Characteristics of Information Warfare: The Battle for the Narrative

Mark G Hazen
Anthony Isenor
Francine Desharnais
Tania Randall
DRDC – Atlantic Research Centre

22nd International Command and Control Research & Technology Symposium
Los Angeles, USA

Date of Publication from Ext Publisher: November 2017

Defence Research and Development Canada

External Literature (P)
DRDC-RDDC-2017-P136
December 2017

IMPORTANT INFORMATIVE STATEMENTS

Disclaimer: This document is not published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada, but is to be catalogued in the Canadian Defence Information System (CANDIS), the national repository for Defence S&T documents. Her Majesty the Queen in Right of Canada (Department of National Defence) makes no representations or warranties, expressed or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

Endorsement statement: This publication has been peer-reviewed and published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada. Inquiries can be sent to: Publications.DRDC-RDDC@drdc-rddc.gc.ca.

Title of Paper: Characteristics of Information Warfare: The Battle for the Narrative
Topic(s): **2 C2 Concepts Theory, Policy and Approaches**
1 Operational Issues: Coalition Command and Control
4 Cognitive and Socio-technical Challenges.

Name of Author(s): Mark G Hazen, Anthony Isenor, Francine Desharnais and Tania Randall
Point of Contact (POC):
Mark G Hazen
Defence R&D Canada
DRDC Atlantic Research Centre
9 Grove St
Dartmouth, NS Canada B2Y 3Z7
902 426 3100 x176
Mark.hazen@drdc-rddc.gc.ca

Abstract

The ubiquitous nature of information in modern warfare has increased interest by the naval community in understanding the concept of Information Warfare (IW). While the control of information has long been a significant supporting activity, the aim of this paper is to explore Maritime Information activities as they relate to a "warfare" area; that is, equivalent to the other warfare areas such as surface, above and underwater warfare. In particular, the paper examines what it means to be a warfare area with emphasis on the maritime domain. As part of this discussion, we propose Narrative Dominance as an over-arching warfare concept that provides the framework within which information warfare exists.

Caveat: The ideas and conclusions expressed in this paper are solely those of the authors and do not represent official Canadian doctrine or opinion.

Introduction

The Royal Canadian Navy (RCN), along with other allies, is investigating the implications of the information battlespace on their operations [1, 2]. The increasing volume of sensor data and ability to exchange, analyze and disseminate information is fundamentally changing the information space within which military forces operate. Not only are our military capabilities increasingly dependent upon timely and accurate information, but the results of military actions are often widely available through social and news media.

Operations to control information are as old as warfare itself, however, the use of information has in the past been seen as a supporting capability, rather than as a warfare area in its own right. In the RCN, some operational officers have questioned whether information warfare (IW) is truly a warfare area, equivalent to more traditional forms such as surface or underwater warfare. Discussion with these RCN officers formed the impetus for this paper and our investigation of maritime information warfare in the context of the RCN.

Our objective here is to address the basic question, is information warfare a “warfare area” in its own right. Although some may suggest that the answer is an obvious ‘yes’, within the RCN the question remains relevant along with the follow-on question, ‘what constitutes information warfare?’

Sun Tzu certainly recognized the importance of information on the battlefield, but arguably the modern-age thinking regarding information warfare began in the early 1990’s. Examinations by Buchan [3], Libicki [4], and later work by the US Air Force [5] began to illustrate the confusion over information warfare and its extant. These works indicated a need to break down IW into its components [3], concluded that IW was not a warfare area [4], and pointed to relationships between IW and the many other information-related operations [5]. The definition of information warfare is, therefore, variable between nations, and has continued to evolve as the nature of warfare in the new information environment has become clearer.

These early studies, and many that followed, examined the concept of IW as related to information usage and information specific operations within the military context. These papers illustrated what IW was, by relating IW to known military operations. Here, we take a different approach. We examine IW from the roots of the terms: first by considering ‘information’ and the characteristics of the information battlespace, and then by comparing the elements of warfare in this space to a NATO definition of ‘warfare area’ [6].

