An Investigation of Data Sharing for DoD DCO Forces

A Research Project for the Naval Information Warfare Center Internship Program

by

Sienne Rodwell

May 2023

Abstract

This report analyzes the status of DoD DCO data sharing. Data sharing in the cyber-defense industry is vital, as it allows for improved analysis of vulnerabilities and attacks, improving the cyber-defense of all parties involved and creating an environment that is more difficult to penetrate. Issues currently encountered in defensive cyber operation (DCO) data sharing as well as multiple proposed solutions are included in this report. This study intends to contribute to the general knowledge of DoD DCO data sharing and the availability of solutions for issues encountered. The issue addressed in this study is that DoD DCO forces do not have a standard way to share data and encounter interoperability issues. To assess this issue, a literature review and interviews were conducted. Limitations of this study include the classified nature of DCO environments and the extent of research being exclusively literature review and interviews. Proposed solutions and current DoD improvements, such as the CYBEX-P platform, blockchain-based platforms, decision tree algorithm-based platforms, the Big Data Platform (BDP), and common information modeling are addressed. It was found that while the integration of a new, consolidated platform may be feasible for private sector cyber defense, it is unlikely to succeed in a government/DCO environment. This study found that the DoD is implementing a "responsibility to provide" data sharing culture, the BDP, and is working on integrating common information modeling. Common information modeling could address issues encountered by DCO forces while still maintaining requirements specific to their environments and allowing for integration into the BDP. It is recommended that common information modeling for DCO forces be expanded and pursued.

Table of Contents

An Investigation of Data Sharing for DoD DCO Forces i

Section 1: Introduction 1

Problem Statement 1

Study Purpose 1

Research Question 2

Significance of the Study 2

Definition of Terms 2

Section 2: Review of the Literature 4

Literature Search Strategies 4

DoD Intent 4

Current Methods 5

Issues with Current Tools and Perceived Barriers 5

The CYBEX-P Platform 6

The Blockchain Platform 7

Decision Tree Algorithm 8

Common Information Model 8

Conclusions 9

Section Summary 10

Section 3: Findings 11

Introduction 11

Results 11

Discussion of Study Findings 15

Section Summary 16

Section 4: Discussion and Conclusions 17

Limitations of Study Findings 17

Interpretation of Study Findings 17

Practice Implications of Study Findings 18

Recommendations for Further Research 19

Conclusion 19

References 20

Section 1: Introduction

Cyber threats are consistently increasing due to elevated motivations, funding, techniques, tactics, and procedures (Abu et al., 2018). In light of this ever-increasing threat, cyber defense forces must be provided with the appropriate tools and cyber threat information (CTI) to perform well (Katos et al., 2020). The DoD acknowledges that their previously ubiquitous policy of "need to know" information sharing will not provide the appropriate data for defense cyber operations to perform at the level necessary and intends to shift to a "responsibility to provide" data sharing culture (DoD, 2020). Currently, the DoD data-sharing techniques are primitive and many issues such as interoperability, redundancy, the scope of capability for current tools, manning, and security are widespread (Castillo, 2020). However, the issues experienced by DoD forces are not isolated and greatly impact the private sector as well (Goethals et al., 2019).

Problem Statement

The problem is that the DoD has yet to create a standard for data sharing across DCO forces (Castillo, 2020). Modern Cyber Criminals are becoming increasingly difficult to combat on account of improved techniques, tactics, and procedures (TTPs), as well as increased persistence, motivation, organization, and funding (Abu et al, 2018). To effectively combat these criminal forces, data such as "security log entries and alerts, reports, and other intelligent information" must be shared across cybersecurity organizations (Katos et al, 2020). Despite the understood benefits and necessity, successful cybersecurity information sharing has been unachievable thus far (Simpson et al, 2019).

Study Purpose

The purpose of this study is to evaluate the status of DoD DCO data sharing and identify what is needed to improve data sharing across DCO forces. The goal of the DoD is to create a data-sharing environment and culture in which data is visible, accessible, understandable, linked, trustworthy, interoperable, and secure (DoD, 2020). This study will conduct a literature review of previous research

on data sharing across different organizations. Intended contributions to professional practice and scholarship include an evaluation of the status of DCO data sharing as well as possible ways to integrate a unified data-sharing platform.

Research Question

The question addressed in this study is: What are some ways in which the DoD could securely standardize data sharing across its DCO forces?

