Military Cyber Affairs

Volume 1 | Issue 1 Article 6

2015

Data to Decisions for Cyberspace Operations

Steve Stone
Robert Morris University, stonesw@cox.net

Data to Decisions for Cyberspace Operations

STEVE STONE, Robert Morris University; The MITRE Corporation

In 2011, the United States (U.S.) Department of Defense (DOD) named cyberspace a new operational domain. The cyberspace domain provides critical capabilities that enable the U.S. Military to conduct operations in all domains (Land, Sea, Air, Space, and Cyberspace). The U.S. Cyber Command and the Military Services are working to integrate the cyberspace domain with the other operational domains in order to conduct military command and control (C2) and achieve national security objectives. To effectively integrate cyberspace operations, DOD requires situational awareness of the Mission, Network, and Adversary based on analysis of operational data in order to make timely and effective decisions. However, the DOD's current capability to use data to make operational decisions does not meet mission needs within critical operational timelines. This paper discusses the data driven decision-making capabilities necessary to effectively conduct cyberspace operations and enable operations in all domains.

• **Cyberspace Operations, Big Data, Analytics, Decision Making; Command and Control; Military.**

1. INTRODUCTION

The growing use of cyberspace has reached the point where a wide range of social, political, informational, economic, and military activities are dependent on it and are vulnerable to both interruption of its use and usurpation of its capabilities.[1] The physical platforms, systems, and infrastructures that provide global connectivity to link information systems, networks, and human users with massive amounts of information that can be digitally sent anywhere, anytime, to almost anyone, have greatly increased access to information and has affected human cognition, dramatically impacting human behavior and decision making.[2]

The U.S. cannot conduct military operations without cyberspace. The DOD defines cyberspace as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[3] The U.S. Military depends on cyberspace to defend the nation, conduct global military operations, and command and control its military forces. The Commander of U.S. Cyber Command stated, "As cyberspace has grown and become more pervasive, military art has changed. No one today can exert or maintain national power without acute sensitivity to the digital networks that underpin the world's communications, prosperity, and security".[4]

1.1 Cyberspace Operations

In 2015, the Department of Defense (DOD) published two documents describing the U.S. strategy for conducting operations in cyberspace: *The DOD Cyber Strategy* and *Beyond the Build - Delivering Outcomes Through Cyberspace: The Commanders' Vision and Guidance for US Cyber Command*. Both documents describe the DOD's mission in cyberspace, "Our mission in cyberspace is to deter or defeat strategic threats to US interests and infrastructure, provide mission assurance for the operation and defense of the Department of Defense information environment, and support the achievement of joint force commander objectives."[5]

---

[1] Kuehl, D.T., (2009), "From cyberspace to cyberpower: Defining the problem," in *Cyberpower and national security*, ed. Kramer, F. D., Wentz, L.K. & Starr, S. H. (Dulles, VA: Potomac Books, Inc., 2009).

[2] Ibid.

[3] U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. (2014). Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[4] U.S. Department of Defense. Beyond the build - Delivering outcomes through cyberspace: The Commanders' vision and guidance for US Cyber Command. Fort Meade, MD: United States Cyber Command, 2015). 2.

[5] Ibid, 2.

In order to effectively conduct cyberspace operations in support of national security and military operations, in 2009 the Secretary of Defense directed the establishment of U.S. Cyber Command.[6] In 2011, the DOD named cyberspace a new operational domain.[7] And in 2013, the DOD published Joint Publication 3-12, *Cyberspace Operations*.[8] This document describes how the DOD defines cyberspace operations and how it intends to conduct military operations in cyberspace to support operations in the other operational domains. The DOD defines cyberspace operations as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace".[9] The DOD describes two cyberspace objectives relevant to the conduct of military operations as providing freedom of maneuver in cyberspace and projecting power in and through cyberspace to achieve campaign objectives.[10]

There are three categories of cyberspace operations for attaining these objectives: DOD information network (DODIN) operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO).[11] DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation. Defensive cyberspace operations are intended to defend DOD or other friendly cyberspace. And offensive cyberspace operations are intended to project power by the application of force in and through cyberspace. [12]

