has directed the use of NIEM-conformant XML data exchanges when appropriate to address the problem of using inconsistent XML and data semantics. (DOD CIO Memorandum, 2013) The implementation of this guidance focuses on promoting interoperability at the information exchange data level, and directs the use of NIEM for all XML information exchanges created or modernized as a part of the normal lifecycle management. (DOD Instruction 8320.07, 2015)

NIEM is comprised of a collaborative partnership of agencies and organizations across all levels of government (federal, state, tribal, and local), private industry, and international participants. The purpose for this partnership is to effectively and efficiently share critical information at key decision points throughout the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise. Figure 5 illustrates the NIEM standards-based approach designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information. NIEM is not a software program, database, network, or a computer system. NIEM is designed to facilitate the creation of automated enterprise-wide information exchanges which can be uniformly developed, centrally maintained, quickly identified and discovered, and efficiently reused. Figure 6 provides a NIEM overview description and contrast. The result is more efficient and expansive information sharing partners, more cost effective development and deployment of information systems, improved operations, better quality decision making as a result of more timely, accurate and complete information, and, as a consequence, enhanced public safety and homeland security. NIEM is a common vocabulary (semantics) that enables efficient information exchange across diverse public and private organizations. NIEM connects communities of people who share a common need to exchange information in order to advance their mission. NIEM provides rules and methodologies (syntax) around the use of the model as well as a standardized Information Exchange Development Lifecycle that can be reused by everyone. NIEM also includes governance, training, tools, technical assistance, and an engaged community to support users and organizations in adopting NIEM. NIEM has developed non-normative guidance to support Java Script Object Notation (JSON) (JSON and NIEM, n.d.), and has demonstrated the ability to incorporate Geography Markup Language (GML) objects. (Geospatial Integration with NIEM, n.d.)

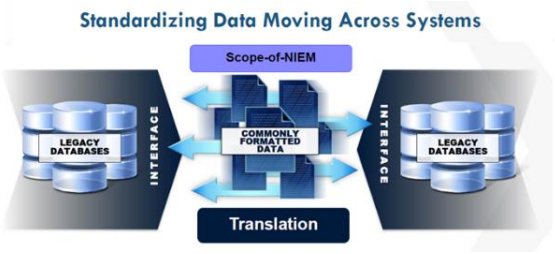

Figure 3 Standardizing Data Exchanges

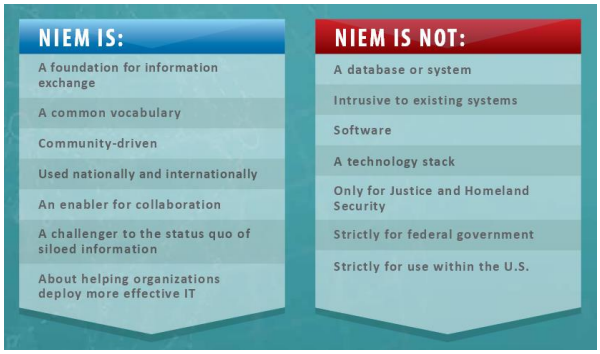

Figure 4 NIEM Overview Description

The NIEM Military Operations (MilOps) Domain was established in March 2014 to extend the NIEM Core to account for the common exchange of military information. The JS J-6 DD C5I serves as the MilOps Domain Steward, as designated by an interagency domain stewardship agreement between the NIEM Program Manager from DHS, DOD CIO and the Vice Director of the JS J-6. The DSD serves as the MilOps Domain Steward Representative and the Secretariat for the day to day operations and maintenance. The MilOps Domain Configuration and Control Board (MO CCB) manages Domain content (Data components and semantics) and addresses technical issues arising during development to include the use/reuse of Information Exchange Package Documentations (IEPDs).