Significance of the Study

This study serves as a consolidated information base for issues as well as possible solutions for cyber threat information sharing following the DoD's intent. This study contributes to current scholarship by providing a summary of DoD intent, current issues, and perceived barriers, as well as an analysis of some of the currently proposed solutions. It is intended that this study be used to inform the reader of the status of cyber threat information sharing regarding both the issues experienced ubiquitously across cyber defense fields as well as solutions that could be implemented or expanded upon to contribute to defense against increasing cyber-attacks.

Definition of Terms

In this section, terms relevant to the theme of cyber defense are introduced. Fields such as DoD intent, the current state of cyber defense operations, threat data sharing implications, and current scholarship in threat data platforms are the focus of this study, which is to be reflected in the definition of terms. While this is not a comprehensive list of terms relevant to the aforementioned fields, this list is intended to encompass all necessary terms that appear in this study.

Program of Record (POR)

This term is frequently used to describe an organization in generality, usually in the context of an organization that works with others to some degree (Castillo, 2020).

Defensive Cyber Operations (DCO)

The DoD defines DCO as "missions to preserve the ability to utilize (friendly) cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent malicious cyberspace activity" (DoD, 2018).

Threat Intelligence Sharing Platform (TISP)

This term is used for data platform solutions for the sharing of threat intelligence offered by a variety of security vendors (Abu et al., 2018).

Common Information Model (CIM)

Common Information Models are used to provide a "common definition of management information for systems, networks, applications, and services" Common information models often also allow for vendor extensions. (DMTF, 2023).

Section Summary

This section contains an introduction, problem statement, study purpose, research question, study significance, and definition of terms relevant to the remainder of this report. The focus of this report is data-sharing status awareness, issues, and possible solutions. The problem statement, research question, and study significance will be used to shape the contents of the literature review.

Section 2: Review of the Literature

In not having a standardized data-sharing platform, the DoD encounters many issues including accessibility, scalability, and security of data (Castillo, 2020). The purpose of this study is to investigate ways the DoD could create better data sharing for its DCO forces using a common information model allowing for the integration of various tools currently used across organizations.

In this literature review, the intent of the DoD, the current status of tools and information sharing, and proposed solutions will be evaluated to provide a consolidated knowledge base on the available options for the DoD to improve their data-sharing environment for DCO forces in coordination with their intent and current state.

Literature Search Strategies

To attain the literature for this section, the University of Hawaii (UH) Manoa and Google Scholar databases were the primary search mechanisms. Using these databases, many sources such as the Institute of Electronical and Electronics Engineers (IEEE) explore, Association for Computing Machinery (ACM) conferences, DoD Executive Summaries, and a range of postgraduate studies were incorporated. Keywords and phrases used in the acquisition of these sources include “DoD data sharing”, “big data security”, “data sharing”, “DoD data sharing DCO forces”, and “cybersecurity information sharing”.

Through the above, a great number of issues as well as possible solutions were revealed. This literature review will evaluate the intent and goals of the DoD, the status of tools used and information sharing, current issues, perceived barriers for information sharing, the CYBEX framework, blockchain framework, a decision tree algorithm-based data sharing platform, and how to integrate various tools used across organizations using a common information model.

DoD Intent

Historically, the information culture of the DoD has been “need to know” (DoD, 2020). This means that regardless of clearance, information was made accessible only if the mission on which

someone was working was directly related to that information. In their Executive Summary: DoD Data Strategy 2020 publication, the DoD indicated that they intended to shift to a "responsibility to provide" culture. Currently, the DoD does not have the appropriate mechanisms in place to create a seamless data-sharing culture, however, DoD intends to move promptly in that direction (DoD, 2020). Despite this, the DoD data strategy publication repeatedly stresses that data sharing is key in successful modern warfighting, stating their goals were to make DoD data visible, accessible, understandable, linked, trustworthy, interoperable, and secure. To accomplish these goals, the DoD needs to improve its abilities in effective data management (DoD, 2020). The progress of the DoD with respect to ensuring that its personnel have access to real-time, usable, secure, and linked data is lacking (DoD, 2020).

Current Methods

As there is no standardized data-sharing platform, most DCO operations use decentralized tools available to everyone (Castillo, 2020). In conducting visits to most major Naval Intelligence operations, it was found that information sharing relies heavily on updates via interpersonal methods, such as chats, briefs, and telephone (Castillo, 2020). In surveying these DCO operations, it was found that there was a wide array of tools used (Castillo, 2020). These include but are not limited to SPLUNK, Forescout, NETSCOUT, MADSS, Tanium, and SHARKCAGE (Castillo, 2020). In addition to these tools, the DoD is also implementing a Big Data Platform (BDP) as well as Elastic (Edings et al., 2022 and Walton, 2021). Not only do DCO forces currently use a large array of different tools for each task, but there are also many different software platforms that are used to achieve the same goal across different commands, creating interoperability barriers (Castillo, 2020).