In 2012, the DOD began to create a new force, the Cyber Mission Force (CMF), to conduct DOD's cyber mission.[13] The DOD also began to integrate the CMF into the larger multi-mission U.S. military force to achieve synergy across all operational domains.[14] The Commander of US Cyber Command stated, "Our task is to make this domain understood by other warfighters and integrated into broader military and governmental operations while providing decision makers and operational commanders with a wider range of options while resources are constrained and threats are growing".[15] As part of integrating cyberspace operations to support full spectrum military operations and to ensure unity of effort, the DOD is developing the capability to enable combatant commands to plan and synchronize cyber operations with kinetic operations across all domains of military operations.[16] The former Director of Operations (J-3) for US Cyber Command has stated: "Commanders must develop the same capability to direct operations in the cyber domain since mission success increasingly depends on freedom of maneuver in cyberspace. The preeminent JFC[17] requirement for freedom of maneuver in cyberspace is command and control (C2). It is impossible to fully employ today's joint force without leveraging cyberspace".[18]

1.2 Command and Control of Cyberspace Operations

The United States Department of Defense has a large body of organizational design documentation that describes how the U.S. military is organized and functions. The U.S. military's term to describe its organizational design and decision-making process is Command and Control. The DOD defines Command and Control as "The exercise of authority and direction by a properly designated

---

[6] U.S. Department of Defense, *Establishment of a subordinate unified U.S. cyber command under U.S. strategic command for military cyberspace operations*. (Jun 23, 2009). Retrieved from: http://online.wsj.com/public/resources/documents/OSD05914.pdf.

[7] Williams, B.T. "The joint force commander's guide to cyberspace operations," *Joint Force Quarterly*, 73 (2014), 12-19.

[8] U.S. Department of Defense. *Joint Publication 3-12(R): Cyberspace operations*. (2013). Retrieved from: www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[9] Ibid. I-1.

[10] Ibid.

[11] Williams, The Joint Force Commander's Guide.

[12] U.S. DOD, Cyberspace Operations.

[13] U.S. Department of Defense. *The Department of Defense Cyber Strategy*. (2015). Retrieved from: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[14] U.S. Department of Defense. The Department of Defense Cyber Strategy.

[15] U.S. Department of Defense. Beyond the build - Delivering outcomes through cyberspace, 2-3.

[16] U.S. Department of Defense, The Department of Defense Cyber Strategy.

[17] Joint Force Commander

[18] Williams, *The Joint Force Commander's Guide*.

commander over assigned and attached forces in the accomplishment of the mission. Also called C2."[19] Because military operations involve large organizations consisting of subordinate organizations distributed in a hierarchical manner, the DOD has also defined Command Relationships to describe the authorities assigned to commanders at different levels and to describe the decision–making relationships between those commanders. In DOD doctrine Command relationships are "The interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command."[20]

The U.S. Military's C2 doctrine, including decision-making processes, has been developed and refined over years of military operations in the industrial age. However, the environment in which the DOD operates has been changed by the rapid development and adoption of information technologies and there is debate as to whether the established decision-making processes will be effective in the information age. The Commander of United States Cyber Command has described the challenge facing command and control of cyberspace operations as, "Our traditional command and control and organizational constructs do not enable the speed and agility required to keep pace with change in the cyber domain".[21] The speed of operating in the cyberspace domain is challenging the DOD's normal decision-making methods. "A cyber attack can happen on a temporal scale that is so brief that it precludes human comprehension, analysis and intervention."[22]

Hoffman describes organizational design as, "the relatively enduring allocation of work roles and administrative mechanisms that creates a pattern of interrelated work activities and allows the organizations to conduct, coordinate, and control its work activities".[23] One of the primary dimensions of organizational design is the decision making structure. Hoffman states that the "Decision making structure involves the centralization and decentralization of decision making. Organizational decision-making has been formally defined as being the process of identifying and solving problems within organizations".[24] The performance of an organization is determined, at least partially, by how well problems are identified and solved. Thus, an organization's decision-making structure is one of the most critical areas of the organization's design.[25]

Dr. David Alberts and Dr. Richard Hayes hypothesize that complex dynamic environments, like cyberspace operations, require more agile approaches to C2.[26] They define C2 agility as, "Agility is the synergistic combination of robustness, resilience, responsiveness, flexibility, innovation, and adaptation. Each of these attributes of agility contributes to the ability of an entity (a person, an organization, a coalition, an approach to command and control, a system, or a process) to be effective in the face of a dynamic situation, unexpected circumstances, or sustaining damage."[27] Alberts and Hayes also describe the value of agile decision-making as "All things being equal, agile decisions (those that work in the face of changes in circumstances) are preferred to decisions that are brittle and will only work well if the situation is as understood and anticipated." [28]

---

[19] U.S. Department of Defense, Joint *publication 1-02*, 44.

[20] Ibid. 46.

[21] U.S. DOD, *Beyond the Build*, 2.