Along with running the MilOps Domain, DSD supports warfighter integration for XML. Working with the CCMD/S/As and Warfighter Communities of Interest, DSD ensures that joint capability requirements are compliant with DODI 8320.07 and also ensures that content within the MilOps Data Model is harmonized with joint doctrine and the joint warfighter community needs.

Tactical Interoperability & Standards

DSD leads J-6 activities for improving U.S. and Partner Nation data interoperability through the C2 Interoperability Program; specific tasks include prioritizing and scheduling Defense Information Systems Agency (DISA) support and identifying required tactical data standards enhancements and standardized XML information exchanges. In support of tactical data standards enhancements DSD assists in the development, and sponsors, interface change proposals into applicable configuration management boards to continuously improve standards based on CCMD validated requirements to improve interoperability between US Forces and Partner Nations. DSD coordinates the release of CCMD validated U.S. Military Standards (MIL-STD) and related NATO standard documents to Partner Nations.

DSD supports the development of tactical data link (TDL) requirements for Ballistic Missile Defense (BMD) and interoperability of the integrated Ballistic Missile Defense System (BMDS). The BMDS includes space, ground and sea-based defense systems, C2, battle management, and communications elements. DSD provides CCMD requirements and JS J-6 oversite during the conduct of peer reviews to address interoperability issues related to missile defense and participates in technical analyses for the development of necessary change proposals to TDL standard and operational procedures.

DSD provides technical and management subject matter expertise for maintaining the United States Message Text Format (USMTF) MIL-STD-6040 Interface Standard. USMTF MIL-STD-6040 details messages that are approved for use by all departments and agencies within the DOD; it provides definitions for USMTF terminology, establishes message standards, and provides a catalog of message and associated C4I data elements for use across DOD. DSD supports the alignment and synchronization of USMTF with partner nations, warfighting publications, and agreements. A primary example is USMTF synchronization with NATO's Message Text Format Capability Team and Allied Procedural Publication – 6 (APP-6).

Information Interoperability Capability Demonstrations

- Coalition Tactical Edge Data Solutions (TEDS) (2010-2013) demonstrated an increase in the quality of military situational awareness and enhanced interoperability with mission partners by incorporating C2 Core as a common data model.
- Tactical Infrastructure Enterprise Services (TIES) Joint Capability Technology Demonstration (JCTD) (2013-2016) demonstrated solutions for joint and coalition tactical edge warfighting C2 information sharing requirements by enabling C2 services to function securely in a Denied, Disconnected, Intermittent, Limited (DDIL) environment.
- Tactical Infrastructure Enterprise Services (TIES) Coalition Warfare Program (CWP) (2013-2016) demonstrated a federated system to verify the identity of network users, automate element-level metadata tagging solutions with coalition partners, and demonstrated machine-to-machine message exchange capability between US Army and coalition C2 systems.
- Simulated Interactive Robotics Initiative (SIRI) (2014-2015) demonstrated the use of XML-based message exchanges for robotic and autonomous systems to assess the utility of binary XML in Robotic and Autonomous Systems.
- NATO Core Data Framework (NCDF) (2016-2018) demonstration will validate the processes used to build Information Exchange Requirements (IERs), Information Exchange Specifications (IES), and implementation methods for NATO-coalition data exchange interfaces. The NCDF Procedural Tiger Team (TT), under the direction of the Data Management Capability Team (DM CaT), will exercise the strawman processes with the goal of improving future NCDF processes. The Procedural TT will track the progress of the Technical TT's at the Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) 2017 demonstration and incorporate 'learned lessons' into the "NCDF Information Exchange Processes and Procedures" guide. The ultimate objective of the NCDF is to advance interoperability by improving information sharing across the NATO Enterprise, the Alliance and coalition Partners.

Proposed Data Interoperability Demonstrations

Looking to the future, DSD has submitted four cross-cutting capability demonstration proposals that leverage ongoing work and horizontally integrate potentially stove-piped efforts.

