

Space Situational Awareness Architecture Vision

Principal Author: David Richmond

Lockheed Martin

CONFERENCE PAPER

1. ABSTRACT SUMMARY

Vast amounts of Space Situational Sensor data are collected each day. Net-Centric approaches are being developed to expose this data. The need to shift from our closed legacy systems to an open scalable architecture has begun. Cloud computing and “Big Data” concepts are also desired to store and process this data. Architecture insights will be provided to highlight how these apparently competing concepts can work together to provide a robust system of systems. Key items that will be covered include:

- 1) An overview of the “As-Is” system of Web Services
- 2) Definition of “Cloud Computing” and “Big Data”
- 3) Vision of “To-Be” SSA system of systems
- 4) Benefits of future approach
- 5) Path forward – Governance and Oversight

2. INTRODUCTION

Achieving Space Situational Awareness (SSA) requires timely information regarding all ground nodes/infrastructure, links and on-orbit assets required to conduct space operations, as well as the hazardous debris environment. The number of near-earth and deep-space satellites has been increasing as more countries increase their space capabilities and through the growth in countries using space. This has significantly increased the number of space related ground stations, communication links, and Resident Space Objects (RSO).

Existing data structures limit the precision of the information being exchanged and limit the precision of key information computed such as the exact location of an RSO at a given time. This can be seen with the Two-Line Element (TLE) set. This data structure captures the orbital parameters of an RSO in two 80 character records. This legacy format, circa 1960, was created to accommodate the 80 character card readers used by mainframe computers and has persisted to this day to accommodate existing software that is dependent upon the data structure. Since each data field is constrained to specific character locations within the TLE, the data structure is not capable of expressing increased precision for any of the data fields. Similar limitations exist in other key SSA data structures caused by legacy formats.

Point-to-point communication channels have bandwidth constraints resulting in restrictions in the quantity of data being exchanged. Policies such as the minimum number of observations used in a track have been established that ensure all data transmitted will be used in processing. This limitation is also addressed procedurally by transmitting only data requested. This results in additional supplemental data not being considered when creating the current situational picture.

Improving the data channels to allow all the available data to flow would simply overwhelm the existing systems. These systems were developed many years ago and were sized to process the data observed at that time. The computing technology deployed to process the SSA data has not kept pace with the increases in SSA data. Computing technologies have advanced considerably since these systems were developed. Use of these new computing technologies would be required to process the increased available data flow.

Several data sources are required to achieve SSA. Currently these data sources lack common protocols, standards and formats. Some of these sources are the result of analysts' reports and these reports may be produced as a word document, PowerPoint presentation, or wiki page. This variety in data formats introduces challenges when attempting to exchange the data for further processing.

The shortcomings of today's SSA data architecture are illustrated in Fig. 1.

Background - Today's Data Architecture

- ★ Multiple stove-piped networks
- ★ Low accuracy and manual data entry
- ★ Gaps in information (ex. maneuvers and surveillance)
- ★ Lack of common protocols, standards, and formats
- ★ Increasing data volume and overload
- ★ Information assurance and Cyber security
- ★ Limited bandwidth
- ★ Unaffordable
- ★ In-flexible
- ★ Untimely



Opportunity for improvement without new, dedicated, or costly sensors

Fig. 1 "As-Is" SSA Data Architecture

To accommodate this growth, an evolution of the Space Situational Awareness Architecture has been underway over the past several years. It has been moving away from a collection of stove piped systems with limited bandwidth, system specific message structures and aging equipment into a collection of systems that expose data net-centrally to establish a loosely coupled architecture that provides data from multiple sources to User Defined Operational Picture (UDOP) visualization clients and data processing clients.

3. "As-Is" SSA ARCHITECTURE OVERVIEW

Various techniques have been developed for net-centric exposure of SSA data. Net-centric data exposure alone will not provide mission utility. Rather, net-centric data exposure enables the creation of client applications that can provide increased capabilities. To maximize the potential benefits of exposing SSA data net-centrally we must maximize five tenants as depicted in Fig. 2.