[22] Henderson, S., Hoffman, R., Bunch, L., and Bradshaw, J., "Applying the Principles of Magic and the Concepts of Macrocognition to Counter-Deception in Cyber Operations" (paper presented at the 12th International Naturalistic Decision Making Conference, McLean VA, June 9 - 12, 2015), 1.

[23] Hoffman, J., "The effects of strategic and operational decision making structure on organizational performance: Technology as a moderator" (PhD diss., University of Nebraska, 1998), 6. Available from ProQuest Dissertations and Theses database. (UMI No. 8818630).

[24] Ibid. 6-7.

[25] Ibid.

[26] Alberts, D. S., & Hayes, R. E., *Understanding command and control*. (Washington DC: Office Of The Assistant Secretary Of Defense For Networks And Information Integration, Command Control Research Program, 2006). Retrieved from http://www.dodccrp.org/files/Alberts_UC2.pdf.

[27] Alberts, D. S., *Agility, focus, and convergence: The future of command and control* (Washington DC: Office Of The Assistant Secretary Of Defense For Networks And Information Integration, Command Control Research Program, 2007), 23. Retrieved from http://www.dodccrp.org/html4/journal_main.html.

[28] Alberts, D. S., & Hayes, R. E., *Understanding command and control*. 148

Alberts argues that the traditional DOD C2 approach is no longer sufficient for military operations in the information age. Alberts also argues that the United States military and its allies must actively consider new approaches to how authorities are allocated and decisions are made in the future. Alberts states, "The need to think about new approaches is driven by: (1) the nature of operations and the environment in which they are undertaken; (2) the capabilities of adversaries; and (3) opportunities provided by advances in technology, particularly information technologies."[29]

Alberts and Hayes describe three dimensions of a theoretical model (see Figure 1) of C2 or, in civilian parlance, organizational culture that is useful in this discussion:

1. The organization's allocation of decision rights.
2. The organization's patterns of interaction.
3. The organization's distribution of information.

This theoretical model of command and control can be visualized as a three-dimensional matrix, with each factor represented as one axis of the cube. Alberts describes the model as having the allocations of decision rights on the horizontal, X-axis, the pattern of organizational interaction on the vertical Y-axis, and the distribution of information along the depth, Z-axis. The inside of the cube represents the sample of all possible command and control arrangements. Any approach to accomplishing command and control of a military operation requires making a choice in each of the three related dimensions.[30] Alberts and Hayes hypothesize that agile C2 requires the organizational ability to rapidly change their approach towards each of the three variables in the theoretical model of C2.[31]

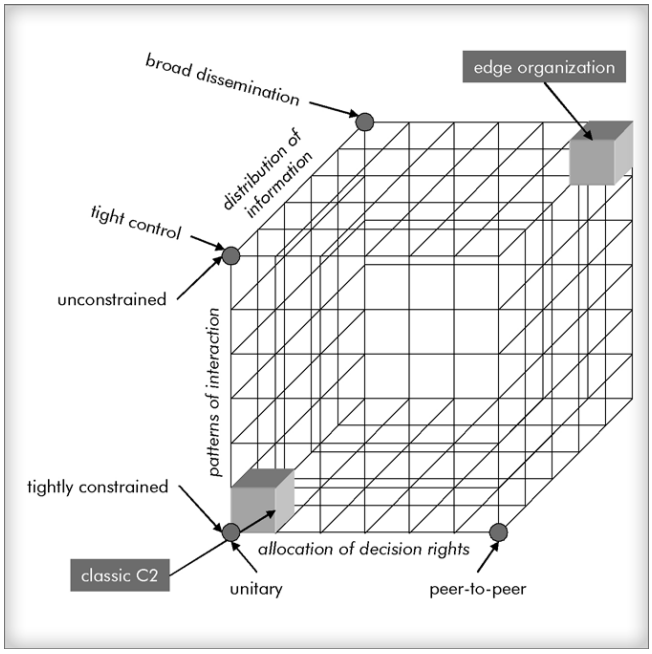

Figure 1. Model of command and control[32]

1.3 Allocation of Decision Rights

The allocation of decision rights is a linear dimension with two logical endpoints. At the origin of the allocation of decision-making rights on the horizontal axis, decision-making rights are unitary, all the rights held by a single actor. At the other end of the axis, decision-making rights are allocated uniformly with every entity having equal rights in every decision.[33] Decisions are choices among

