23rd ICCRTS

"Multi-Domain C2"

Building a Coalition Multi-Domain Learning Environment

Paper #40

Topic 1: Operational Issues: Multi-domain and Coalition Command and Control

Mr. Ken D. Teske

ASIF Methodologies

Mr. Mark E. Miller

ASI Consulting

Mr. Patrick J. Guerin

Aligned Cybersecurity Solutions

Mr. Jeffrey A. Lauver

Key Management Solutions

Point of Contact

Ken D. Teske

ASIF Methodologies

Virginia Beach, VA 23454

(757) 514-1218 kteske@asif-methodologies.com

Abstract

For several decades mission partners that include Coalitions, Alliances, Governments, Ministries, Departments, Bureaus, Agencies, Special Operations, and Conventional Forces have not been able to capitalize on a holistic learning environment. We collectively capture lessons learned and best practices from combat, exercises, training events, and external assessments to improve our processes and procedures enhancing command and control (C2) abilities. However, we collectively fail to institutionalize and apply the documented lessons learned and best practices because we approach this from an induvial organization/unit perspective verses a collaborative sharing environment for all.

What is needed is a Coalition Multi-Domain Learning Environment to share and learn lessons from all types of operations and units' experiences to address the challenges associated with working with different mission partners in any operation. This learning environment will encourage stakeholders to engage and grow the environment into a holistic learning ecosystem enabling analysis, studies, new policies, provide technical advice, and enable better C2 recommendations. The ecosystem will need to consider how to store data, simplified access with next generation encryption that is quantum resistant, content delivery (information sharing), multi-domain aggerating from lowest to highest levels of protection, and the ontology or lexicons.

Introduction

A Coalition Multi-Domain Learning Environment needs to be created to share and learn lessons from all types of operations and units' experiences to address the challenges associated with working with different mission partners in any operation. This learning environment will encourage stakeholders to engage and grow the environment into a holistic learning ecosystem enabling analysis, studies, new policies, provide technical advice, and enable better recommendations. The ecosystem will need to consider how to store C2 data, simplified access with next generation encryption that is quantum resistant (a C2 enabler), content delivery information through effective sharing, multi-domain aggerating from lowest to highest levels of protection, and the ontology or lexicons. These changes will enhance the C2 Decision Cycle that is often represented by the Observe, Orient, Decide, and Act (OODA) Loop as well as four classes of information processing functions: [A]

- Information acquisition
- Information analysis
- Decision and action selection
- Action implementation

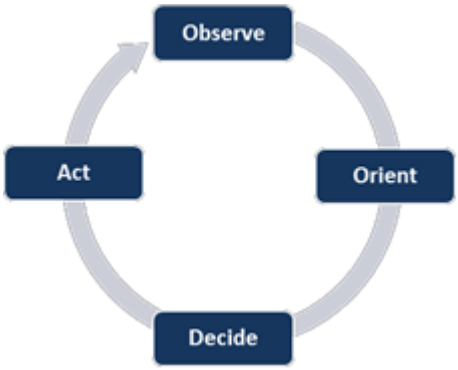


Figure 1: The OODA Loop

Background

The availability of various sources of information in mass quantities can potentially contribute to reducing the uncertainty of collected data, nevertheless, alignment of large amounts of diverse data with inconstant levels of accuracy remains a multifaceted problem. Currently, most data analysis is predominantly accomplished by a manual process using analyst Tactics, Techniques and Procedures (TTPs) that haven't changed significantly for decades. Due to the exponential increase in the volume, velocity, and authenticity of collected most data over these same decades, it is now virtually impossible for human analysts to keep up. Expertise in data mining, data analysis, and data science which bring into play statistical models, artificial intelligence (AI)

and advanced programming [B, C], is now required to address this problem. As our technology continue to evolve, learning from the data available is more important than ever preventing data overload and loss of critical information [D].