Issues with Current Tools and Perceived Barriers

Most of the tools currently used are incomplete, as they can provide near real-time data sharing in a limited scope, causing great detriment to effective information sharing (Castillo, 2020). Many different tools are used to accomplish the same task across different DCO forces (Castillo, 2020). As

there are so many different tools used by DoD DCO forces, it is difficult for DCO forces to provide data to the DoD BDP, because the data used exists in a variety of different formats (Arnold, C., personal communication, 24 Feb. 2023). In addition to stating issues specific to each tool, Castillo (2020) also states issues that affect DCO forces in generality, such as poor manning, using many different tools to accomplish the same goal, accessibility of requested tools, poor interoperability, and difficulties caused by contracting complications, such as delays in network operations vital to security, information sharing, and near real-time awareness. The DoD also encounters basic operability issues when using commercial tools, as the DoD has a larger range of data types and usages not usually accounted for in commercial tools (Ritchey, P., personal communication, 1 Mar. 2023).

Many issues facing DCO forces are also shared in the private sector and current research fields. The volume of data needed, cloud computing complications, and communications networking issues are challenging every field of cyber forensics (Goethals et al., 2019). In a survey study, it was found that the majority agreed with the statement “Standardization issues continue to hinder threat intelligence sharing” (Simpson et al., 2019). In general, the community's attitude toward information sharing is that it is too cumbersome of a task to undertake (Simpson et al., 2019). In examining Threat Intelligence Sharing Platforms (TISP), the themes of issues are threat data overload, threat data quality, privacy and legal issues, and interoperability (Abu et al., 2018). Furthermore, interoperability is often restricted by data quality and verification issues (Katos et al, 2020).

The CYBEX-P Platform

A suggested solution for the data sharing issue is the CYBEX-P framework. CYBEX-P uses a two-step privacy handling mechanism, blind processing, and “other trusted computing paradigms” to create an information-sharing platform that supports real-time threat data sharing and prevents the spread of new malware (Bakhshaliyev, et al., 2019). This platform collects heterogeneous threat data and organizes it to provide reports (Sadique et al., 2021). CYBEX-P is based on a mutual value policy,

meaning users must contribute their data to access the data of others (Cassel et al., 2021). CYBEX-P organizes data into four different levels of sensitivity, allowing for the sharing of threat data without including private information (Bakhshaliyev et al., 2019). Furthermore, the instantaneous sharing of threat indicators makes it difficult to create new attack patterns (Bakhshaliyev et al., 2019). To tackle the issue of large data-set analysis, CYBEX-P is designed to be easily integrated with machine learning, which also results in better performance with zero-day attacks (Bakhshaliyev et al., 2019). The main shortfall of CYBEX-P is that the machine-learning algorithm is only as good as the training dataset (Bakhshaliyev et al., 2019), however, this machine-learning algorithm has already improved and can detect phishing URLS that have been previously unseen with an accuracy of 86% (Sadique et al., 2021). Unlike many other threat-sharing platforms, CYBEX-P has its own indexable threat data query language, TAHOE, that allows for advanced analysis of large volumes of threat data, allowing for both threat data sharing and analysis on the same platform (Sadique et al., 2021). Additionally, CYBEX-P has a well-developed user interface, allowing for advanced threat data visualization that was not previously possible (Cassel et al., 2021). There is work being done to make CYBEX-P horizontally scalable, facilitating large-scale implementation (Bakhshaliyev et al., 2019).

The Blockchain Platform

The iShare Framework is one example of an information-sharing framework using the Blockchain concept that has become well-known for its role in Bitcoin's security (Kamhoua et al., 2018). With the iShare framework, information is anonymized and summaries and solutions are shared with others (Kamhoua et al., 2018). The iShare framework enhances data integrity, protects privacy, and eliminates the need for third-party security using a trusted auditable public ledger (Kamhoua et al., 2018). One of the appeals of the iShare framework is that users can control their data, and never lose ownership of it (Kamhoua et al., 2018). Other strengths of Blockchain based information sharing frameworks include good scalability, anonymity, and data integrity (Baek et al, 2018). The main

vulnerabilities of blockchain frameworks are double spending (aka race attacks), data storage, and publicly available transaction ledgers, which allow for transaction patterns to be observed and potentially linked to a user identity (Baek et al., 2018). Many of the blockchain framework weaknesses will be greatly reduced or eliminated with present and future AI capabilities (Baek et al., 2018).