Characterization of the Information Battlespace

What does an information battlespace look like? In the literature and in society, there is an understanding that data, information and knowledge are related, and that they are transmitted from one person/source or place to another. There are also many different definitions of data, information and knowledge [7], with the relationships between these concepts historically described as a hierarchy [8].

In this paper we take the view that data are processed or transformed in some manner to create information. If the information is received by a decision maker who has a pending decision, and if the information is in an understandable form and of relevance to the decision, then the information has value to the decision maker. To generalize the situation, both the producer and decision maker represent nodes in this information network. When information has been internalized by a decision-maker it then becomes part of the decision-maker’s knowledge.

Thus, we characterize the information battlespace as consisting of nodes containing or using data and information, and connections between the nodes through which this content is transferred. It should be noted that this description is not limited to a computer-based network. A network of people equally qualifies.

The production of information and its subsequent usage is a complex process. Early efforts to define information science point to Brookes [9], who developed the ‘fundamental equation of information' that relates an increment of information to a change in the knowledge structure of the receiving party. Raber [10] continued the work by providing a thorough examination of information indicating that information exists in both a physical and cognitive form. This description of the space in which information exists, aligns well with the description in Kuebl [11], based upon US Joint Publication 3-13 (Feb 06), of the information environment as three interrelated domains:

- physical networks (i.e., information conduit),
- information content, and
- cognitive effects on humans.

It is this more general breakdown that we will use in subsequent discussion of the characteristics of the information space. In particular, we are interested in detailing characteristics that may be relevant to a battle within the information space.

We first consider the physical network component of the battlespace. Today's networks are constantly changing in numbers of relevant nodes, and connections between nodes. However, as the number and types of connections increase, the shape of the network is no longer strictly constrained by the physical environment. Two computer nodes that are physically side by side may be totally isolated from one another in the information space. Further, the existence of a connection between two nodes does not mean that information is passed between them. Thus, when analyzing the information space "terrain" it is important to understand not only the physical connections (i.e., both computer and non-computer based) but also the actual usage of the connections. We include in this domain the characterization of what types (or formats) of information content a link in the network can move, how fast it can be moved, what error rates are associated with the link, when the link is available, and the physics of the communication medium(s). In addition, the increasing numbers and types of communication connections between network nodes has altered the information space such that within the constraints of western culture the network has become essentially uncontrollable in shape, and in the movement of content.

Next consider the characteristics of the information content domain of the battlespace. This is the domain of "what" is moved between, and stored at nodes. In the literature, content elements are characterized by attributes such as precision, veracity and format. Given that hoaxes or factual content are both equally difficult to purge from a network, we conclude that content veracity may be better handled as a characteristic of the cognitive domain. Instead, we are interested in domain characteristics relating to how content storage, access and movement may affect the elements. While not an exhaustive list, characteristics of the content domain that may be relevant to information warfare include:

- Clone-able - content is unchanged by making multiple copies;

- Storable – content is unchanged by being instantiated in multiple forms and formats that have differing longevity;
- Non-atomic – a node may only accept part of an arriving information packet;
- Filterable – Not all arriving or stored information is re-transmitted to other connected nodes.
- Mutable - the same arriving information can lead different nodes to store different information;
- Inter-related - content is rarely unique, each element generally has some relation to other elements; the overall content of a particular sub-space is likely to have some consistency amongst its elements; and,
- Contextual - for a node to accept arriving content information, it has to have some relation with the knowledge context of that node.

Finally, consider the cognitive component. While the network connections and nodes have physical instantiations, the characterization of the battlespace in many ways has its ultimate existence in a cognitive layer; that is in the minds of decision-makers and consumers. At the operational/strategic level the RCN concept for MIW [1] notes that Maritime Information Warfare (MIW) is a war of narratives; that is for our narrative to be dominant. A dominant narrative is defined as the dominant ideas that drive a society's decisions on how society should work [12]. This idea of narrative provides a context for operations in the cognitive domain.