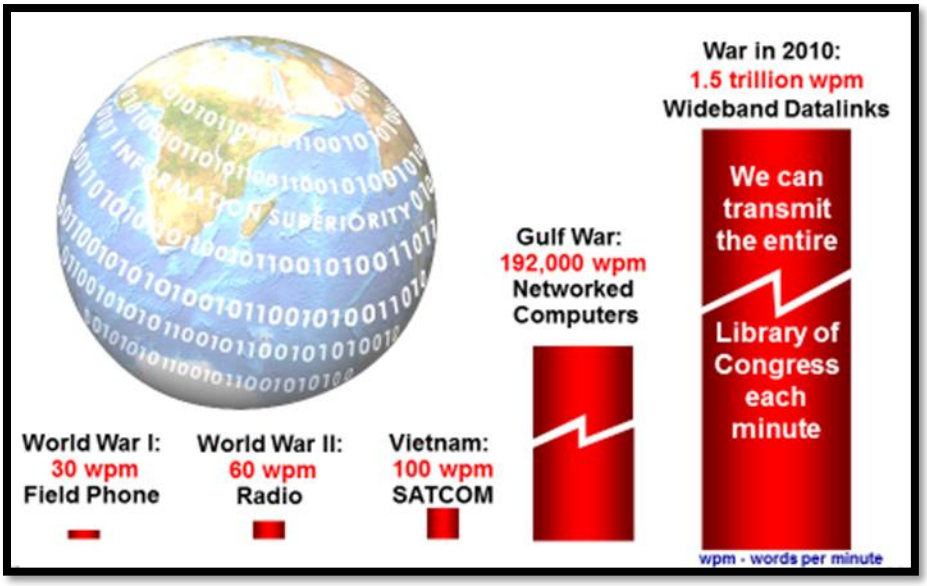


Figure 2: Information Overload [D]

"We are facing a major disconnect between the volume of collection, available digital data and our ability to derive meaningful intelligence from that collection, and we don't have much time to fix it." *Lt Gen Shanahan, June 2016*

To maintain effective C2, all mission partners must continuously take advantage of the latest technological developments and produce dynamic algorithms, incorporating machine-to-machine learning and artificial intelligence capabilities to address the vast amounts of C2 data being produced. The concept for CMDLE is an idealized networked environment consisting of overlapping layers; Collaboration, Data, Analytics & Toolsets, and software development (Dev) and software operation (Ops) (Dev/Ops) [E].

The alignment, synchronization, and integration of these overlapping layers enhances the ability of the four levels of effort to feed and support the CMDLE which assists in developing a picture and a shared understanding of the events and issues challenging our Commanders and

organizational stakeholders. The development of the CMDLE has the following challenges that stakeholders must consider during the development: [F, G, and H]

- Cultural Resistance within Operations and Intelligence leaders
- Changes to current policy
- New policy development
- Acquisition Challenges and funding issues
- Intellectual property
- Data privacy rights, protections and consent, e.g. Europe's General Data Protection Regulation (GDPR)
- Interoperability issues
- Cybersecurity issues

Using the CMDLE, when transitioned into operations, with machine learning and artificial intelligence applications will allow stakeholders and analysts to:

- Automate portions of their workflows
- Improve the quality of their operations and intelligence products by including much more data in the analysis than is currently possible today
- Discover new operations and intelligence information they didn't know existed
- Make use of collected data that previously "fell on the floor" because there aren't enough humans to analyze it

The vision for the CMDLE is to establish a dynamic learning environment to develop and deploy machine learning and artificial intelligence applications and capabilities on any network that analyzes existing feeds in order to impact the speed of access, speed of decision, and speed of action. As there is a built in AI into units they can actively solve problems, understand and obey orders, and learn from both its experiences and the experiences of others. [I, J] It will require management and control of all of the mission data to meet the intent: ensuring the visibility and transparency of data needed for sound, timely, and effective decision making, is available to achieve common goals and objectives to enhance the analyst's ability to provide actionable information to commanders in order to make informed decisions.

The ultimate goal is to enhance autonomous operations by leveraging machine-aided decision-making capabilities in a machine-to-machine environment to take full advantage of autonomous systems enabling the human analyst to be able to better see the needle in the haystack. A secondary goal is to put the power of advanced analytic tools and a dev/ops environment in the hands of operational users with the ability to persist custom user-built tools because all forms of information to support detection, targeting and engagement, where different force components use combat power in coordinated action to produce desired effects on a target [I].