Decision Tree Algorithm

While much work has been done with decision tree algorithms for cybersecurity, currently, Badsha et al. (2019) are the only ones to implement it into an original data-sharing platform. Badsha et al. (2019), suggest a privacy-preserving cyber threat information-sharing platform based on a decision tree algorithm. In this platform, homomorphic encryption is used to encrypt data before sharing (Badsha et al., 2019). The resulting ciphertexts are then sent to a central server, which finds the encrypted results and sends the information back to participating organizations without learning the organization's private information (Badsha et al., 2019). The decision tree algorithm categorizes information based on the path it had to take to get there (Badsha et al., 2019). The encryption (done individually before sharing) uses one public key (shared only with the central server, which does not learn anything other than ciphertext material) and one private key (Badsha et al., 2019). Throughout the process, none of the secret keys are disclosed to any other party, and decryption is performed locally by the organizations, which creates a secure sharing environment (Badsha et al., 2019). The protocol presented addresses the common industry challenge of learning the decision tree without disclosing private information to other parties (Badsha et al., 2019). In the future, there is potential for this protocol to become an unsupervised machine learning algorithm, allowing data sharing while maintaining the same privacy with minimal human oversight (Badsha et al., 2019).

Common Information Model

While it is not a data-sharing platform, a CIM defines a set of standards to increase interoperability through a set of rules and standards that allow for data sharing across organizations

(DMTF, 2023). A CIM can be used for data transport and does not include data storage capabilities (Ritchey, P., personal communication, 13 Mar. 2023). Many search tools, such as SPLUNK and Elastic, have a CIM or common schema built in, even allowing for customizability (Mathieu et al., 2019 and SPLUNK, 2022). These CIMs allow data to be stored in a common format (Ritchey P., personal communication, 13 Mar. 2023). CIMs can collect data from a wide variety of tools to create a uniform search platform (Mathieu et al., 2019). Common schemas for information modeling can collect data from disparate data types, such as logs, metrics, and contextual data, heterogeneous environments with differing vendor standards, and similar-but-different data sources, including tools that create multiple sources of endpoint data, such as Tanium (Mathieu et al., 2019). Common information models allow for the consolidation of various data types from multiple types of sources (DMTF, 2023). Industry standards for common information models provide the ability for each organization to create a CIM specific to their needs, while still ensuring interoperability in data sharing (Krishnan, 2021).

Conclusions

Cybercriminals are becoming advanced in their techniques, tactics, and procedures making them increasingly difficult to detect and combat (Abu et al., 2018). Considering the advancements of cybercriminals and augmented data requirements needed to combat them, the DoD intends to shift to a “responsibility to provide” data-sharing culture (DoD, 2020). Currently, DCO forces are experiencing a variety of issues regarding data sharing, namely interoperability challenges with current tools (Castillo, 2020). There have been a variety of proposed solutions, including CYBEX-P, iShare blockchain framework, a decision tree algorithm-based platform, and common information modeling. Despite the understood need, the DoD has yet to implement a standard for data sharing across its DCO forces (Castillo, 2020).

Section Summary

This literature review was conducted using keywords such as “DoD data sharing”, “big data security”, “data sharing”, “DoD data sharing DCO forces”, and “cybersecurity information sharing”. The UH Manoa Database and Google Scholar were the main databases used. After narrowing scholarly articles for applicability, the subtopics that emerged during the research were DoD intent, current tools, issues with current tools and perceived barriers, and suggested solutions. The information included in this literature review will be used in support of later sections of this paper. The remaining sections of the paper will focus mostly on how a common information model could be used to share data in coordination with DoD intent as well as current tools used by the DoD.

Section 3: Findings

Introduction

The purpose of this study is to assess the status of DoD DCO data sharing regarding DoD intent, issues, and possible solutions. The problem is that there is no DoD standard for data sharing across DCO forces (Castillo, 2020). In this section, the findings resulting from the literature review are included.

Results

DoD Intent

It was found that the DoD intends to move away from a "need to know" and towards a "responsibility to provide" data-sharing culture (DoD, 2020).