[29] Alberts, D. S., *Agility, focus, and convergence: The future of command and control*, 7.
[30] Alberts & Hayes, *Understanding command and control.*
[31] Ibid.
[32] Reprinted from *Understanding Command and Control* by D.S. Alberts & R. E. Hayes, 2006, p. 75. Copyright 2006 by the Office Of The Assistant Secretary Of Defense For Networks And Information Integration, Command Control Research Program. Reprinted with permission.
[33] Alberts & Hayes, *Understanding command and control.*

alternatives. The U.S. Department of Defense defines a decision as, "…a clear and concise statement of the line of action intended to be followed by the commander as the one most favorable to the successful accomplishment of the assigned mission."[34] Alberts and Hayes describe decision rights as:

Decision rights belong to the individuals or organizations accepted (whether by law, regulation, practice, role, merit, or force of personality) as authoritative sources on the choices related to a particular topic under some specific set of circumstances or conditions. The allocation of decision rights is their distribution within the international community, a society, an enterprise, or an organization. In this context, the organization of interest is a military, a coalition, an interagency effort, or an international effort including military elements. There can be different distributions of those rights across functions, echelons, time, or circumstances.[35]

1.4 Patterns of Interaction

Patterns of interaction describe how organizations interact in conducting command and control. At the origin of this axis, patterns of interaction are tightly controlled. At the opposite end of this axis, organizational interactions are unconstrained. As current military operations involve large organizations consisting of subordinate organizations distributed in a hierarchical manner, the patterns of interaction in a classic C2 structure are designed to ensure control from the center. Hence, the pattern of interaction follows the chain of command established for the operation. However, in cyberspace patterns of interaction can be considered networks.[36] The technology underpinning cyberspace makes it possible for all entities participating in a military operation to communicate.

Collaboration, working together toward a common purpose, is the most desirable pattern of interaction.[37] Collaboration involves actors actively sharing data, information, knowledge, perceptions, or concepts when they are working together toward a common outcome and how they might achieve that outcome efficiently or effectively.[38] Collaboration provides the opportunity for the parties to exchange views about the clarity of the data and information, as well as what it means or implies, not just to receive information.[39]

1.5 Distribution of Information

Information is a strategic asset and it is critical to the conduct of military operations. How information is distributed affects the ability of an organization to deal effectively with the challenges it faces. The distribution of information can be thought of as ranging from fully centralized repositories to fully distributed approach where everyone has access to everything.[40] At the origin of this axis, information is typically stored in a central location and the access of each user was predetermined and controlled by a central authority. At the opposite end of the axis, advances in communications and information technologies and the accompanying changes in the economics of information made it feasible to distribute information much more widely and make it accessible to all.[41]

The distribution of information within a military operation is influenced by the allocation of decision rights, the patterns of interaction, the organization's willingness to share information, and the tools and skills they have to share it. The distribution of information is also driven by the organization's need and ability to collaborate, and the ability to share information, awareness, and

[34] U.S. Department of Defense, *Joint publication 1-02,* 66.
[35] Alberts & Hayes, Understanding command and control, 83.
[36] Ibid.
[37] Ibid.
[38] Alberts, D. S., Garstka, J. J., Hayes, R. E., & Signori, D. A., *Understanding information age warfare*, (Washington DC: Assistant Secretary Of Defense, C3I/Command Control Research Program, 2001).
[39] Alberts & Hayes, Understanding command and control.
[40] Ibid.
[41] Ibid.

understanding. Ultimately, the distribution of information governs the capacity for sense making at both the individual and collective levels.[42]

The three key dimensions of this C2 model are not independent. In fact, they are highly interdependent. Showing them as three axes of a cube is somewhat over simplified. However, the model is useful to describe the three dimensions and how they interrelate. Any consideration of an approach to C2 must fully consider and describe the choice made in each dimension. "The most fundamental dimension is allocation of decision rights, which impacts the other two and, together with patterns of interaction, goes a long way toward determining the distribution of information."[43]

2. CYBERSPACE OPERATIONS IS A BIG DATA PROBLEM

The intersection of the choices made regarding the allocation of decision-making rights, patterns of interaction, and the distribution information will determine how the cyber mission force will conduct operations to achieve national security and military objectives in and through cyberspace. An important outcome of these decisions will be the determination of the technology and data necessary to make decisions during conduct of operations. As the Cyber Mission Forces are being created, the need for new and better technologies for the cyberspace operations mission has become apparent. The Commander of U.S. Cyber Command has stated, "Our cyber teams will be tangible and operationally ready to execute their assigned missions. To do this they require platforms, tools, training, and infrastructure, just like maneuver elements in all other domains".[44] One of the most pressing needs is the capability to have situational awareness of all operational domains. Endsley states, "Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."[45] The Commander of U.S. Cyber Command describes this need as, "To operationalize the cyber mission set, we must create common shared situational awareness tailored to the mission sets and requirements of operational commanders".[46]