Additional enabling objectives include:

- Provide a Collaboration Environment that includes Dev/Test for the control of the code that allows for responsive change based on technical evolution and to focus resources on high priorities that enable us to stay ahead of very flexible adversaries
- Development of a new capability that dynamically constructs and reasons about type relationships based on content and structure and this mechanism will based on the execution of a SPARQL type query [K]
- Architect the data layer to support the vision and present a logical & physical approach to managing data separate from the applications (modularity) and provide open, modular design for Data access with fully documented services
- Provide an operational implementation that is aligned with the Reference Implementation within the Collaboration Environment.
- Clarify the needed wholesale changes in people/culture, governance, methodology, and technology required to achieve the vision and support Machine Learning.
- Parse various scenarios, plans, and gaps into logical solution space to update data layer defined data delivery methodologies and provide / allow for disruptive applications.
- Develop and enforce data standards and APIs.
- Provide dB management for disparate components of the architecture.
- Provide an ecosystem for “objects” and “observations” to be normalized for use throughout the user community from a variety of sources.

- Create and produce Object Management as a Service and the underlying data structures… to leverage machine-added decision-making capabilities in a machine-to-machine environment to take full advantage of autonomous systems.

Provide a set of tools by which all levels of the user community and stakeholders can better understand the interoperability challenges facing the CMDLE today, and then target selected, high return on investment areas for improvement.

CMDLE Evolution

The evolution of CMDLE through the establishment of an organizational framework will provide leaders (strategic through tactical) with required flexibility, to establish operable policies, training and manage the integration of disparate networks and capabilities, to establish criteria for joining instructions, to affect architectures, standards, transport, systems, tools and applications. The objective capability is the establishment of agreed upon set of common mission threads and an environment in which stakeholders can connect with their own infrastructures, to exchange authoritative data through CCMD established standards, interfaces and joining instructions. It is a mission focused information environment that is agile, flexible, scalable, and mission assured, enabling command and control of US and coalition forces, and coordination with inter-agency and international civilian partners.

CMDLE will enable the effective exchange of relevant operational and intelligence information and become the new normal supporting planning, situational awareness, coordination, and decision-making within and amongst stakeholders. CMDLE is a desired end-state that will be pursued with the objective, evolving over time, to meet the needs of a changing operational landscape while taking advantage of technical advances and technology refresh. CMDLE will be an operationally driven capability framework from strategic through tactical with a focus across the DOTLMPF-P.

The Environment

CMDLE will be an environment where analysts/programmers will be able to post proposed algorithms which intel analysts can test and apply to real world all data sets to see if the algorithm enhances intel products to support commander's and decision making. Analysts will be able to adopt algorithms and apply them to operational systems once proven in the CMDLE Dev Ops tool allowing faster review of all data using machine-to-machine learning and artificial intelligence. To do this we must use dynamic semantic relationships to exploit the structure and semantics of managed information and various information type representations. [L]

CMDLE will reside on many networks to provide warfighters with a centralized resource for ALL mission data to include live data, archived data, and derived data. CMDLE will also make available a dev/ops environment where warfighters can write their own tools for filtering or data aggregation. There will be data visualization services available plus the ability to setup machine to machine data flows from authoritative sources.

CMDLE will have 3 operating modes: Subscription based services; direct machine to machine connections, and through a Web-based GUI.

CMDLE will provide a framework to leverage US forces and mission partner efforts and information. It is essential that authoritative information will be available from the full spectrum of providers enabling analysis, decision making and increased access.

This concept integrates CMDLE capabilities into a common understandable environment that is:

- Leader focused
- Created with common standards, interfaces, and instructions
- Focused on common mission capability definitions
- Scalable for user access across all levels (strategic, operational and tactical)

Paradigm Shift in Understanding and the Role of Individual Perceptions

The operational requirement is to increase speed of access to data to the operational warfighter across all mission effects and networks to enhance information sharing and the exchange of data capable of supporting all stakeholders and Mission Partners. The environment must be capable of ingesting, segregating, and storing data and applications. This capability will, as a result of all stakeholders and Mission Partners having access to all shareable data; enhance "mission" planning and decision making by having a better understanding of our global capabilities.