Figure 1

Modernization Strategy Alignment with National and DoD Guidance

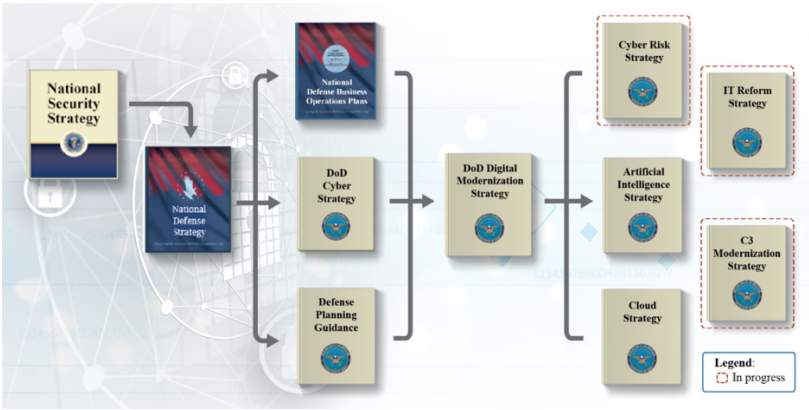


Figure 1 shows the DoD modernization strategy in accordance with the four sub-strategies and the DoD CIO priorities (DoD, 2019). The DoD highly prioritizes the modernization of its cyber forces, including DCO, as a matter of national security (DoD, 2019).

Current Tools and Issues

The DoD DCO forces are spread across the globe in many different commands (Castillo, 2020).

Figure 2

NCTAMS PAC Area of Responsibility

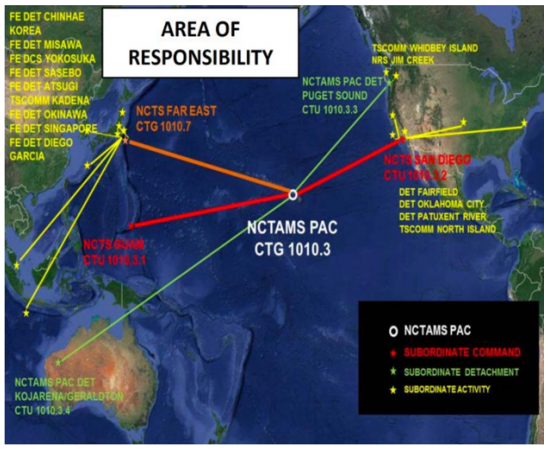
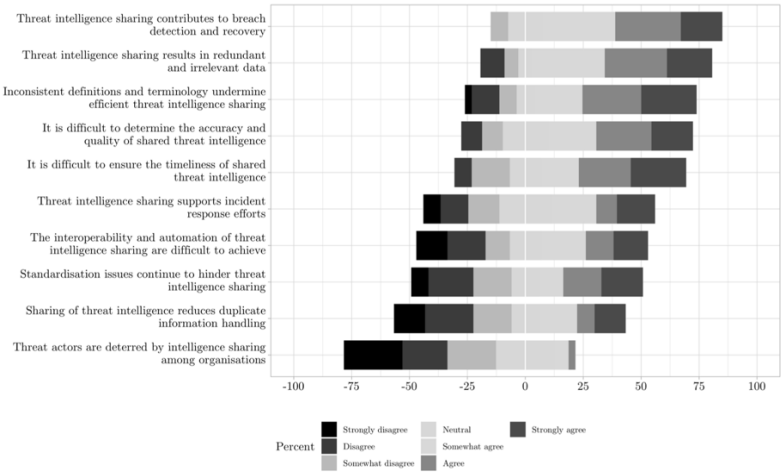


Figure 2 shows the area of responsibility of the NCTAMS PAC (Castillo, 2020). Each DCO force must communicate and share data with many others (Castillo, 2020). Despite the need for efficient communications, there are currently a wide variety of tools used by DCO forces to accomplish the same task, often differing from command to command (Castillo, 2020). This causes considerable issues in interoperability (Castillo, 2020).

The issues that affect DoD DCO forces are ubiquitous across the data-sharing industry (Goethals et al., 2019). In addition to the technical issues encountered, it was found that there were complications in the industry's attitude toward data sharing (Simpson et al., 2019).

Figure 3

Respondent's Attitudes Towards Cyber Threat Information Sharing Benefits and Barriers



The issues that affect DoD DCO forces are ubiquitous across the data-sharing industry (Goethals et al., 2019). Figure 3 shows that in addition to the technical issues encountered, it was found that there were variations in the industry's attitude toward data sharing (Simpson et al., 2019). Figure 3 shows the results of surveying industry professionals on threat data sharing (Simpson et al., 2019). The consensus among participants is that while there may be some benefits, implementing data sharing to be more helpful than harmful is unfeasible (Simpson et al., 2019). Furthermore, the integration of data-sharing capabilities is greatly impeded by the organization's lack of ability to work cohesively (Ritchey, P., personal communication, 13 Mar. 2023).

Suggested Solutions

Copious proposed solutions to the data sharing issue were found. These include the CYBEX-P platform, the iShare blockchain platform, and the decision tree algorithm-based platform.