Shared situational awareness, also described as collective awareness, is a critical element of collaboration within communities, especially computer-mediated communities. Pitt et al. describe collective awareness and collaboration as, "…users must understand how their individual actions contribute to a greater whole. In other words, they must be aware of the same data and share the same legal, social, and cultural context to interpret that data. This collective awareness is a critical element of collaboration within communities, especially computer-mediated communities."[47] The Commander, U.S. Cyber Command has also stated, "The nation's cybersecurity requires a collaborative approach with a range of interagency and industry partners contributing authorities, capabilities, and insights to protect US infrastructure and information, detect attacks, and deter adversaries in cyberspace. By working together we improve our collective knowledge about what is happening across the cyber domain and protect our networks".[48]

Effectively conducting cyberspace operations requires that the DOD to be able to take common action based on collective awareness of the state of the cyberspace domain, the military mission in the supported domains, and the activities and intent of its cyberspace adversaries. "Collective awareness can be achieved by analyzing big data generated by networked sensors and devices as well as ICT[49]-enabled users. Search, data mining, and visualization technologies make it possible to spot trends and predict the trajectories of higher-level variables. This in turn enables collective action, without which it might be impossible to change community behavior to reach a desirable outcome."[50] To achieve this

[42] Ibid.
[43] Ibid. 81.
[44] U.S. Department of Defense, *Beyond the build*, 8.
[45] Endsley, M. R., "Toward a theory of situation awareness in dynamic systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), (1995), 32-64.
[46] U.S. Department of Defense, *Beyond the build*, 6.
[47] Pitt, J., Bourazeri, A., Nowak, A., Roszczynska-Kurasinska, M., Rychwalska, A., Rodríguez Santiago, I., Lopez Sanchez, M., Florea, M., & Sanduleac. M., "Transforming big data into collective awareness". *Computer* 46, no. 6, (2013), 40-45.
[48] U.S. DOD, *Beyond the Build*, 3.
[49] Information and communication technologies
[50] Pitt et al., Transforming big data into collective awareness, 40.

collective awareness and action requires that the DOD cyber mission force have the capability to collect and analyze the big data generated by the networked sensors and devices that comprise cyberspace.

2.1 Definition of Big Data

Big data and big data analytics have been a topic of considerable attention in the literature. There are many definitions and descriptions of big data. Big Data is a term used to describe datasets that cannot be managed with current methodologies or data mining software tools due to their large size and complexity.[51] There is agreement in the literature that big data has several characteristics. These characteristics are:

- Volume: Petabyte-scale sets of data that come from click streams, transaction histories, sensors, and elsewhere.[52]
- Velocity: Data that must be processed quickly.[53]
- Variety: Data that doesn't fit neatly into existing processing tools.[54]
- Variability: Structure of data and how users want to interpret that data changes.[55]
- Value: Big data creates competitive advantage thru making decisions and answering questions that were previously considered beyond reach.[56]

The cyberspace environment has all of these big data characteristics. The network devices, processors, sensors, mobile devices, and users all create huge volumes of data each day. The increasing volumes of data presents challenges for the DOD cyber mission force to collect, analyze, and act in order to accomplish their mission. Chen, Chiang, & Storey describe the problem as:

Intelligence, security, and public safety agencies are gathering large amounts of data from multiple sources, from criminal records of terrorism incidents, and from cyber security threats to multilingual open-source intelligence… Processing and analyzing security-related data, however, is increasingly difficult. A significant challenge in security IT research is the information stovepipe and overload resulting from diverse data sources, multiple data formats, and large data volumes.[57]

One of the greatest challenges for the cyber mission force and other cybersecurity organizations is to develop the capabilities to uncover patterns and subtle indicators of adversary activity through enhanced data integration and analysis.[58] This is a challenge for all parts of the cyberspace operations community.

3. DATA TO DECISIONS FOR CYBERSPACE OPERATIONS

Collecting and analyzing large amounts of data is not useful in itself. Analyzing this data is only useful when the results of the analysis are used to make decisions and take action to achieve national objectives in and through cyberspace. It is critical that the DOD's cyber mission forces have the capability to use the results of big data analysis to rapidly make decisions and take action to accomplish their mission. Schwartz has stated that security decision systems for DOD missions, including cyberspace operations, must focus on finding threats in a large data volume, with limited