As for individual perceptions, research focused on information sharing among individuals has found that certain individual beliefs may affect personal willingness to share. These findings tend to focus on beliefs specifically regarding individuals, however, and are less likely to be applicable to motivations for information sharing at an organizational or nation-state level. Nevertheless, we dis- cuss the findings here to illustrate additional psychological factors that have been found to be important influences on information sharing. For example, He and Wei argue that user beliefs are paramount in maintaining knowledge-sharing systems and communities. [M] Other's note that some barriers to knowledge contribution may not be selfishly motivated. [N]

Principal Paths to success

The multi-domain character of C2 in modern warfare is best captured under the concept of Hybrid Warfare, where military capabilities are only one among many 'instruments of power' that can be used to target opponent vulnerabilities. The operational outcomes of such strategies are no longer described in terms of their physical and non-physical manifestation, but in terms of linear and non-linear effects that they produce across the full spectrum of societal functions; political, military, economic, social, informational and infrastructure (PMESII). [O] The alignment, synchronization, and integration of the following areas of effort are critical to the success of the CMDLE:

- **Network Integration & Access** to increase mission data availability
    - Situational Awareness (SA) is an important aspect of Command and Control (C2), and a key enabler for military sovereignty. [P]

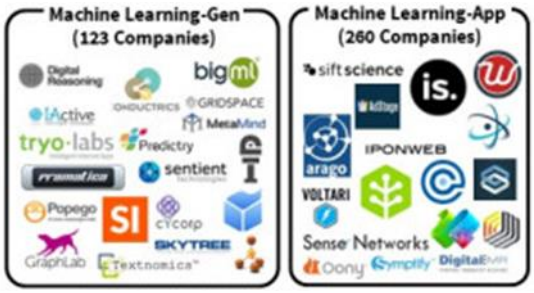
    - Enable federation of the Air, Land, Maritime, Space, and Cyber domain data between multiple network and/or system classifications
    - Accelerate integration potential
    - Common Intel Picture/Common Operational Picture (CIP/COP) for key senior decision makers
- **Institutionalize Data as a Priority**
    - Big data capabilities and approaches on aggregated data sets (open source, reporting, etc.)
    - Example usages:
        - Integrate disparate data
        - Automatic target recognition set of algorithms
- **Agility to Research, Adopt, Integrate, Test or Develop at the Operational and Tactical Edge**
    - Critical enabler for many strategies
    - Open Systems Architecture & Agile methodologies will require wholesale changes in people/culture, governance, methodology, and technology

CMDLE Development Approach

In the future warfare environment completely transformed by technological advances, deliberative decision making, increasingly reliant on ISR and intelligence analysis, is expected to be punctuated with reactive phases, during which commanders will have to counter the unprecedented speed and reach of adversary operational tools within reduced decision timeframes, with the help of automation-based decision aids. [Q] The envisioned development approach for the CMDLE with emphasis on the focus areas identified as follows:

- Collect and analyze and look for “Best Practices” in the categories listed below:
    - Deep Learning/Machine Learning:
        - Organizations that build computer algorithms that operate based on their learnings from existing data. Examples include predictive data models and software platforms that analyze behavioral data.

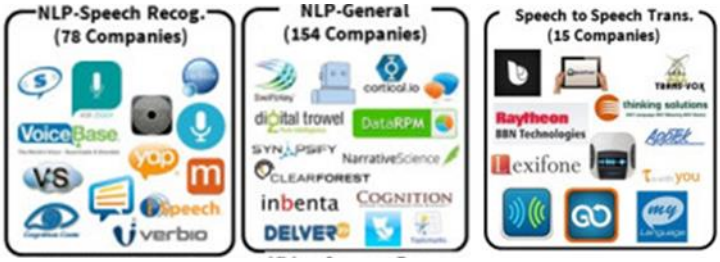
- Organizations that utilize computer algorithms that operate based on existing data in vertically specific use cases. Examples include using machine learning technology to detect banking fraud or to identify the top retail leads.



- Natural Language Processing:
  - Organizations that build algorithms that process human language input and convert it into understandable representations. Examples include automated narrative generation and mining text into data.

  - Organizations that process sound clips of human speech, identify the exact words, and derive meaning from them. Examples include software that detects voice commands and translates them into actionable data.

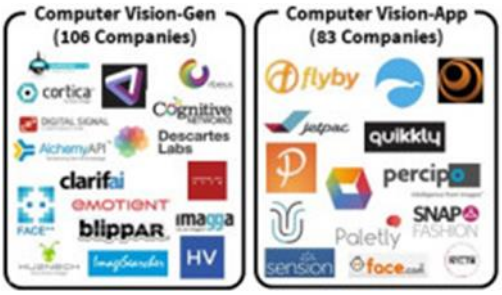
- Speech to Speech Translation: Software which recognizes and translates human speech in one language into another language automatically and instantly. Examples include software that translates video chats and webinars into multiple languages automatically and in real-time.