The CYBEX-P platform organizes data into 4 different levels of sensitivity, allowing for graduated security and access parameters (Bakshaliyev et al., 2019). This platform is easily integrated with machine learning algorithms, allowing for less analysis requirements (Sadique et al., 2021). This platform also includes its own cyber-threat language, TAHOE, allowing for the analysis of large volumes of threat data (Sadique et al., 2021).

The iShare blockchain-based framework allows for the sharing of anonymized summaries and solution data (Kamhoua et al., 2018). The strengths of the iShare framework are that it eliminates the need for third-party security, users can control and own their data, and has good scalability, anonymity, and data integrity (Kamhoua et al., 2018, and Baek et al., 2018). With future work in AI, many of the blockchain vulnerabilities like double spending attacks, data storage, and transaction pattern tracking are likely to diminish or be eliminated (Baek et al., 2018).

The decision tree-based information-sharing platform proposed by Badsha et al.,(2019), is highly secure and categorized with potential improvements leading to minimal oversight in a large data-sharing environment (Badsha et al., 2019).

The DoD is currently integrating a big data platform, BDP (Edings et al., 2022). The intent of the BDP is the consolidation of data from various sources across government intelligence operations (Edings et al., 2022).

Figure 4

Big Data Platform Overview

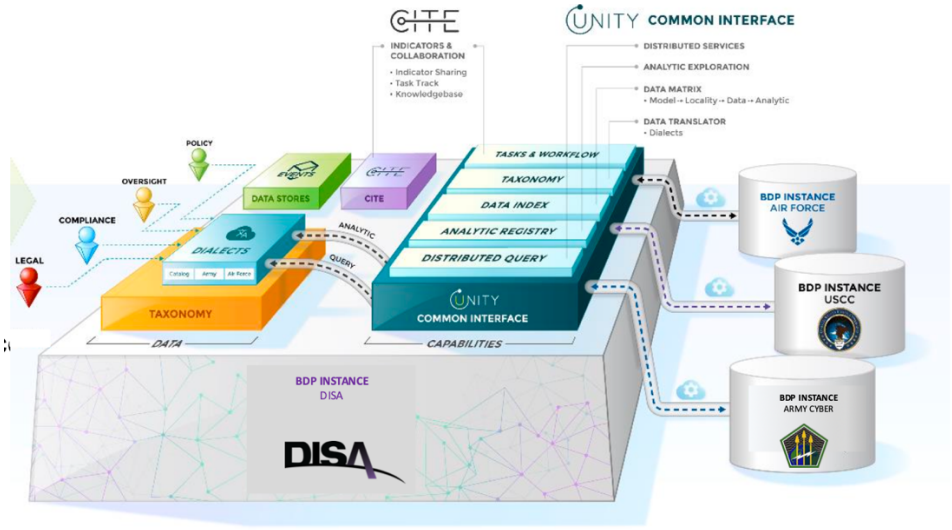


Figure 4 shows the intended implementation of the BDP (Edings et al., 2022). This platform is intended to be the main data hub of DoD information network sources and provide information sharing, DCO, and situational awareness abilities (Edings et al., 2022). While the implementation of the BDP is still in progress, it may encounter dependency issues due to its architectural complexity (Ritchey, P., personal communication, 13 Mar. 2023).

The DoD is also implementing Elastic to increase the accessibility and interoperability of data (Walton, 2021). Elastic has capabilities that address all eight guiding principles in the DoD data strategy

(Walton, 2021). Despite this, due to the wide variety of tools used across DCO forces, data sharing through Elastic and the BDP have yet to be successful (Castillo, 2020).

Common Information Modeling

Common information models are not platforms, but sets of standards defining management information for services, networks, applications, and systems (DMTF, 2023). Many tools used by the DoD, such as SPLUNK and Elastic, have common information models or schemas built in (Mathieu et al., 2019 and SPLUNK, 2022). Due to the uncommon data requirements of DCO forces, most tools are commercially available to not satisfy the needs of DCO forces (Ritchey, P., personal communication, 1 Mar. 2023). CIMs are highly customizable, and an organization can create its own to satisfy that organization's needs (Krishnan, 2021). A customized CIM could be used with the wide array of existing DCO tools to share data through Elastic and ultimately the BDP (Arnold, C., personal communication, 24 Feb. 2023). Currently, there is work being done to create and integrate CIMs for DCO use (Ritchey, P., personal communication, 13 Mar. 2023).