- Robotic and Autonomous Systems Information Interoperability (RASI2) Joint Capability Technology Demonstration (JCTD) proposal to demonstrate the utility of common data interfaces for improving cross-system, cross-Service robotic and autonomous systems information sharing capability.
- Standardizing Coalition Command & Control Access, Data, and Services (SCC2ADS) JCTD proposal to demonstrate secure information exchanges in coalition network using publish / subscribe services, automated access controls based on user credentials and automated machine-to-machine standardized data exchanges.
- U.S. Air Force (USAF) Unmanned Aerospace System Command and Control Information – U.S. Navy Common Control Station Data Exchange (UCI-CCS Exchange) proposal to demonstrate the viability of using standardized data format to exchange mission information between different operational systems.
- U.S.-United Kingdom (UK) Multilateral Interoperability Programme (MIP) NIEM Exchange proposal to demonstrate an UK-US Army data exchange using MIP-NIEM formats.

Cyber Symbology

Cyber operations and joint doctrine are evolving to keep pace with technology and threats. Cyber terminology has changed within the Department from Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE) to Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO), and DOD Information Network Operations (DODINO). Consequently, these changes must be reflected across Joint Doctrine, Organization, Training, Material, Leadership Development, Personnel, Facilities and Policy. (DOTMLPF-P). DSD chairs the Cyberspace Symbology WG that is working to standardize operationally relevant cyber objects within the DOD Interface Standard for Joint Military Symbology MIL-STD-2525, ensure that Joint doctrine and cyber symbology are synchronously maintained to reflect changes in doctrine, force, and operational essential tasks necessary to conduct Cyber operations. Integrating cyber symbology into the C2 COP provides JTF commanders with better situational awareness across the full range of military operations that include Sea, Air, Land, Space, and Cyber domains. Benefits include de-confliction of operations and tasks and enable Commanders to apply cyber effects. Figure 7 provides three examples of potential cyber symbology. The "Cyber Threat Actor (Full Frame)" icon is derived from google and iconfinder.com images. (ICONFINDER, 2017)

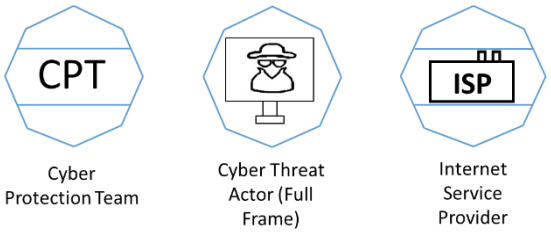

Figure 5 Potential Cyber Symbology

OPERATIONAL ENVIRONMENT (OE) UNIFIED DATA (UD) ALLIANCE

DSD is leveraging the U.S. Army enterprise effort to promote a shared understanding of a complex operational environment that enables decision making and mission execution across all levels of operation. The U.S. Army Mission Command and M&S Office community stakeholders are collaborating to develop enterprise solutions to common OE data representation, visualization, decision making, and analysis problems. DSD is extending this collaborative approach to the other military Services, DOD Agencies, Interagency, and multinational partners to advance information sharing in a Mission Partner Environment (MPE). All community missions need timely access to some OE data. No one community is resourced to deliver all needed OE data services. Reusing capabilities and collaboratively developing new data services as enterprise solutions are critical to our collective mission success. The OE UD concept provides an organizing construct to align cross-community activities and focus deliberate collaboration between organization that are seeking solutions to common OE data needs, Figure 8. ADS providers publish their holdings using standardized syntax and semantics, such as NIEM. Web services are available to provide warfighters and decision makers with data discovery, retrieval, extract, transform, load (ETL), and integration capabilities to serve integrated and normalized OE data holdings to support big data analytics. Value added data that is generated from decision support systems becomes available to the MPE to aid in trend analysis. The intent is to horizontally integrate the development of interdependent data service capabilities to deliver data sharing as a critical capability.