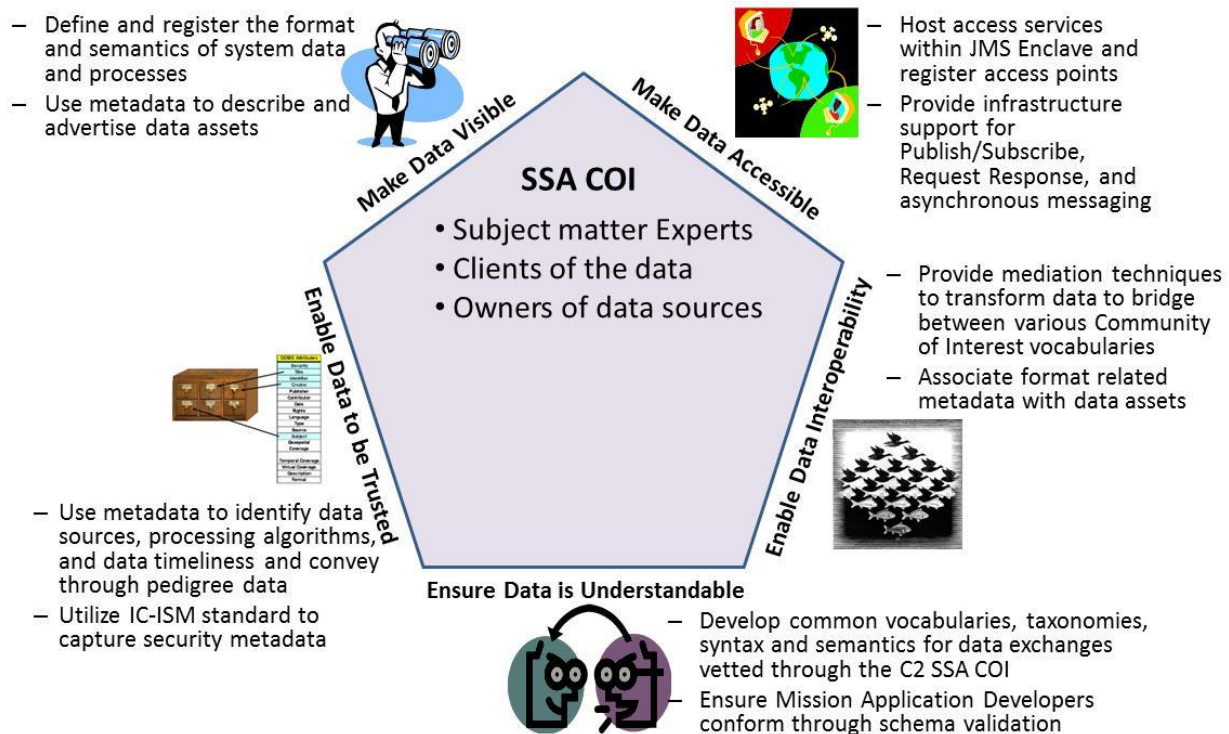


Fig. 2 Net-Centric Data Exposure Tenants

Transitioning from point-to-point communication to a net-centric paradigm requires the data be understood. Common terms may have different meanings to different people. A good example would be the term “Satellite”. This could mean:

- all man-made objects performing a mission
- all man-made objects
- all objects orbiting a celestial body

Establishment of a Community of Interest (COI) plays a key role in implementing understandable net-centric data sharing. Understandable data focuses on reaching agreement on the meaning of information between the producers and consumers. This COI has Subject Matter Expert (SME) participation to arrive at a common vocabulary, lexicon, ontology, and eXtensible Markup language (XML) data schema. The artifacts that make up the data model form a common vocabulary to exchange information between major program components, as well as with external systems, applications and services. The data model consists of the following artifacts:

- Data Definitions (Logical Data Model)
- XML Schema (Physical Data Model)
- Service Description Documentations
- Web Service Description Language (WSDL)s
- Design & Implementation Guidance

To make the information visible to the community, many of these products are registered into the Data Services Environment (DSE). Thus, client application developers can gain access to the information necessary to understand and access exposed data items.