Many of the content characteristics given above are manifestations of how the cognitive layer manipulates received information. The accumulation and aggregation of information may then lead to the development of new knowledge and understanding, or the confirmation of previously developed knowledge and understanding, regardless of actual factual veracity [13]. This knowledge and understanding can lead to the generation of new content, and be used to formulate and direct actions.

Table 1 summarizes the characterization of the information battlespace into three domains; each with their own characteristics that may be exploited as strengths or vulnerabilities.

Table 1. Characterization of the information battlespace as broken down by domain.

physical networks	information content	cognitive effects on humans
- Constantly changing/uncontrolled shape - Near instantaneous transmission - Access to content volume - Uncontrolled movement of content - Content longevity - Disconnection from physical terrain	- Clone-able - Storable -- Non atomic - Filtered - Mutable - Inter-related - Contextual	- Veracity / acceptance of information - Accumulates and aggregates information - Develops new knowledge and understanding - Suffers from confirmation bias - Formulates and directs actions - Develops conception of battlespace that evolves - Understanding of objectives and acceptable methods: narrative

Is Information Warfare a Warfare Area?

A warfare area was defined for NATO by Ibrugger [6] in his report to the NATO Parliamentary Assembly in 1998 as:

> "a *form* of warfare with *unique military objectives*, characterised by *association with particular forces or systems*." (italics added)

Using this definition of a warfare area, there are three questions about Information Warfare that need to be answered in order to determine if it is indeed a warfare area:

- What is the *form of warfare*?
- What are the *unique military objectives*?
- What are the particular *forces or systems* with which information warfare is associated?

What is the form of warfare?

Essentially *warfare* is about convincing an adversary to do something you want them to do, but they do not want to do. Even defensive warfare is about making the adversary stop attacking. This level of battle maybe for concrete things, but may also be a battle of will. *Information* warfare therefore must be a battle *in the information space* which is aimed, ultimately, at changing adversary actions.

From our examination of the information space, information warfare can then be broken down into three general areas of conflict:

1. A battle for control of the information conduit; i.e., the flow of information;
2. A battle for control of the information content within the information space; and,
3. A battle in the cognitive domain for the narrative.

Each of these battles requires a unique, but related, form of warfare that is different from other forms of warfare. The battle for conduits is about controlling the spectrum, network routers and media. The battle of content is about controlling the integrity and quality of the information, and the battle of the narrative is about preserving our message and discounting the adversary's. Thus, we contend that there is a unique form of battle in each of the three interconnected domains and thus the first element of Ibrugger's definition is achieved.

What are the unique military objectives?

A potential objective of the modern military is complete control the information space; conduit, content and cognitive. However, in a complex world of increasing amounts of, and increasing access to, information, achieving this ideal is unlikely, without a degree of control that is currently contrary to western societal norms. Thus, in practice the military objectives are more focused on controlling the adversaries' information about our forces and objectives, and the shaping of the battlespace such that the information the adversary collects biases their decisions to align with our objectives. At the same time, we try to ensure we have valid information on our adversaries and that our decisions are true to our objectives. This situation scales from the smallest engagement to the largest strategic plan.

These objectives seem very similar to the Effects-Based Operations (EBO) concept objectives which are defined by Smith [14] as

> "coordinated sets of actions directed at shaping the behaviour of friends, foes and neutrals in peace, crisis and war."

The US Navy [15,16] has adopted the concept of Information Dominance (ID) which is defined as,

> "… the operational advantage gained from fully integrating Navy's information capabilities, systems and resources to optimize decision making and maximize warfighting effects in the complex maritime environment of the twenty-first century."

Thus, a more focussed *warfare objective* could be to achieve Information Dominance in the local battlespace and successfully implement EBO. This is in line with the ideal to control the information space and has implications for the control of conduit and content, but do not explicitly address the third area of battle: control of the narrative. It is also unclear from the concepts of ID and EBO how to define the local information battlespace, or which operations to conduct. For a particular operation the characteristics of Table 1 illustrate attributes that may need to be protected or exploited.