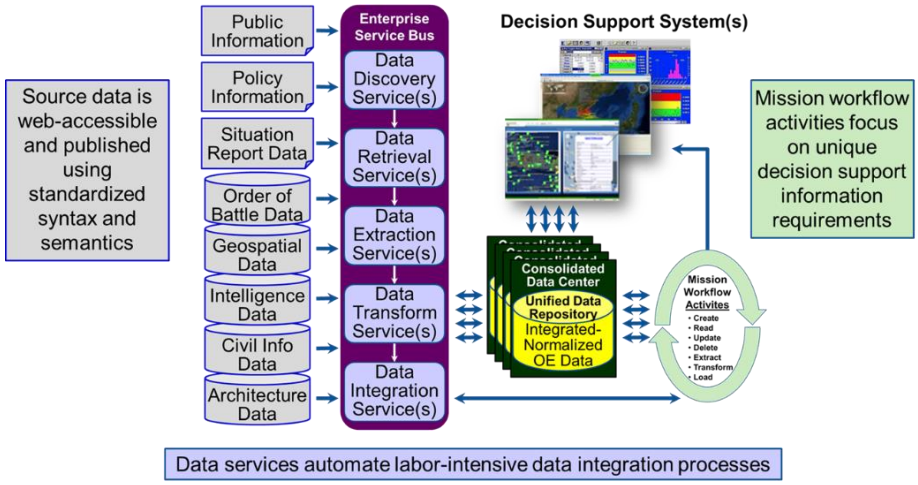

Figure 6 Unified Data Concept

Future Concept Engagement

DSD supports pre-decisional Joint Concept development by advocating the maturation of the Department's data strategy into the next version of the Capstone Concept for Joint Operations. DSD incorporated key principles of data sharing into the interoperability annex of the recently signed Joint Concept for Robotics and Autonomous Systems. Further, engagement with the Global Integration and Common Strategic Understanding workshop, as part of the Capstone Concept for Joint Operations Exploration, ensures that the Unified Data Concept and the need for standardized semantics and syntax to enable information exchanges are identified as key enablers for supporting future decision makers.

WAY AHEAD

DSD supports the development of community specific standards and facilitates collaboration across interdependent DOD CCMD/S/A capability development activities to lead the convergence towards Joint enterprise data standards and enterprise information technology services. As the DOD converges on standardized information exchanges, DSD coordinates with other U.S. departments and agencies to advance national data exchange standards such as NIEM. DSD is collaborating with the Department of Homeland Security (DHS) to demonstrate the value of standardized information exchanges between the DOD, DHS, Federal Emergency Management Agency (FEMA), state and local governments, and first responders in a U.S. disaster relief/humanitarian assistance scenario.

As the U.S. establishes Joint standardized information exchanges, DSD coordinates with multinational partners to promote convergence with international data exchange standards. The way ahead to advance multinational partner information sharing is heavily dependent upon coordination and collaboration with NATO.

NATO's agreement to evolve the NATO Core Data Framework (NCDF) in a manner that aligns with DOD and US standards will promote interoperability and understanding of data across Alliance and Federated Mission Networking environments. A key objective of this framework is supporting the harmonization of shared data components and interoperability between communities of interest (COIs). The focus of the framework approach is to unambiguously describe well-defined operational concepts and their relations.

A critical piece of the framework is cross-COI and cross-domain harmonization. Governance creates, optimizes and refines a set of business rules which shares common data assets across the domains and COIs of the NATO enterprise. Positive governance can therefore be seen as a process for the exercise of rules and control which will encourage COI and domain implementation of the NCDF.

To develop an IES from an IER, efficiency gains can be realized by standardizing the content and structure of the IER. In addition to the information elements, which describe the operational content, other explanatory information is helpful to create an IES that matches the operational intent of the IER. In essence, syntax enables the linkage between and IER and an IES. COIs should be able to extend and modify the IER within their own domain and provide feedback to the NATO NCDF custodians that may trigger a change to the NATO reference. The initial approach for NCDF Naming and Design Rules (NDRs) is the implementation of the XML; however, future iterations must address the use of other languages such as JSON, HTML, etc.