The *The JSpOC Mission System (JMS) Common Data Model: Foundation for Net-Centric Interoperability for Space Situational Awareness* [1] defines the steps being taken to establish the SSA COI and develop the JMS Common Data Model.

The *Net-Centric Sensors and Data Sources (N-CSDS) Ground-based Electro Optical Deep Space Surveillance (GEODSS) Sidecar* [2] defines one approach to make data accessible. The Sidecar concept is to publish data in Near-Real Time (NRT) via the Net-Centric Enterprise Services (NCES) interface and provide Request/Response queries via Web Services. A sidecar has been defined as an on-line, computer processing system that net-centrally exposes data from a host system in a non-interfering manner that effectively decouples the sidecar processing and communication paths from the host system operational string. The initial N-CSDS Sidecar was developed in support of the Space Surveillance Network (SSN). However, the N-CSDS Sidecar can be adapted to support any data source. The mission of the sidecar is to provide a net-centric, one or two-way path for access to the data of a particular data source and to provide input data. The GEODSS sensor located in Socorro, New Mexico is the first Space Surveillance Sensor (SSN) to receive the N-CSDS Sidecar. Plans are being formulated to deploy the N-CSDS GEODSS Sidecar to additional locations.

Multiple data sources offer similar information. When these sources do not agree it is important for the client to understand the source. Providing the data pedigree with the mission data will enable the client to trust the data provided from a given source. Additionally, steps to encrypt the data in transport ensure the information has not been altered and allow the clients to trust the data sources information.

Several web services have been created exposing SSA data that fall short on one or more of the net-centric tenants. These web services still have the potential to enable mission utility. However, improvements in satisfying the net-centric tenants can further client applications ability to provide mission utility.

4. BIG DATA AND CLOUD COMPUTING

Increases in the number of SSA data sources exposed net-centrally will enable the ability to leverage the concepts of 'Big Data' and 'Cloud Computing'. These concepts mean different things to different people. To establish context for the author's usage of these terms they will be defined.

Doug Laney, in 2001, noted three dimensions of data management: Volume, Velocity, and Variety. He established a framework for managing the phenomenon that would become known as 'Big Data', though he never used the term. A system has a Big Data problem when one or more of these dimensions exceed the processing capacity of the conventional database solution. The data is too big, moves too fast, or doesn't fit the structures of the systems database architectures. To gain value from this data, an alternative way to process it must be selected. The National Institute of Standards and Technology (NIST) have been developing a 'Big Data' definition [3] that is illustrated in Fig. 3.

The evolution of exposing SSA data net-centrally will increase the volume and velocity of data received by the SSA architecture. The variety of the data will continue to be diverse in the future due to the need for unstructured reports generated by analysts. Thus, the SSA Architecture vision must deal with the 'Big Data' issue or rely on improvements in traditional database approaches. The frameworks available focus on approaches to store the information such that it can easily be retrieved and on processing data in parallel.

