Information Advantage Activities:

A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations

Lieutenant Colonel Robert J. Ross, Ph.D.

INTRODUCTION

The Multi-Domain Operations (MDO) doctrinal framework is the driving mechanism for transforming the U.S. Army into a dominant information-age military force. To address the informational power aspects associated with MDO, the U.S. Army's Training and Doctrine Command (TRADOC), in partnership with the Cyber Center of Excellence (CCoE), developed the Information Advantage (IA) and Decision Dominance (DD) doctrinal framework. Within this framework, "commanders seek to achieve DD, a desired state in which a commander can sense, understand, decide, act, and assess faster and more effectively than an adversary by gaining and maintaining positions of relative advantage, including IA."[1] IA is "a condition when a force holds the initiative in terms of relevant actor behavior, situational understanding, and decision-making using all military capabilities through the conduct of Information Advantage Activities (IAA)."[2] Lastly, IAA is defined as "the employment of capabilities to enable decision-making, protect friendly information, inform and educate domestic audiences, inform and influence international audiences, and conduct information warfare."[3]

The exponential growth in powerful computer network technologies and its effects on human cognition are radically changing the character of 21st century warfare. The unceasing pace in the growth of Internet of Things (IoT) devices has created ubiquitous human access to voluminous amounts of information. This access, coupled with the individual's ability to influence global audiences from these devices, is creating radical social and political change across the world, including the character of warfare. The technological and cognitive effects stemming from using these devices have been demonstrated within conflicts waged thus far in the century. These conflicts have demonstrated that the means for waging war depends more and more on artificial intelligence, machine learning, computer networks, and autonomous/semi-autonomous vehicles. The U.S. Army is at a point

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

Lieutenant Colonel Robert J. Ross is the Strategic Initiatives Group Chief for the Commanding General of U.S. Army Cyber Command, Fort Gordon, GA. Lieutenant Colonel Ross advises the ARCYBER Commanding General on cybersecurity, information-age conflict, and information warfare strategy initiatives. Lieutenant Colonel Ross is a former assistant professor in the Electrical Engineering and Computer Science Department at United States Military Academy at West Point, NY. As an assistant professor, Lieutenant Colonel Ross taught primarily information technology courses and course directed the Academy's information warfare course. He is a former Chief Research Scientist for the Army Cyber Institute, where he served as the Information Warfare Team Lead. Lieutenant Colonel Ross has a B.S. in Computer Science from Rowan University, an M.S. in Computer Science from Monmouth University, and a Ph.D. in Information Science from the Naval Postgraduate School. Lieutenant Colonel Ross is a cyberwarfare officer and former artilleryman with two combat deployments to Iraq. His research interests are organizational science, strategic foresight, information warfare, 21st century conflict, and financial technology.

in which all six of its warfighting functions (Movement and Maneuver, Intelligence, Fires, Protection, Sustainment, and Mission Command) will be totally dependent upon the Army's portion of the Department of Defense Information Network (DoDIN) to effectively conduct MDO by 2028.

The changing character of warfare in the 21st century should serve as a catalyst for the U.S. Army to reexamine its contextual view of information, how is used to describe capabilities, and how operational art is applied within the IA and DD doctrinal framework. The word "information" is used broadly throughout Army doctrine and literature. There are 259 instances of "information" used within Field Manual 1-02.1, which defines information as "in the context of decision-making, data that has been organized and processed to provide context for further analysis."[4] Before the publication of Field Manual 1-02.1, there was no definition for the word "information" within any U.S. Army doctrine. However, this semiotic definition begs further explanation, particularly regarding the role information plays within the human dimensions of operational environments. Members of the Army community have many different understandings of how "information" is used within mixed professional specialties on Army staffs. The many differing definitions of the word "information" are dependent upon the context of its use. Unfortunately, dependent upon branch or military occupational specialty (MOS), interpretations of the context will lead to misunderstanding. These differing perspectives or contexts used to understand the meaning of "information" affect its usage, particularly as it applies to capabilities and operations. This article aims to raise the philosophical and contextual question, "what is information?" within the context for Army operations then examine its application across the range of capabilities and current operational art.