A war of narratives leads to a strategic/operational level mission concept of "narrative dominance" as an objective. What would Narrative Dominance entail? At the simplest level it means that our narrative - the outline of why our means, actions and effects are justified and are the best solution to the situation - is accepted by the other participants (i.e., friends, foes and neutrals). As a corollary, it also means that we need to be seen to "walk the talk", that our actions are consistent with the narrative we are putting forth. Narrative dominance means that our operations are, and are believed to be, in-line with our stated objectives, and those objectives are accepted by the other participants. Once a narrative is defined, then it provides a context for other warfare concepts.

To achieve Narrative Dominance we return to the three information domain breakdown and contend that the objectives of Narrative Dominance are:

1. control of information flow, to ensure the adversary receives only inputs and effects that will drive their decision-making towards our narrative, while we receive the information we require;

2. control of information content, to ensure we have the information to understand the adversary and can generate appropriate content and effects; and,
3. control of the narrative through operations that reinforce our narrative, by both effects and resulting information content.

Narrative Dominance thus provides a context and framework for making decisions about what information is important and what effects are needed. The Narrative Dominance concept can therefore tie together the concepts of Information Dominance and Effects Based Operations. Figure 2 provides a suggested concept hierarchy showing the relationships of the concepts and primary objectives. Since Narrative Dominance provides the context for the other concepts to operate within, it sits at the top. In this framework, the implementation of Information Dominance provides the objectives for the control of information flow and content, while EBO provides the structure for taking action. That is, to maintain sufficient control of the information space that challenges to our narrative (whether from enemy or own actions) can be identified and countered/resolved in network-based/media timescales.

At the same time, we need to understand the adversary's narratives sufficiently that we can challenge them and/or impede their ability to spread them. Thus, Information Dominance means being able to starve them of the information required for their operations or that would allow them to take advantage of situations to bolster their own narrative. We may not want or need to control all of the information space but we do need to dominate the parts that can affect the dominance of our narrative.

Thus, we contend that the unique objective of IW is the adversary's acceptance of our narrative, with this brought about through the sub-objectives that deal with the control of information content and flow that is consistent with the defined narrative (i.e., the cognitive component).

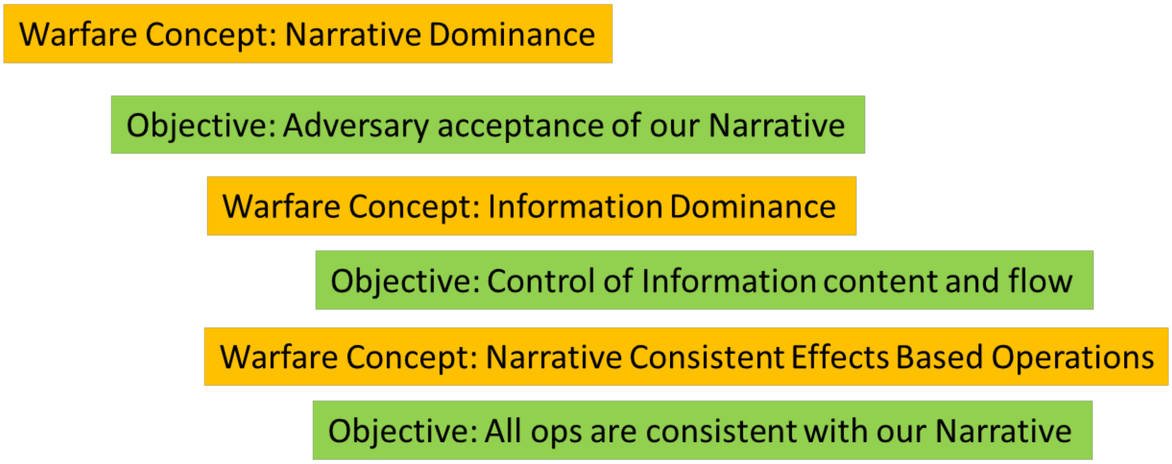
Warfare Concept: Narrative Dominance
Objective: Adversary acceptance of our Narrative
Warfare Concept: Information Dominance
Objective: Control of Information content and flow
Warfare Concept: Narrative Consistent Effects Based Operations
Objective: All ops are consistent with our Narrative

Figure 2: Proposed warfare concept hierarchy and objectives.