Big Data Overview

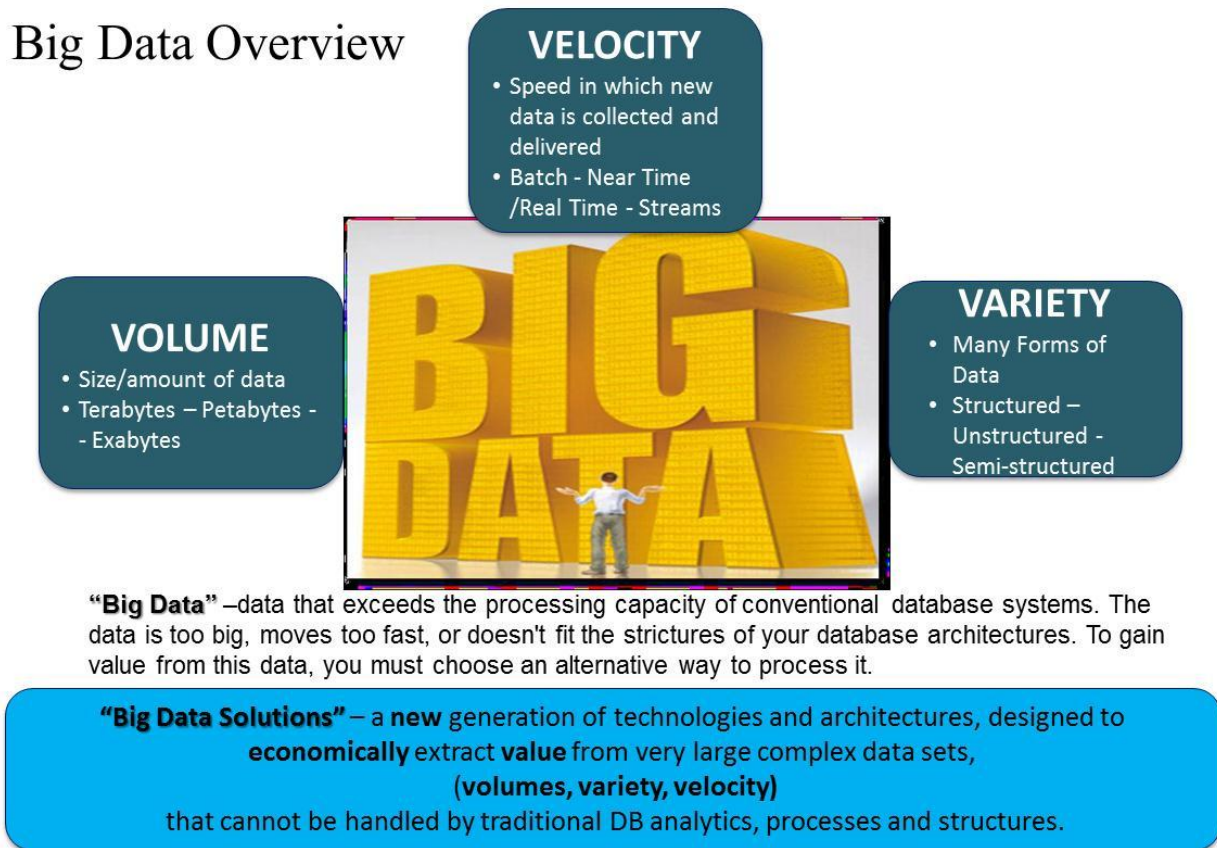


Fig. 3 Big Data Defined

NIST published a Cloud computing definition [4] that stated:

"cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The NIST definition lists five essential characteristics of cloud computing and three service models. The definition is intended to serve as a means for broad comparisons of cloud services and deployment strategies.

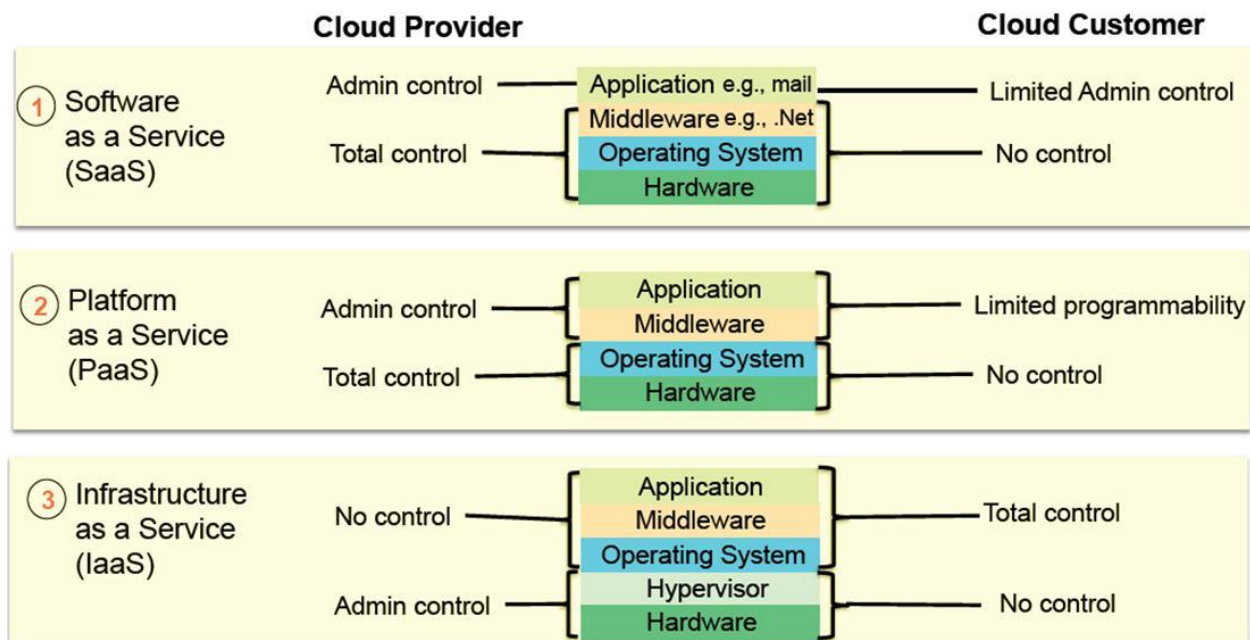
The characteristics of Cloud Computing include:

- On-Demand Self Service. Capabilities available for users to obtain, configure and deploy cloud services themselves using cloud services catalogues, without requiring the assistance of IT
- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
- Resource Pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- Rapid Elasticity. Capabilities can be elastically provisioned and released in some cases automatically, to scale rapidly outward and inward commensurate with demand.

- Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

Cloud Computing can be categorized into service models. These are illustrated in Fig 4 to be:

- Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. The consumer does not manage or control the underlying cloud infrastructure with the possible exception of limited user-specific application configuration settings.
- Platform as a Service (PaaS). The capability provided to the consumer is the ability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, but has control over the deployed applications and possibly application hosting environment configurations.
- Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating system, storage, deployed applications, and possibly limited control of select networking components.



Source: NIST

Fig. 4 Cloud Deployment Models

Opportunities exist to host enterprise wide capabilities that can be leverage by multiple commands to reduce overall program costs.

5. SSA “To-BE” ARCHECTURE VISION

Modifications to the SSA Architecture must improve the mission utility for the warfighter otherwise the changes cannot be justified. The evolution from point-to-point communication to a net-centric communication model has the potential to increase the precision of the data exchanged and unlock additional data collected but not utilized by today's systems.

Vast quantities of relevant SSA data exist today. Efforts have been underway for several years to make this data available Net-Centrically. Common requirements have been levied on each of these efforts. These common capabilities should be considered as potential Cloud computing opportunities.

Each System is required to provide some level of data archiving. All systems require the security logs be archived and most systems require the mission data be archived. Based on the value of the data, timeliness requirements for backup and restore are imposed. Cloud computing data archive solutions have been well established on the internet and should be leveraged to meet this critical need.

Making data available on a network must also be accompanied with capabilities that restrict access to authorized users. Authentication and authorization of users requesting access to the mission data is also a common requirement across all programs and would be a good candidate as a cloud computing capability. Establishing an enterprise level authentication/authorization capability has the potential of reducing overall sustainment costs since provisioning new users or revoking access could be performed once at a central location versus multiple times for each system a user is granted access. A centralized authentication/authorization capability would also provide a single sign on method reducing the access time for the end user.

The net-centric data exposure efforts offer clients the ability to receive the data in near-real time through publish/subscribe capabilities. In many cases this was accomplished through the Enterprise Message capability provided by NCES. This Enterprise Message capability was designed to be scalable to address additional systems in the future.

Leveraging these cloud computing capabilities will reduce the overall development and sustainment cost of systems. The reduced costs are realized through reductions in the hardware needs and COTS license requirements of the system under development. Additionally, the overall development timeline of the system is reduced since these capabilities are not being developed.

The cloud computing capabilities will introduce new concerns to the program under development that must address. The RMA computation must account for this external dependency. The system under development will need to evaluate the impact of cloud application outages on mission needs. Additionally, modifications to the cloud application may drive the need for modifications to the mission system. Updates to the cloud applications should be treated similar to COTS vendor product updates and planned for by the mission system.