Information is inherent in every capability at an Army commander's disposal. The combination of

organization, strategy, and integrated technologies defines a capability regardless of context. Understanding this informational principle about a capability removes the confusion, misunderstandings, murkiness, and ambiguities associated with categorizing it as "information-related." Every capability is "information-related" and popular definitions for "information" in the academic and information science literature support this assertion. Therefore, the Army should eliminate the term, "information-related capability," during the development of future IA capabilities. A second proposition would be to maintain a more traditional view of capabilities with the caveat that a capability is more than a material resource or technology. It is a system comprised of organization, strategy, and integrated technology. Operational art is defined in Army doctrine as a "cognitive" process that involves "skill, experience, creativity, and judgement," therefore, contemporary operational art requires a holistic approach unrestrained from the ambiguous categorizations associated with the term, "information," or its use as an adjective for capabilities. Such categorizations are constraining and get in the way of the efficient deployment of capabilities in 21st century operating environments. Therefore, an amenable model is proposed later in the paper as a base of knowledge for discussions about future Army organization and the role of information within the commander's operational art at all levels of Great Power Competition.

WHAT IS INFORMATION?

Meaning and context are the two biggest challenges for the Army's use of the word "information," particularly when it is used to categorize an "information-related capability." Information is too abstract and omnipresent to be treated as an entity of its own within the operational environment. The cyberspace operations, electromagnetic warfare, and signal community often view information within the context of Shannon and Weaver's telecommunications research. They define "information" within the context of mechanistic or engineering perspectives.[5] These communities view information through the lens of digitization, radiated frequency, or optical signals. Conversely, PSYOP, public affairs, and information operations professionals view information from a perspective more akin to Howell's definition in which information is defined as "not only facts and figures, but all the relationships, vague ideas, hunches, feelings, in fact, everything people have stored inside them or have picked up from the outside world." [6]

This same notion holds true in the military intelligence community, which views cyber intelligence information using both mechanical and cognitive lenses. Intelligence professionals working in the cyber community view social media, commercial cyber vulnerabilities, or advanced persistent threat (APT) information in all forms, often from proprietary sources, in a context that does not typically integrate well with traditional forms of military intelligence. People can have various understandings of what information is within a particular Army operation, therefore, "information" and the context in which it is being used cannot have a common understanding or definition. This is particularly true as it pertains to the varying and voluminous amounts of information used for decision-making and the use of capabilities.

Information should be novel and inform its human consumers. However, larger philosophical and contextual questions need to be answered before a consensus can be reached on the use of the term within Army operations, including its use as a description for capabilities. Does data received from sensors which are a part of an automated system, then analyzed, and used in automated decision making constitute "information?" What about digitized, electrical representations of information residing on computers or being transported across a network? Some would argue that artificial intelligence and machine learning counter the proposed philosophy that information is purely a human process.

However, for argument, the Army, as an organization, is currently a human information processing entity.[7] It exists to acquire and process information used for human—not artificial—decision-making. It also exists within a military context to disrupt, degrade, deny, destroy, or manipulate adversarial organizations' information acquisition and processing capabilities while doing the same concerning their cognitive will to fight. Taking a practical view of information will remove much of the ambiguity, confusion, murkiness, and misunderstandings that terms like "information-related capabilities" convey. All capabilities should be treated as information-related capabilities, which would summarily eliminate categorizing labels that describe capabilities as either information-related or kinetic. Distinctions between capabilities, particularly when commanders are integrating information warfare capabilities (cyberspace, electromagnetic warfare, and information operations) into combined arms operations (infantry, armor, and artillery) during conflict hampers the application of their operational art.

CAPABILITIES VERSUS INFORMATION RELATED CAPABILITIES

> "Everything we say and do, and everything we fail to say and do, will have an impact in other lands. It will affect the minds and the wills of men and women there."
>
> *- Presidential candidate Dwight D. Eisenhower, campaign speech, 1952*

It must be inculcated into the Army's culture that all capabilities at commanders' disposal are information related. Whether firing suppressive fires through artillery or amplifying narrative supporting Army operations across social media to a targeted audience, it makes no difference, "information" affecting human cognition is still being conveyed during the application of a commanders' operational art. All actions, communications, and even the identity the Army conveys to populations for whom they are engaged, conveys information, because, intentionally or unintentionally, the Army's presence influences the behaviors of these societies simply as an outcome of the capability's the commander is leveraging during operations. The United Kingdom's (UK) Ministry of Defence uses a similar concept conveyed in their Defence Strategic Communication Doctrine Note. This document defines operations in the information environment as "advancing national interests by using Defence as a means of communication to influence the attitudes, beliefs, and behaviours of audiences."[8] Most importantly, this document does not view information as a separate and distinct entity from

the diplomatic, military, and economic instruments of national power. The Joint Note defines information as the integrating function, the glue, binding the instruments of national power together.[9] A definition and philosophical understanding that should be adopted within the context of the IA doctrinal framework and commanders' operational art.