---

[51] Fan, W. & Bifet, A., "Mining big data: current status, and forecast to the future," *ACM SIGKDD Explorations Newsletter* 14 (2013), 1-5.
[52] Ibid.
[53] Ibid.
[54] Ibid.
[55] Fan & Bifet, Mining big data.
[56] Ibid.
[57] Chen, H., Chiang, R. H., & Storey, V. C., "Business Intelligence and Analytics: From Big Data to Big Impact," *MIS quarterly*, *36*(4), (2012) 1165-1188.
[58] U.S. Department of Homeland Security, The 2014 Quadrennial Homeland Security Review, (2014). Retrieved from http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

manpower, within a specified time window.[59] The Defense Advanced Research Projects Agency (DARPA) has described the decision making challenge as, "Current DOD systems and processes for handling and analyzing information cannot be efficiently or effectively scaled to meet this challenge. The volume and characteristics of the data, and the range of applications for data analysis, require a fundamentally new approach to data science, analysis and incorporation into mission planning on timelines consistent with operational tempo".[60] For the purpose of this paper, decision-making for Defensive Cyberspace Operations (DCO) is used to describe the required capabilities.

Figure 2 shows the decision-making challenge facing the DOD's cyber mission forces. Schwartz describes three categories of decision-making: automatic, assisted, and discovery[61]. Automatic decisions are those made by automated systems analyzing data in near real time in order to respond to changes in state of the network. In the cyberspace environment, automatic decisions are made by the by networked sensors and devices that comprise cyberspace and are normally made within seconds of the data being collected. Internet Protocol routers, intrusion detection systems and firewalls are examples of the devices that make automatic decisions in cyberspace.

Assisted decisions are those decisions made by humans with the assistance of a decision support system. In cyberspace operations, decisions regarding the identification of cyberspace incidents, the threat vector being used and the technical impact of an incident are types of assisted decisions made using analytic tools and decision support aids. These decisions are normally made within minutes, hours or days of the data being collected.

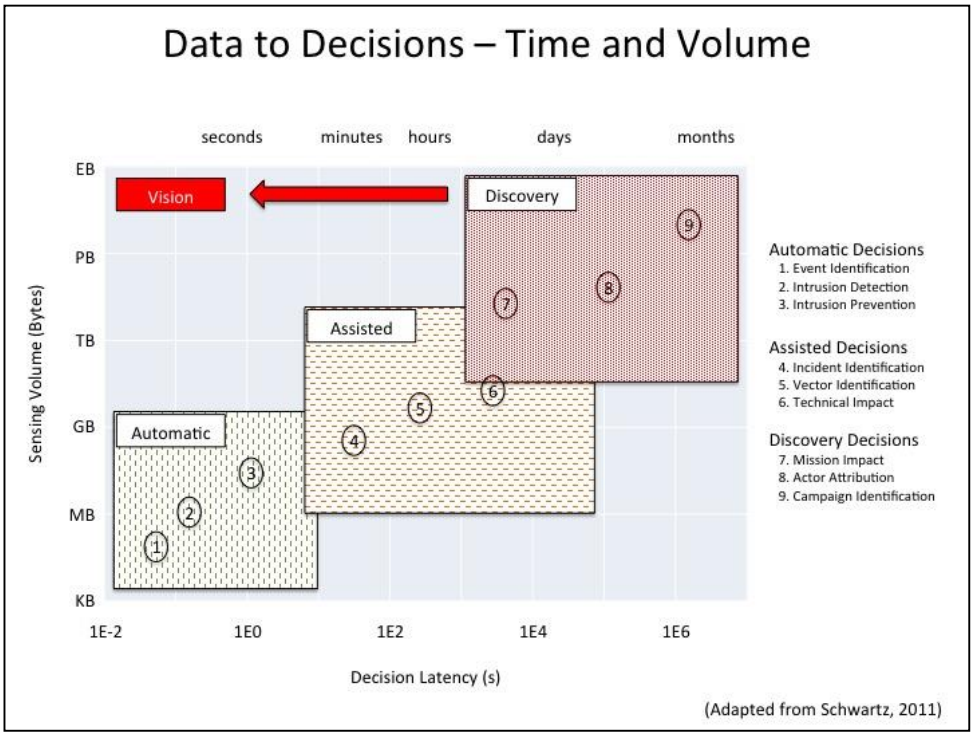

Figure 2. Data-to-Decisions for Defensive Cyberspace Operations – Time and Volume[62]

Discovery decisions are those decisions, made by a human, usually resulting from manual analysis of larger volumes of data over periods of hours, days or months. Examples of these types of decisions

[59] Schwartz, C., *Data-to-Decisions S&T Priority Initiative*, (Arlington VA: Office Of Naval Research, 2011). Retrieved from: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA554682.