- Computer Vision/Image Recognition:

- Organizations that build technology that process and analyze images to derive information and recognize objects from them. Examples include visual search platforms and image tagging APIs for developers.

- Organizations that utilize technology that process images in vertically specific use cases. Examples include software that recognizes faces or enables one to search for a retail item by taking a picture.



- Context Aware Computing: Software that automatically becomes aware of its environment and its context of use, such as location, orientation, lighting and adapts its behavior accordingly. Examples include apps that light up when detecting darkness in the environment.

- Recommendation Engines and Collaborative Filtering: Software that predicts the preferences and interests of users for items such as movies or restaurants and delivers personalized recommendations to them. Examples include music recommendation apps and restaurant recommendation websites that deliver their recommendations based on one's past selections.

- Video Automatic Content Recognition: Software that compares a sampling of video content with a source content file to identify the content through its unique characteristics. Examples include software that detects copyrighted material in user-uploaded videos by comparing them against copyrighted material.

- Testing using Reference Operational Environment in Lab environment
- Use the "Best practices" from existing Reference Architectures and DevOps environment(s) to facilitate rapid transition to the CMDLE environment and foster reuse and interoperability from the community

LEVERAGES EXISTING CAPABILITIES

CMDLE is being designed to support Warfighting Operators, Decision makers, and Analysts by making previously stove-piped mission data available in real time while providing state-of-the-art analytics to those who want to examine the collected date in detail. The importance of leveraging intelligence capabilities in support of operations has been repeatedly emphasized by defence strategies. [R, S] CMDLE will enable machine to machine users, subscription-based customers, and interactive users to learn more about their battle-space and target sets by being directly connected to data. Users can choose real-time event monitoring or monitoring a specific feed or indicator. Subscription based customers would be using RSS feeds, email, ftp, etc. to send CMDLE product to their local system. Machine to Machine customers would be provided with up-to-the minute compliant map layers and overlays and links to ongoing collections. Interactive users would engage with the CMDLE Web GUI and DevOps environment querying the system and writing code which will use organic services like IFTTT (If This Then That) to provide custom alerts, feeds or product mashups. However, it is reasonable to assume that the usage of this type of autonomous systems in warfare will increase rapidly over the next 10-20 years, and that the technical development and maturity of such systems will be swift, which thus most likely will entail a move towards autonomy in its true sense. [T]

Tactics, Techniques, and Procedures (TTPs)

Major changes to the CMDLE will be approved by a Configuration Control Board (CCB) consisting of a minimum of three members and chaired by a Deputy. At least one technical representative with knowledge of most networks and server availability will be a CCB member. The CCB will determine the individuals responsible for updating and maintaining the CMDLE. The CCB will also determine the timeline for the future transition of the CMDLE to other network environments of security domains.

All CMDLE sources/references should be used to continuously update and refine the current data elements at least semiannually. Provided templates to assist in verifying, adding or updating additional information for reference.

The CMDLE framework will be characterized by providing all mission partners a standard set or baseline of expected common policies and operating standards. These policies may be strategic cyber considerations or may be those more tactical concerns such as the mission partner "joining instructions." Developing common policies and standards requires the establishment of CMDLE governance bodies to agree to parameters that articulate specific mission network requirements to mission partners in advance of a crisis situation.

The organizational relationships and responsibilities required to achieve success, ensure visibility, monitoring, coordination, management, defense, and control of the CMDLE are provided here within. These relationships will establish positive end-to-end distributed management and control. Provide an organizational structure to support the CMDLE where:

- CMDLE will be institutionalized to support mission commander, functions, and operations in a manner that enables authorized users and their mission partners to access and share timely and trusted information within the defined CMDLE.

- CMDLE will be the responsibility of the mission commander in the defined cyber operating area. Commanders must recognize the risk inherent with CMDLE and

implement discipline and high standards to ensure prompt adherence to all CMDLE operation directives and instructions.

- CMDLE data will be shared and exchanged through common interoperable standards in accordance with a data centric strategy.