Figure 1. Information's relationship with the instruments of National Power.
Diagram adapted from the Joint Doctrine Note 2/19.

Information and the contemporary information dimension of operational environments pose significant challenges for the Army of the future. The exponential growth of technological innovation coupled with a global society consuming information from the vast and ad-hoc socio-technical networks being formed are creating complex operational environments. These technologies cause the planning and deployment of capabilities to become more complicated by attempting to distinguish information-related capabilities from all other capabilities at a commander's disposal. This is particularly true as nearly every capability within the auspices of the Army's six warfighting functions is dependent upon the vital data flows streaming across the Department of Defense Information Network – Army (DoDIN-A). This is a condition that will only become more pervasive as the growth and reliance on powerful technologies grows exponentially in the foreseeable future. Every Army weapon, command and control, signals intelligence, and sustainment system is dependent on a functional and secure DoDIN-A to successfully train, deploy, sustain, and support winning the joint fight in contemporary operating environments. If commanders are going to successfully adapt to tomorrow's technologically driven operational environments, the focus should be on viewing all capabilities as conveying information and considering the network as part of the combined arms fight within the application of operational art.

Like our British Allies have done with their national defense strategy, the U.S. Army should create capabilities (organizations, strategies, and integrated technologies) with the view that information is not a separate or distinct framework, such as maneuver versus support. It exists within the integrated components of all warfighting functions. Instead of distinguishing information-related capabilities from all other capabilities, we should inculcate a culture that views the use of all the commander's capabilities for the purposes of information advantage activities in competition, crisis, and conflict. An example would be firing an artilery round for the purposes of getting enemy counter-fire radar to radiate, then using electromagnetic warfare capabilities to detect the radar's location, then jam its location, and finally, an air asset to subsequently destroy the radar. In this example, the commander uses a range of unique capabilities to conduct information advantage activities that first disrupts then destroys an adversary's abilities to conduct signals collection activities.

The U.S. Army's concepts and strategies of the future need to be based on the commander's operational art, defined as "the principles of joint operations to envision how to establish conditions that accomplish their missions and achieve assigned objectives" using the combination of all capabilities at their disposal.[10] The future operational art will require that commanders apply the range of their capabilities as information advantage activities during periods of competition, crisis, and conflict. War is a clash of human will and the will is a cognitive function; therefore, all actions—physical, informational, violent, non-violent, however they are categorized—are intended to achieve cognitive effects. The commander's goal should be to destroy the adversary's will to fight without fighting.[11] We would be best served to eliminate categories that ultimately impede the commanders' operational art.

CONSIDERATIONS

Before proposing an organizational view for the future information-advantaged force, the U.S. Army needs to consider the following:

a. Free market innovation, research, and development have created exponential growth in socio-technical networks through the availability of inexpensive, commercial-off-the-shelf (COTS) technologies that provide state and non-state actors' information parity with the U.S. in most operational environments.[12]

b. The current military acquisition processes are intended for success in the 20th century, the era of industrialization, not the information-age. The rapid availability of cheap COTS equipment renders most of the Army's information technology equipment and battlefield operating systems (BOS) obsolete long before they are fielded.

c. Information advantage activities faced by the Army should be dependent on strategy, not solely on information technology.[13]

These considerations serve as a framework for describing and explaining the role of information advantage activities within a commander's operational art.

OPERATIONAL ART AND INFORMATION ADVANTAGE ACTIVITIES

Information activities are persistent and not bound by the traditional phases of operations; they persist across all phases of military operations for which commanders are responsible (Competition → Conflict → Return-to-competition).[14] Since all capabilities at a commander's disposal are intended to deny, delay, disrupt, destroy, or manipulate information, information advantage activities need to be raised to a continuous level of consciousness among commanders and their staffs during the application of operational art. Cultural change concerning information and its application within operational art must be adopted throughout the Army's professional military education (PME) system for all levels of Army leadership.