[60] U.S. Department of Defense, Defense Advanced Projects Agency, *DARPA calls for advances in "big data" to help the warfighter,* (2012). Retrieved from http://www.darpa.mil/NewsEvents/Releases/2012/03/29.aspx.

[61] Schwartz, C., Data-to-Decisions S&T Priority Initiative.

[62] Adapted from Data-to-Decisions S&T Priority Initiative by Carey Schwartz. 2011. Copyright 2011 Office Of Naval Research Arlington VA. Reprinted with permission.

are the determination of the mission impact of an event, the attribution of adversary activity, and the identification of adversary activity as part of a larger adversary campaign.

To meet the decision making speed and agility required to keep pace with change in the cyber domain described by the Commander of US Cyber Command, the cyber mission force must be able to make assisted and discovery decisions much faster than currently possible. The ultimate goal is to have the capability to make discovery decisions within seconds or minutes of data collection. In order to make these decisions, it is necessary to identify the types of data required to make an informed decision. In cyberspace operations missions, the operating forces require collective awareness of the mission status, technology status and the adversary characteristics and intent.

3.1 Mission Status

The DOD has a global responsibility for military operations. To meet this responsibility, the DOD has established nine combatant commanders with responsibilities for U.S. military operations within a specified geographic region or for a functional mission with global responsibilities. These combatant commands are responsible for multiple operational plans, covering all military missions.[63]

Knowledge of the status of active missions is necessary to measure the impact of the incident to the mission. This knowledge is necessary to ensure the mission context is considered and factored into the risk of what otherwise may be considered a simple technical issue. This data set is operationally based, specifically describing ongoing combatant command operations. The data necessary to understand the impact of an incident on the mission includes mission timing, location, types of services affected, and any effect to personnel. It also must include the effects on confidentiality, integrity, and availability of different types of operational information required to make the decisions necessary to accomplish the mission.

3.2 Technology status

Also necessary to create situational awareness of cyberspace is data on the status of the information technology systems comprising cyberspace. The DOD has a significant number of networks and devices to support military operations. It is reported that the Department of Defense has 15,000 networks, 7 million computers, and 1.1 billion Defense Department Internet users worldwide.[64]

Technically focused data is necessary to answer questions related to the technical scope of the incident. The technical context of an incident determines how widely affected the network is and the difficulty of resolving the incident. The characteristics of this set are on technical issues. These data focus on topics related to the scope of affected assets, categorization of incident, and compromised user privileges. This set also addressed the current security posture of the network, any existing mitigation strategies, and estimated cost to mitigate the incident.

3.3 Adversary Status

The third set of data necessary for defensive cyberspace operations is data about the adversary, their capabilities, and their intent. Hutchins, Cloppert, & Amin have identified knowledge of the adversary as essential to effectively defending cyberspace. They posit that it is possible to anticipate and mitigate future intrusions based on knowledge of the threat.[65]

The adversary-focused data set is used to assess the characteristics and intent of the adversary applicable to the incident. This data set includes available intelligence on the likely actor. This data is

---

[63] U.S. Department of Defense, *Joint Publication 1: Doctrine for the armed forces of the United States,* (2013). Retrieved from: www.dtic.mil/doctrine/new_pubs/jp1.pdf.

[64] McCullagh, D., "NSA chief downplays cybersecurity power grab reports", *CNET*, April 2009. Retrieved from http://www.cnet.com/news/nsa-chief-downplays-cybersecurity-power-grab-reports.

[65] Hutchins, E. M., Cloppert, M. J., & Amin, R. M., "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, *1*, (2011), 80.

used to determine the cause of an incident, the characteristics, tactics, and resourcing of the adversary. Michael and Miller describe the value of big data in understanding the adversary as:

Big data can expose people's hidden behavioral patterns and even shed light on their intentions. More precisely, it can bridge the gap between what people want to do and what they actually do as well as how they interact with others and their environment. This information is useful to government agencies as well as private companies to support decision-making in areas ranging from law enforcement to social services to homeland security.[66]

One of the most pressing analytic needs for DCO is counter-deception. Cyber espionage and cyber attacks involve deception, even when deception is not the sole purpose of the cyber attack.[67] While the primary purpose or intent of cyber espionage and cyber attacks is to achieve some effect, that effect is frequently enabled by deception. Most examples of cyber attacks involve deception that is brought about by various means. Deception is defined as a deliberate action to induce erroneous sense making and subsequent activity within a target audience to achieve and exploit an advantage.[68] Deception is fundamentally psychological.[69] "Deceptive actions by one actor influence the behaviors of another actor, so deception is a form of influence and persuasion, although the target of the deception may be completely unaware of being persuaded or influenced".[70] The purpose of the deception is to influence the decision-maker, either to get the decision-maker to do something or to keep them from doing something. The cyber mission force must have the capability to rapidly detect cyber deception and make decisions that counter the adversary actions.