What are the particular forces or systems?

It follows from the above, that the systems associated with IW are those systems that impact information flow, content, or context. The control of information flow is associated with many of the systems linked to cyber warfare [17], but also elements of electronic warfare and information management. The control of content incorporates much of the intelligence world but also has aspects of cyber warfare for information security, and includes aspects of most other warfare areas that either generate or can modify information content. The control of context is dominated by public relations and information operations, is informed by Human Intelligence, and must also have a significant input into the formulation of EBO. Every one of these warfare areas has a role in implementing an IW operation, but none of them span the entire battlespace, the only force/system that does, is command and control.

However, this does not imply that IW replaces traditional warfare or that all warfare has become IW. Instead, the claim is that IW is in part about building and coordinating traditional warfare areas where they impact upon the information space. Thus, information warfare forces and systems are those that assist the decision-maker to plan and coordinate operations that will bolster our narrative while undermining the narrative of the adversary. These systems need to provide situational awareness of the information battlespace and help predict how traditional operations will affect that battlespace.

It is the function of the commander to integrate all of the forces together to achieve a particular mission or objective. The commander must consider the effect of an operation on the perception of the narrative by the adversary, local neutral and civilian organizations, allies, and national organizations. All of whom may learn of any outcome effectively instantaneously. Thus, the commander not only must understand the basic kinetic warfare issues of traditional warfare operations, but the sociological and cultural effects of those operations as communicated through conduits such as social media and word-of-mouth. They must understand complex cultural contexts that are foreign to them, and perhaps to their chain of command. On top of this they must understand the capabilities available to them to conduct their operation and protect their own information sources.

Thus, while there are specific forces that will implement specific aspects of information warfare, the particular information warfare forces are the traditional command team. The question then is, do traditional command teams have the systems and staff to comprehend and exploit the increased complexity implied by the new information space and systems.

Discussion

There was considerable discussion in the late 1990's and early 2000's on the extent of information warfare [3, 4, 18]. Buchan reports two threads, one that information warfare is over arching and the second that it is essentially limited to what is now known as cyber warfare. Over the intervening time the understanding of information warfare has evolved in a number of nations [1,2,19] from the constraints of cyber warfare, towards concepts that integrate the information space effects of all other warfare areas, without subsuming the other warfare areas.

Since warfare is about changing the decision-making of an adversary, the cognitive domain is critical to IW as it is the domain where the decisions are made. These decisions are shaped by the information being consumed by the human, including raw data, metadata, and more generally the circumstances of the evolving situation; i.e., the context. The cognitive domain attempts to connect these situational inputs into a knowledge structure [9], mental story-line, or more generally a narrative that makes sense of the situation. Control of the narrative then is a goal of IW in the cognitive domain.

The three domains of the information space may now be linked directly to the Ibrugger warfare characteristics. Table 2 illustrates through examples, how the warfare characteristics are met in the various domains. Consider two examples described by the table.

In the first example (see Table 2, superscript 1), there is a battle for control of a physical computer network. This represents the terrain and form of the conflict. The military objective for the terrain is to control (the adversary's) access to the network. To complete Ibrugger's characteristics, the scenario requires cyber defence systems to counter any such access attacks.