Information advantage activities are continuous across all phases of military operations whose outcomes are intended to be either coercive or non-coercive. They are dependent on a powerful Army network that serves as a global projection platform capable of transporting, storing, and processing voluminous amounts of holistic and real-time information. The goals for these activities should be integrated, coordinated, and synchronized across the strategic, operational, and tactical levels and focused on achieving US strategic aims during Multi-Domain Operations. The goal of information advantage activities is to enable commanders to achieve decision dominance and ultimately break an adversary's will to fight before reaching armed conflict.[15] The challenge will be inculcating a culture that adopts some variation of the proposed information advantage activities' definition and is willing to apply it to the application of operational art.

A good analogy for this conceptual view could be defined as looking at the operational environment from the perspectives of quantum (multiple) states versus binary (two) states (Johnson, 2019).[16] In the quantum view, the human, physical, and information dimensions of an operational environment are integrated, continuous, and interconnected. Events and activities are connected and impact all three dimensions of the operational environment simultaneously, rapidly, and unpredictably across both time and space. The physical and human dimensions, independent of the information dimension, exist in a binary-like state in which activities have probabilistically predictable conclusions that are observable and measurable in ways that commanders can understand and effectively respond. Subsequently, effects in the information dimension, at the level of human cognition, are persistent and reside in an infinite state, the effects of which are not always observable, measurable, or predictable. The proposed information advantage activities concept could serve as a mechanism for bridging the divide in how commanders view the operational environment as a gestalt comprised of the physical, human, and information dimensions. It must be emphasized that the information advantage doctrinal framework is designed to add to a commander's operational art, not take away current applications of the form. The U.S. Army's ability to kinetically overmatch our adversaries and break their will to fight during periods of armed conflict must be maintained.

PROPOSED CONCEPTUAL INFORMATION ACTIVITIES MODEL

The following proposed model provides a view that maintains the Army's current warfighting function (WfF) posture.[17] Note the model illustrated in figure 2 does not add a separate and distinct information warfare WfF. Rather it is intended to change the way commanders view all the capabilities at their disposal and the role of persistent information advantage activities across all phases of military operations.

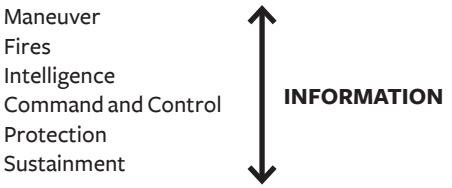

Figure 2. Information's relationship with the U.S. Army's WfF.

Figure 2 above illustrates a view that reflects information as an integrating element of all WfFs as adapted from the UK's Joint Doctrine Note 2/19. This figure reflects the role of information as pervasive across all WfF and likewise across the range of capabilities available to commanders. Capabilities are used to enact the commander's operational art, and all capabilities are considered information related.

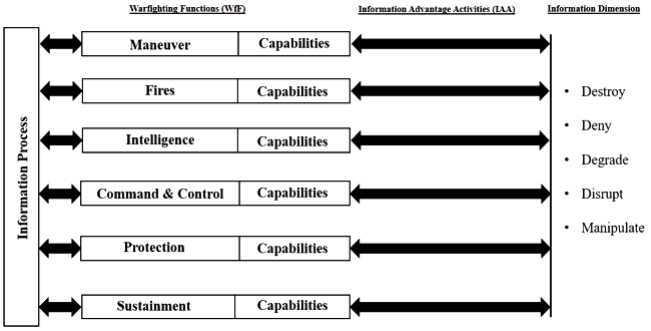

Figure 3 The role information advantage activities within the commander's operational art.

Figure 3 above illustrates the Army organization as an information processing entity. It illustrates the information processing relationship between the Army's WfFs that are integrated, synchronized, and coordinated. It also illustrates how capabilities executed by the WfFs are intended to analyze or react to information advantage activities within the operational environment.[18] The figure also presents a typology for intended information advantage activity outcomes. Information advantage activities are intended to acquire information, disrupt information, engage with populations (influence/inform), or destroy sources of adversarial information activities. Information advantage activities are persistent and constant, while military operations across competition, crisis, and conflict are dynamic. The model is intended to integrate the range of kinetic, non-kinetic, coercive, and non-coercive capabilities at a commander's disposal in a way that eliminates the confusion, ambiguity, murkiness, and tribalism that would be created by defining information as a new warfighting function (WfF).