Discussion of Study Findings

The results found in this study are consistent with current scholarship. Data sharing challenges face not only DCO forces and the DoD but private sector organizations as well. Although there are many possible platform solutions in the private sector, many tools offered commercially do not fit the needs of DCO forces (Ritchey, P., personal communication, 1 Mar. 2023). The DoD is currently implementing a big data platform, BDP (Edings et al., 2022). DCO forces will need to export data through Elastic into the BDP (Arnold, C., personal communication, 24 Feb. 2023). Currently, DCO forces use a wide array of tools across different commands causing many interoperability issues (Castillo, 2020). Common information modeling allows for data from many different sources and tools to be consolidated using a common standard (Mathieu et al., 2019). Currently, there is work being done to integrate CIMs for DCO use (Ritchey, P., personal communication, 13 Mar. 2023). While some data-sharing tools have a common

information model or schema built-in, it is also possible for organizations to create their own, customized to suit their needs.

Section Summary

This section contains the findings of the literature review study. The findings include the current intent of the DoD, tools currently used by DCO forces, and the issues encountered as a result, as well as issues encountered with data sharing in the private sector. Platforms offering potential solutions were also found. It was found that the DoD is in the process of integrating a central data platform, the BDP, and is also implementing Elastic. Information regarding common information modeling and its applications was also found.

Section 4: Discussion and Conclusions

This section will present an analysis of the study findings and implications. The limitations of the study, interpretations of findings, implications of the findings, and recommendations for future work will be discussed. The purpose of this study is to evaluate DOD DCO data sharing and identify what is needed to improve data sharing across DCO forces. The problem addressed in this study is that the DOD has yet to create a standard for data sharing across DCO forces (Castillo, 2020).

Limitations of Study Findings

A limitation encountered in this study was the accessibility of information due to the classified nature of DoD DCO forces. While it was possible to attain general information regarding DOD data sharing and DCO operations, the exact intricacies and limitations in these fields are not available to the public. A second limitation was the scope of research. This study was conducted solely through a literature review and interviews, and there was not an experiment specific to this study.

Interpretation of Study Findings

The DoD is in the process of a culture shift from “need to know” to “responsibility to provide” data sharing. In doing so, many issues have arisen, especially regarding DCO forces. This study found that interoperability is among the most considerable challenges faced by intelligence commands. While there are some tools that are commonly used, many commands use differing tools, causing data to be both presented and stored with formatting and methodology often unique to a specific command.

With some exceptions, it is accepted that data sharing is a vital part of DCO forces in both the government and private sectors. There have been many platforms created to attempt to resolve the issue of data sharing on a large scale. While these platforms may be effective in some private organizations, due to the differences in needs and environment of government cyber operations, they are unlikely to succeed in such a setting.

The DoD is in the process of implementing a central data repository known as the BDP. DCO forces will need to provide their data to the BDP. Currently, this process could prove to be quite disorganized and therefore largely unhelpful, as DCO forces each create and store their data differently. A potential solution that is currently being developed is data sharing through a CIM. This is not a data platform, so it would not require DCO forces to drastically change their day-to-day operations but would still allow for data sharing in a uniform way, enabling organizations to effectively access data from multiple sources. CIMs have already been successfully integrated in a wide range of organizations and can be manipulated to fit the specific needs of an organization.

Practice Implications of Study Findings

The problem is that the DoD has yet to standardize data sharing within DCO forces. While many platforms are providing proposed solutions to this data-sharing issue, there are a few reasons why their implementation for this purpose would be unlikely to succeed. It is difficult to create a tool that will integrate well with the specific needs of DoD DCO on account of the variation from private sector operations. This causes tools that would generally be implemented well in the private sector to encounter challenges when attempting to be integrated into a government environment.

DoD DCO forces already have tools that they use well and are accustomed to for daily operations, often varying in different commands, and it would be problematic to mandate a large-scale change to a uniform platform, not only on account of administrative challenges but also due to the training requirements for personnel. The integration of a CIM would circumvent these issues, allowing for use with current tools and minimal change in day-to-day operations. CIMs are adaptable and would allow DoD DCO forces to continue using the tools they have already integrated, without compromising the quality of data shared. The integration of a CIM is the most likely solution to the data sharing issue on account of its customizability and capacity to be used with a wide array of current tools.

Recommendations for Further Research

The advancement of CIM integration is highly recommended. The development and integration of a CIM or multiple CIMs for DoD DCO forces could greatly advance cyber defense capabilities. While there are many solutions available for private sector use, it is recommended that the DoD does a "ground-up" analysis of the needs for DCO. Often in government organizations, management, and technical fields are highly separated, causing operations issues or ideas for improvements to go largely unnoticed or ignored by those with the power to act upon them. The identification of issues and improvement ideas on every level is needed, as well as their analysis to create a coherent system able to be implemented with minimal difficulty.