Survivability will be a concern of the SSA Architecture. How and where the data is stored will be a key to a survivable architecture. Existing Big Data frameworks provide a means of storing data for later retrieval and the frameworks provide data replication between nodes. These data storage and replication capabilities can be combined as a Cloud Computing service referred to as a Regional Gateway. Fig. 5 illustrates three of these regional gateways to enable a fault tolerant solution when portions of the enterprise or network become unavailable. Data sources providing data to the regional gateways are also depicted.

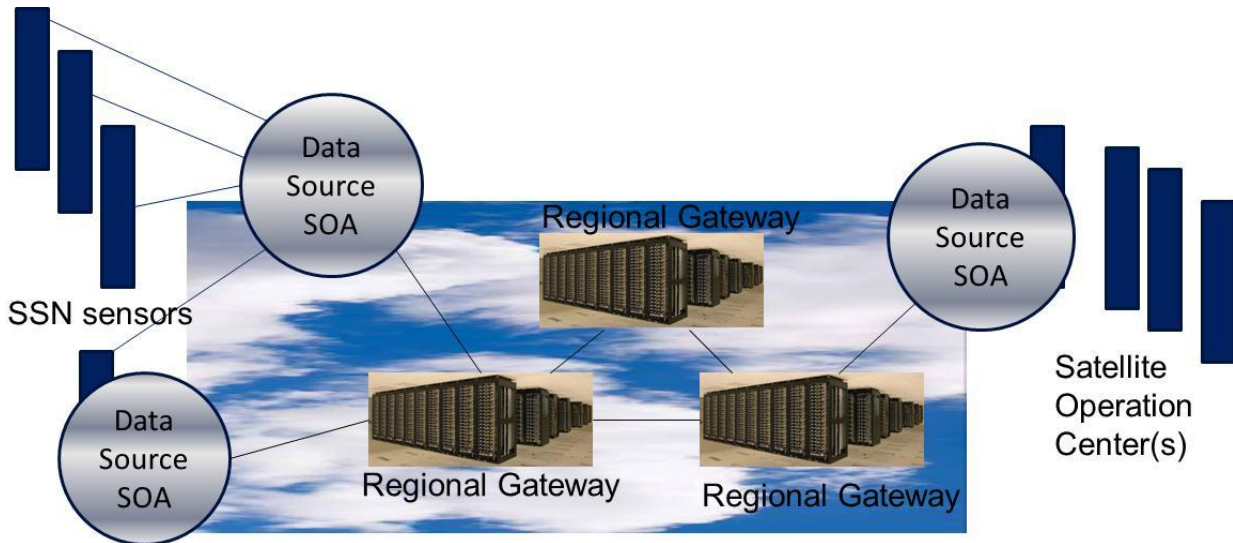


Fig. 5 Multiple Regional Gateways

The volume of data produced from a data source should be considered in the decision to expose raw or processed data. Large volumes of data could exceed the capacity of the attached network. The Big Data frameworks offer approaches to move processing to the data instead of moving data over the network. This has the potential of reducing the load on the network while taking advantage of all the data available. This capability also supports local processing in distressed network conditions.

The velocity of the data arriving at the Regional Gateways will continue to increase. The Big Data framework offers approaches for parallel processing of the data and it also offers methods to replicate the data between regional gateways. These Big Data capabilities can be combined with cloud publish/subscribe capabilities and net-centric data exposure approaches to offer a complete data management solution. The data could be exposed from a data source using N-CSDS capabilities, published using the NCES capability in the cloud, received by a regional gateway through a subscription. The regional gateway would replicate the data to the other regional gateways. Further processing would be done using parallel processing providing:

- Current situational awareness
- Threat prediction
- Event attribution
- Anomaly resolution

Colonel Mike Wasson, Chief, Combat Operations Division, 614th Air and Space Operations Center, stated [5]:

“The JSpOC requires highly responsive SSA capabilities that rapidly detect, track, and characterize objects in space. As such, new developments in SSA tools and capability to assess and respond to events in space are imperatives for the future.”