Collecting and analyzing the data that describe the military mission, the technical status of cyberspace, and the characteristics and intent of the adversary is essential to conducting effective cyberspace operations. The DOD must continue to develop the data management and data analysis capabilities necessary to make assisted and discovery decisions much faster than currently possible.

4. CONCLUSIONS

The U.S. cannot conduct military operations without cyberspace nor can it exert or maintain national power without acute sensitivity to the digital networks that underpin our ability to conduct operations. In order to effectively conduct cyberspace operations in support of national security and military operations, the DOD must improve its ability to rapidly make effective decisions in the dynamic environment presented by cyberspace.

Chen, Chiang, & Storey state, "The decade of the 2010s promises to be an exciting one for high-impact BI&A[71] research and development for both industry and academia. The business community and industry have already taken important steps to adopt BI&A for their needs".[72] The DOD has begun to leverage this research and to adopt its results to the military mission. However, much work remains to be done.

Collecting and analyzing large amounts of data is not useful in itself. Analyzing this data is only useful when the results of the analysis are used to make decisions and take action to achieve national objectives in and through cyberspace. To meet the decision making speed and agility required to keep pace with change created by the cyber domain described by the Commander of US Cyber Command, the cyber mission force and other military forces must be able to make assisted and discovery decisions much faster than currently possible. The ultimate goal is to have the capability to make discovery decisions within seconds or minutes of data collection.

In order to make these decisions, it is necessary to identify the types of data required to make an informed decision. In cyberspace operations missions, the operating forces require collective

[66] Michael, K. & Miller, K., "Big Data: New Opportunities and New Challenges," *Computer* 46, no. 6, (2013), 22-24.

[67] Henderson, S. M., "Deceptive Thinking Workshop", (paper presented at the 1st MilDec Military Deception Symposium, Defence Academy of the United Kingdom, Shrivenham, 2nd-3rd November 2011).

[68] Ibid.

[69] Heckman, K. E., & Stech, F. J., "Cyber Counterdeception: How to Detect Denial & Deception (D&D)," in *Cyber Warfare*, (Springer International Publishing, 2015), 103-140.

[70] Boush, D., Friestad, M. & Wright, P., Deception in the Marketplace: The Psychology of Deceptive Persuasion and Consumer Self Protection, (New York: Routledge Taylor & Francis, 2009).

[71] Business Intelligence & Analytics

[72] Chen, Chaing, & Storey, Business Intelligence and Analytics, 1168.

awareness of the mission status, technology status and the adversary characteristics and intent. Counter deception analytics is one of the most critical analytic needs. The cyber mission force must have the capability to rapidly detect cyber deception and make decisions that counter the adversary actions.

While most of the cyberspace mission force needs can be met by development from industry and academia, there is a need for DOD to continue its efforts to develop the mission specific capabilities to enable the cyber mission force to rapidly analyze cyberspace operations data and make critical mission decisions within mission timelines. It is essential that the DOD's cyber mission forces have the capability to use the results of big data analysis to rapidly make decisions and take action to accomplish their mission. In order to realize the operational capabilities necessary to conduct cyberspace operations, the DOD must accelerate its research and experimentation in big data analytics for cyberspace operations.

AUTHOR BIOGRAPHY

Lieutenant Colonel (Retired) Steve Stone is a doctoral candidate in the Doctor of Science in Information Systems and Communications program at Robert Morris University. He retired from the United States Army in 2006 as a Functional Area 24 Information Systems Engineer. His assignments included: Deputy Technical Director for Joint Task Force Global Network Operations (JTF-GNO); Chief of the JTF-GNO Strategy Branch; Operations Officer, U.S. Army European Theater Network Operations and Security Center, 5th Signal Command; and Operations Officer, US Central Command Intelligence Systems Division. Since retiring from the US Army, he has worked as a Principal Cyberspace Operations Engineer at the MITRE Corporation in McLean, Virginia. He currently leads MITRE's work at US Army Cyber Command. He received his bachelor's degree in Aerospace Engineering from the United States Military Academy, a Masters of Science in Computer Science from the Naval Postgraduate School, and a Masters of Education from Old Dominion University. He will complete his doctorate in 2016. His research interests include Military Command and Control, Decision Making, Knowledge Creation and Management, and Cyberspace Operations.