Conclusion

It was found that the DoD is shifting into a "responsibility to provide" data-sharing culture. Data sharing for DCO forces is an integral contributor to their success. Despite this, the status of data sharing in DCO is primitive and disorganized. There are many platforms created to provide data-sharing capabilities, however, they are unlikely to succeed in a government environment on account of unique requirements. To circumvent the challenge of introducing a new platform and manipulating the daily operations of all DCO forces, a CIM could be integrated. With the integration of a CIM, data-sharing needs can be met, daily operations can remain largely unchanged, and DCO forces could still export their data into Elastic and the BDP per DoD requirements. It is recommended that the creation and integration of a CIM for DoD DCO be advanced.

References

Abu, M., Aswami, A., Selamat, S., Yusof, R. (2018). Cyber threat intelligence – issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science.* http://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Badsha, S., Sengupta, S., Vakilinia, I. (2019). Privacy preserving cyber threat information sharing and learning for cyber defense. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. https://doi.org/ 10.1109/CCWC.2019.8666477

Baek, U., Cho, K., Hasanova, H., Kim, M. (2018). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *Institute for Information and Communications Technology Promotion*. https://doi.org/10.1002/nem.2060

Bakhshaliyev, K., Sadique, F., Sengupta, S., Springer, J. (2019). A system architecture of cybersecurity information exchange with privacy (CYBEX-P). *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC).* https://doi.org/10.1109/CCWC.2019.8666600

Cassel, A., Dascalu, S., Sengupta, S. (2021). Navigating cyberthreat intelligence with CYBEX-P: dashboard design and user experience. *University of Nevada, Reno Proquest Dissertations Publishing*.

Castillo, E. (2020). Information sharing within the FLTCYBERCOM/C10F organization. *Naval Postgraduate School*. https://apps.dtic.mil/sti/pdfs/AD1114632.pdf

Distributed Management Task Force, DMTF. (2023). Common information model. *DMTF Standards – CIM. https://www.dmtf.org/standards/cim*

DoD. (2020). Executive summary: DoD data strategy, unleashing data to advance the national defense strategy. *Department of Defense Office of Prepublication and Security Review*. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

DoD. (2019). DoD digital modernization strategy. *DoD Information Resource Management FY 19-23.* https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

DoD. (2018). Joint publication 3-12: cyberspace operations. *Joint Publications Operation Series*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Edings, A., Steinbaum, D. (2022). BDP – Big data platform. *Defense Information System Agency*. https://disa.mil/-/media/Files/DISA/News/Events/TechNet-Cyber---April-2022/Big-Data-Platform.ashx

Goethals, P., Hunt, M. (2019). A review of scientific research in defensive cyberspace operation tools and technologies. *Journal of Cyber Security Technology*. https://doi.org/10.1080/23742917.2019.1601889

Kamhoua, C., Kwait, K., Njilla, L., Rawat, D. (2018). iShare blockchain-based privacy-aware multi-agent information sharing games for cybersecurity. *International Conference on Computing, Networking, and Communications: Communications and Information Security Symposium*. https://doi.org/10.3390/computers9010018

Katos, V., Kritsas, A., Ilioudis, C., Papanikolaou, A., Rantos, K. (2020). Interoperability challenges in the cybersecurity information sharing ecosystem. *Computers*. https://www.mdpi.com/2073-431X/9/1/18

Krishnan, P. (2021). How a common information model can help factories improve performance. *DIMOFAC EU*. https://dimofac.eu/2021/02/24/how-dimofac-common-information-model-helps-production-plants-share-manufacturing-information/

Mathieu, M., Settle, M. (2019). Introducing the elastic common schema. *Elastic Tech Topics*. https://www.elastic.co/blog/introducing-the-elastic-common-schema

Sadique, F., Sengupta, S. (2021). Cybersecurity information exchange with privacy (CYBEX-P) and TAHOE – a cyberthreat language. *University of Nevada, Reno Proquest Dissertations Publishing.*

Simpson, A., Zibak, A. (2019). Cyber threat information sharing: perceived benefits and barriers. *Proceedings of the 14th International Conference on Availability, Reliability, and Security*. https://doi.org/10.1145/3339252.3340528

SPLUNK. (2022). Overview of the splunk common information model. *Splunk Documentation.* https://docs.splunk.com/Documentation/CIM/5.1.0/User/Overview

Walton, W. (2021). Building a data-centric DoD starts with search. *Signal, Armed Forces Communications and Electronics Association International*. https://www.afcea.org/signal/resources/content/_SIE_Elastic_JUN21.pdf