CONCLUSIONS

This article presented information advantage activities as core components of the Army's new Information Advantage and Decision Dominance doctrinal framework. It also proposed

a definition and model for the deployment of capabilities at the commander's disposal during their application of operational art. The proposed definition and model are intended to remove the confusion, misunderstandings, murkiness, and ambiguities created by categorizing capabilities as "information-related." It also explains the causes for confusion between the different warfighting functions when the term "information" is used based on different understandings, meanings, and contexts for the terms of use between these groups. A couple of definitions of information from the academic literature support this assertion. As a result, this article proposes eliminating the term "information-related capabilities" because all capabilities are information-related. Distinguishing between what is a capability and what is an information-related capability creates a far more complicated view for how commanders see themselves, see the adversary, understand, decide, act, and continually assess during the application of operational art within contemporary operational environments. These complicated views cause the events involving information for decision-making to become blurred and the commander's actions involving capabilities to be unsupportive of one another instead of coordinated. The UK's Ministry of Defence's Joint Doctrine Note 2/19 Defence Strategic Communication: An Approach to Formulating and Executing Strategy was used to support this functional view.

Finally, a model is proposed that does not view the physical, human, and information dimensions as separate entities. Instead, it provides a view of the operational environment as a gestalt in which the physical, human, and information dimensions are fully integrated parts. Again, this model is supported through example found in the UK's Ministry of Defence's Strategic Communication: an Approach to Formulating and Executing Strategy, Joint Doctrine Note 2/19, in which information is viewed not as a separate instrument of national power, but the glue that binds diplomacy, military, and economic power together. [19] The same view should be adopted within the Army's culture in which information is not viewed as a separate or distinct component within the operational environment, but the glue that flows through and binds together every capability enabling operations. In closing, the model presented as a concept in this paper integrates information advantage activities in a way that adds to our current model for the application of operational art and does not take away from it. Adopting these proposed views into Army culture surrounding use of the term "information" and the future application of operational art will only reinforce IA and DD as a doctrinal framework that will effectively support future multi-domain operations (MDO).

ACKNOWLEDGEMENTS

The author would like to thank Lieutenant General Stephen G. Fogarty (Commanding General, U.S. Army Cyber Command) and Mr. Bryan Sparling (U.S. Army Cyber Command's Information Warfare Transformation Advisor) for the invaluable insights they provided to this article.

NOTES

1. U.S. Army Training and Doctrine Command, 2021, *Information Advantage and Decision Dominance version 15*, unpublished Whitepaper, Fort Gordon, GA.
2. Ibid.
3. Ibid.
4. U.S. Department of the Army, 2021, *Field Manual 1-02.1 Operational Terms,* Washington, DC.
5. C. Shannon and W. Weaver, *The mathematical, theory of communication* (Champaign, IL: University of Illinois Press, 1963).
6. W.S. Howell, *The empathic communicator* (Belmont, CA: Wadsworth, 1982).
7. J.R. Galbraith, *Organization Design* (Boston: Addison Wesley, 1977).
8. U.K. Ministry of Defence, 2019, *Joint Doctrine Note 2/19 Defence Strategic Communication: an Approach to Formulating and Executing Strategy*, Shrivenham, Swindon, Wiltshire, 4-17.
9. Ibid.
10. U.S. Department of the Army, 2017, *Field Manual 3-0 Operations.* Washington, DC.
11. S. Tzu, 1971, *The art of war* (Vol. 361). Oxford University Press, USA.
12. B.D. Johnson, D. Alida, J. Brown, and R.J. Ross 2020, *Information Warfare and the Future of Conflict,* Arizona State University Threatcasting Lab. https://threatcasting.asu.edu/publication/threatcasting-report-information-warfare-and-future-conflict.
13. H. Rothstein, 2007, Strategy and psychological operations. *In Information Strategy and Warfare,* Routledge, 176-202.
14. U.S. Army Training and Doctrine Command, 2018, *TRADOC Pamphlet 525-3-1 the U.S. Army in Multi-Domain Operations 2028*, Fort Leavenworth, KS.
15. S. Tzu, *The art of war* (Vol. 361).
16 B.D. Johnson, 2019, *Information Disorder Machines.* Arizona State University Threatcasting Lab. https://threatcasting.asu.edu/publication/threatcasting-report-information-disorder-machines.
17. U.S. Department of the Army, 2017, *Field Manual 3-0 Operations.* Washington, DC.
18. J.R. Galbraith, 1977, *Organization Design.* Boston, MA: Addison Wesley.
19. U.K. Ministry of Defence. (2019). *Joint Doctrine Note 2/19 Defence Strategic Communication: an Approach to Formulating and Executing Strategy*. Shrivenham, Swindon, Wiltshire.