To address some of these needs Lockheed Martin has developed the Intelligent Space (iSpace) capabilities. It leverages multiple data sources that have been exposed net-centrally and Big Data concepts to perform intelligent catalog maintenance and continuous conjunction assessment. It uses a rule-based analysis of space events to perform a threat assessment and provide automated forensic and predictive threat analysis. It supports dynamic tasking of both conventional and non-traditional sensors. It utilizes multiple best of breed astrodynamics algorithms, including advanced UCT processing to address the ever increasing catalog maintenance size. iSpace is a prime example of how net-centric data sources enable client applications leveraging Big Data concepts to provide mission utility.

The Advanced Space Mission Utility (ASMU) experiment was conducted to investigate opportunities and challenges in performing cross-sensor operations via horizontal integration. The ASMU experiment included

electro-optical, laser, and radar test facilities with iSpace C2 and mission data processing. The experiment demonstrated sensor tipping/queuing, rapid target identification, continuous track custody, automated threat assessments, distributed data fusion, and RSO fingerprint creation. Data exposed net-centrally enabled the ASMU experiment and Big Data concepts were used to provide mission utility.

Technologies and skills for advanced cloud computing and Big Data analytical techniques continue to improve. These improvements coupled with data exposed net-centrally form the basis of the SSA Architecture vision to provide the mission capabilities required by the JSpOC. Fig. 6 illustrates the SSA Architecture vision with Cloud Computing and Big Data.