The primary purpose of the Semantic Reference Model (SRM) is to provide a common information reference that can be used to discuss, harmonize and relate the different terms in an operationally meaningful way. A fully developed NCDF model can be used to define an application independent view of information which can be validated by users and then transformed into a design for any of the various standards / technologies. IES development can be accomplished efficiently through the reuse of existing specifications. The disciplined application of security tagging metadata will ensure data is only accessible by authorized users. The authors believe that IES reuse will led to solutions with lower development costs and reduced time to create, test and field new capabilities. The same techniques will also improve the use and reuse of data and information across an operation, which will improve the shared situational awareness across a Combined / Joint Force.

Evolving a suite of standardized tools will improve IER and IES development. Features of the tool suite include the ability to search the NCDF data model, map to NCDF, and create IER and IES artifacts. Conformance and interoperability testing tools will be required to link the NCDF concepts, IER and IES, and will assist developers in creating, with a high level of confidence, that the IES meets all operational and technical requirements of an IER.

While the long term vision is to implement a standard NCDF across existing and emerging information systems, the transition will require the interoperability between NCDF conformant and non-conformant systems. In this interim period the Computer Information System (CIS) could facilitate information exchange between heterogeneous systems using gateways, translators, and/or an enterprise service bus to provide and receive information through middleware which can accommodate different (structured and unstructured) data formats.

Achieving standardized information exchanges with NATO will require an effective governance structure to maintain and evolve data standards in a dynamic global environment. The objective will be to incorporate MIP and Message Text Format (MTF) domains within the NIEM enterprise standard. The NATO Data Management (DM) and Message Text Format (MTF) Capability Action Teams (CATs) will provide the necessary configuration management to adjudicate change requests and promote interoperability.

CONCLUSION

Due to the distributed nature of data sharing, the Department cannot ‘acquire’ a ‘data sharing’ weapon system, yet enabling warfighters to make decisions and take action at the speed of the problem is a priority need that requires an uninterrupted flow of shared data at all levels of warfare. The ability to deny adversaries’ data sharing is also critically important. Accessing and processing authoritative data is prerequisite to achieving a globally integrated joint force. Incorporating enterprise data standards, reuse, sharing requirements into the combat capability developer process will lead to an effective data sharing warfighting capability. JS-J-6 DD C5I DSD focus and tenacity will help overcome the cultural, political, and technical obstacles necessary to deliver data sharing as a critical capability to our deserving warfighters.

DISCLAIMER

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the US Joint Staff, JS J-6 or the US Government. The US Government is authorized to reproduce and distribute reprints for Government purposes.

REFERENCES

DOD CIO Memorandum. (2013, March 28). Adoption of the National Information Exchange Model within the Department of Defense. Adoption of the National Information Exchange Model within the Department of Defense.

DOD Instruction 8320.07. (2015, August 03). Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense. Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense.

Geospatial Integration with NIEM. (n.d.). Retrieved from https://www.niem.gov/techhub/geospatial-integration

ICONFINDER. (2017, February 5). ICONFINDER. Retrieved from Agent, big brother, cia, crime, cyber, fbi, government icons: https://www.iconfinder.com/icons/213384/agent_big_brother_cia_crime_cyber_fbi_government_hacker_justice_law_nsa_spy_tor_user_icon

Joint Publication 1-02. (2016). Department of Defense Dictionary of Military and Associated Terms.

Joint Publication 5-0. (2011, August 11). Joint Publications. Retrieved from Joint Electronic Library: http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf

JSON and NIEM. (n.d.). Retrieved from https://www.niem.gov/techhub/json

National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report.

U.S. Geological Survey . (n.d.). Retrieved from https://www2.usgs.gov/datamanagement/plan/datastandards.php