- The management responsibility of CMDLE inherently falls to the stakeholders, hence individual(s) are required to ensure that CMDLE remains a viable asset. The management roles include but are not limited to:
- A common set of CMDLE mission-driven metrics, measurements, and reporting criteria shall be used to assess CMDLE operating performance and to determine the mission impact of service degradations or outages.
- Perform routine CMDLE risk assessments to mitigate risks to the global information sharing.
- Training will be provided for the operation, maintenance, and minor coding/ programming changes for the CMDLE to include how to refresh/update the data. Major coding/programming changes should be contracted out for assistance.
- Current access has been limited to a few members in the CMDLE during the testing and demonstration of the CMDLE. Future access will be granted by the CMDLE maintainer upon request of those wanting/needing access. Access will initially be controlled by establishing log-in and password permissions and later with pre-shared key (PSK) based access controls to better enhance access control and protection.

Conclusion

It is envisioned that CMDLE will evolve into a multi-classification Integration Platform as a Service (iPaaS). As defined by Gartner, Inc. a world's leading research and advisory company, an iPaaS is "a cloud service that provides a platform to support application, data and process integration projects, usually involving a combination of cloud-based applications and data sources, APIs and on-premises systems."[V] An iPaaS is usually provided to its users as a multi-tenant service and is used to integrated Software as a Service (SaaS) applications, either with other SaaS applications, or with on-premises systems.

References

A. Parasuraman, R., Sheridan, T. B., and Wickens, C. D. A Model for Types and Levels of Human Interaction with Automation, IEEE Transactions on Systems, Man, and Cybernetics

B. Monnappa, A., https://www.simplilearn.com/data-analyst-vs-data-scientist-article

C. Najafabadi, M. M., Villanustre, F., Khoshgoftaar, T. M., Seliya, N., Wald, R., & Muharemagic, E., Deep learning applications and challenges in big data analytics, Journal of Big Data

D. Teske, K. D., National Defense University (NDU) PINNACLE, CAPSTONE, and KEYSTONE Joint Operations Modules 2004-2007

E. Loukides, M. What is DevOps? What we mean by "operations," and how it's changed over the years, https://www.oreilly.com

F. van der Geest, J., van den Broek, C. C., Bastiaansen, H. H., & Schenk, M. M., Enabling a Big Data and AI Infrastructure with a Data Centric and Microservice Approach: Challenges and Developments, NATO STB IST-160 Specialists' Meeting

G. European Commission, General Data Protection Regulation (GDPR), https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

H. Endsley, M. R., From here to autonomy: lessons learned from human–automation research. Human factors

I. Joint Fire Support, https://www.army.mil/e2/c/downloads/361884.pdf, June 2010.

J. Argall, B. D., Chernova, S., Veloso, M., & Browning, B., A survey of robot learning from demonstration. Robotics and autonomous systems

K. Ayodele, T. O., Machine Learning Overview, New Advances in Machine Learning

L. DuCharme, B., Learning SPARQL, O'Reilly Media, http://www.oreilly.com

M. Allemang, D., Hendler, J., Semantic Web for the Working Ontologist: Effective Modeling in RDFS and OWL, Morgan Kaufman

N. He, Wei, and Kwok-Kee Wei, "What Drives Continued Knowledge Sharing? An Investigation of Knowledge Contribution and -Seeking Beliefs," Decision Support Systems

O. Ardichvili, A., Page, V., and Wentling, T., "Motivation and Barriers to Participation in Virtual Knowledge-Sharing Communities of Practice," Journal of Knowledge Management
P. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, MCDC January 2017.
Q. Alberts, D., Garstka J., and Stein F., Network centric warfare. Developing and leveraging Information superiority
R. United States Army Training and Doctrine Command, The Operational Environment and the Changing Character of Future Warfare, smallwarsjournal.com
S. Strong, Secure, Engaged, Canada's Defence Policy, Minister of National Defence, 2017
T. National Strategy of the United States of America, Sharpening the American Military's Competitive Edge, 2018.
U. Ministry of Defence, DCDC, Joint Concept Note on Human-Machine Teaming. Forms and Publication Section, Bristol, UK
V. Thoo, E., Guttridge, K., Use iPaaS to Unify Data and Application Integration, https://www.gartner.com