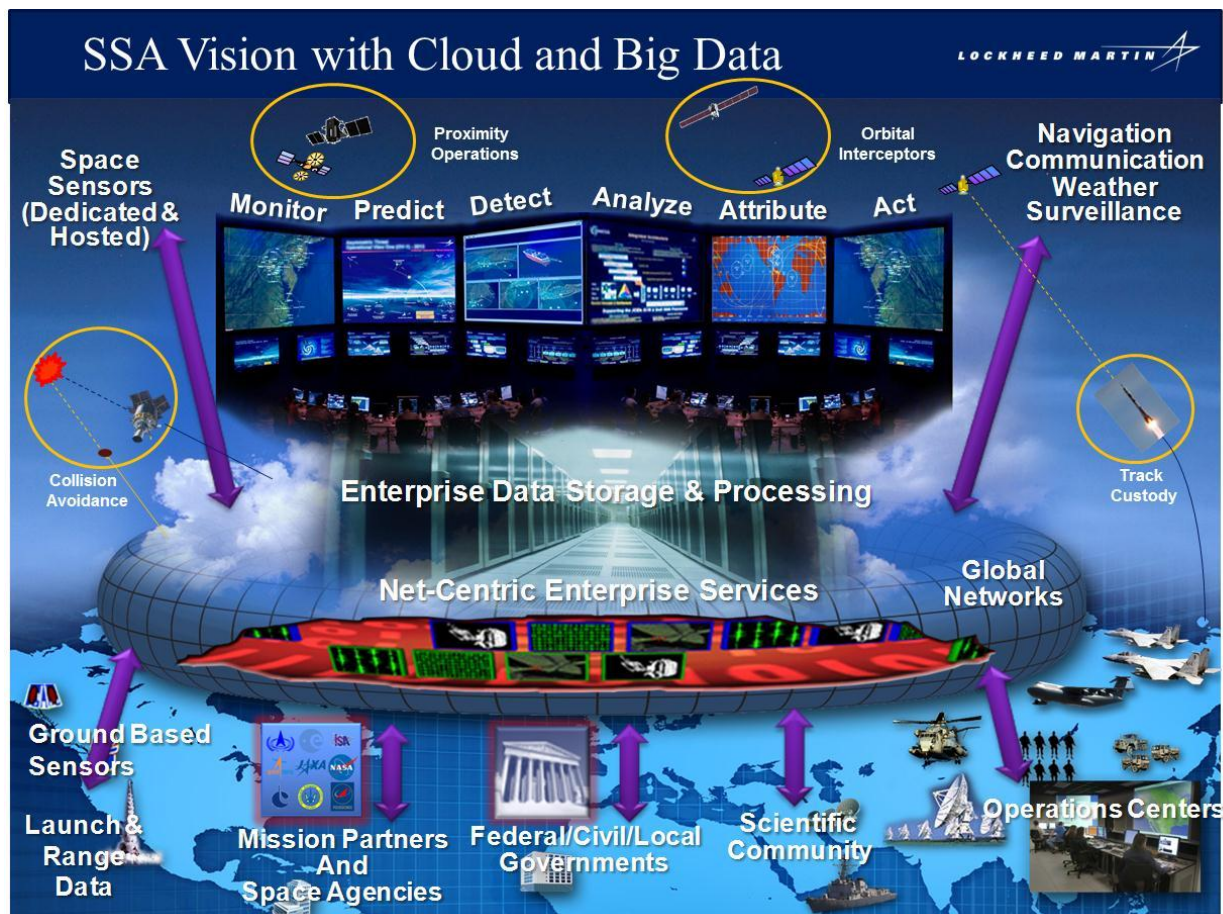


Fig. 6 "To-Be" Vision

6. BENEFITS OF FUTURE APPROACH

Existing traditional and non-traditional data sources are evolving from stove piped connections to net-centric data exchanges. This makes secondary data not currently transmitted available for SSA. Additionally, the new data structures allow the transmission of greater precision improving the quality of information exchanged.

Utilizing a common lexicon and agreed to data schemas will facilitate clients ability to understand and use the data. Thus, clients outside of the traditional set (Joint Space Operations Center) can quickly gain access and understand the available data enabling innovation of new usages for the existing data. Exposing available data sources net-centrally versus developing new sources will make necessary data available to clients faster.

Exposing this data net-centrally will facilitate getting space situational awareness data into cloud computing architectures. As this data becomes available net-centrally, new and innovative uses will provide mission utility. Big Data techniques will address the increasing data volumes and the rapid velocity of the data to provide innovative mission utility tools. Replicating the data over multiple Regional Gateways will improve the overall survivability of the system.

Non-technical, as well as technical challenges are being addressed to ensure data availability.

7. PATH FORWARD – GOVERNANCE AND OVERSIGHT

The efforts to expose the data net-centrally need to continue. Additional data sources are needed to characterize and attribute space events. This will require continued work within the SSA COI to define the usable data structures.

Developers will need to continue to produce innovative tools from this data. A governance process is necessary to evaluate these products and provide a path for incorporation into the operational JMS baseline.

8. CONCLUSION

The enterprise is moving from stove-piped systems to a collection of net-centric systems. Over time this transition will support a large variety of space protection stake-holders with differing needs. Establishing common architecture components deployed as a service in a Cloud will reduce both development and sustainment costs of multiple programs.

Existing data sources contain untapped information. Net-centric data exposure techniques will make this data available versus developing new data sources. Non-technical, as well as technical challenges are being addressed to ensure this data will become available. The common lexicons and data models facilitate data understanding between disparate development teams. Thus, overall development costs are reduced.

Big Data frameworks are available for usage in new and innovative ways to provide mission utility. Web Services exposing data net-centrally, Cloud Computing, and Big Data are synergistic technologies that can work together to provide the future SSA Architecture vision.

9. REFERENCES

1. Hutchinson, M., *The JSpOC Mission System (JMS) Common Data Model: Foundation for Net-Centric Interoperability for Space Situational Awareness*, The Aerospace Corporation, Colorado Springs, CO, 12 Sep 2012.
2. Richmond, David, 2012 AMOS Conference paper, *Net-Centric Sensors and Data Sources (N-CSDS) Ground-based Electro Optical Deep Space Surveillance (GEODSS) Sidecar*, Lockheed Martin Corporation, Valley Forge, PA, 12 Sep 2012.
3. National Institute of Standards and Technology (NIST), *Big Data Definitions, v1*, 17 Jan 2013 NIST Cloud/BigData Workshop
4. National Institute of Standards and Technology (NIST), *Cloud Computing Definitions, v1*, 17 Jan 2011 NIST Cloud Computing Workshop
5. Wasson, Mike, Colonel, Chief, Combat Operations Division, 614th Air and Space Operations Center, 2012 AMOS Conference paper, *Space Situational Awareness in the Joint Space Operations Center*, 12 Sep 2011.