Similarly, a second example (see Table 2, superscript 2) can be generated using the information content domain. Here the information content may be surveillance data. Our desire to control or influence our adversary's surveillance data implies an objective to control the content in the information space. On the defensive side we employ extensive processes to validate and correlate information using picture compilation teams to ensure that the command team has the best data possible on which to base their decisions. On the offensive side, we wish to control/manage the type and quality of data available to adversaries. This implies controlled information release, signature management of blue forces, signature spoofing and other means of controlling the information content gathered by adversary surveillance efforts.

As always, the more difficult battle is the one in the cognitive domain for the narrative. In this case we want to ensure that our operations bolster our narrative, while the adversary is forced to conduct operations that undermine their narrative. On our side, this implies personnel and systems that can assess the state of acceptance of either narrative and predict the impact of operations by either side on that acceptance.

Porche et al. [18] do an in-depth analysis of information warfare in the US Army, including a review of the spectrum of warfare concepts and implementations. Our conclusion mirrors that of the Rand Study–that Information Warfare is not everything, but touches everything. That is, information warfare is an over-arching and integrating warfare area that coordinates and constrains the implementation of more specific and kinetic-based warfare areas such as anti-submarine warfare or interdiction operations where they touch the information space.

Table 2. Example relationships between the information space and the warfare characteristics. Unshaded cells are defensive aspects of a form of warfare while shaded cells are more offensive aspects. Superscripts relate to the Discussion section.

		Ibrugger characteristics of warfare			
		Form of warfare?	Military objectives?	Particular forces or systems?	Operations
Domains of the information space	Information Conduit[1]	Network[1]	Control access[1]	Cyber Defence[1]	IT Security
			Gain Access	Cyber Ops team	Network infiltration
		xHF comms	Maintain comms	Frequency hopping radio	Dynamic spectrum management
			Disrupt comms	Jamming	EW
		Emissions	Covertness	Signature mgmt.	EMCON
			Disrupt adversary sensors	Jamming	EO/IR/EW
	Information Content[2]	Surveillance data[2]	Validated/correct data[2]	Picture generation[2] (e.g., association, fusion)	ISR
			Invalid adversary data[2]	AIS[2]	Spoofing
		Social media	Control military social media footprint	IWD; Intell Officers	OPSEC
			Adversary network maps	Intell apps (e.g., web crawlers)	Intell. Ops
	Cognitive	Narrative	Narrative consistent decisions-	C2 teams, Planning systems	EBO
			Influence adversary decisions	Psy Ops teams; public affairs	Information operations
		Situational Awareness	Trusted understanding of battlespaces	Holistic cross warfare awareness system / IW Team	Targeted ISR
			Adversary confusion	Planning Teams	Spoofing; Feints

xHF: generalized High Frequency (e.g., UHF, VHF);
EW: Electronic Warfare;
EMCON: Emissions Control;
IT: Information Technology
IWD: Information Warfare Director
AIS: Automatic Identification System
OPSEC: Operational Security
EO: Electro optical
IR: Infrared
ISR: Intelligence, Surveillance and Reconnaissance

The Porche et al. [18] study recommends that information warfare officers should be implemented at the command level to provide a combination of coordination and advocacy. We go slightly further though, in advocating that full sense-making and planning of appropriate effects based operations requires personnel and systems that fully understand the information space – what information is available, what is not, the quality of the information, what information the adversary is likely to have, etc. Thus, commanders need staff trained in modern information systems and analyses, and that staff needs to include personnel that understand the adversary as well as a deep understanding of the capabilities and limitations of the available information sources, networks and analyses.

Conclusions

In the most general sense, the military objectives of information warfare are to present the adversary (i.e., the targeted decision maker) with information such that they make a decision that complies with our objectives. The adversary must believe that the information they are using is trustworthy and that it does not allow any other decision besides the one we want them to make. Likewise, we must collect and protect our information so that it is not vulnerable to similar attacks. In order to achieve this we need to understand what information will sway the adversary to a decision complying with our objectives and what is needed to maintain our own will to adhere to our objectives. We need to understand the battlespace, and how the adversary views the battlespace.

Using a three domain taxonomy of the information space (i.e., conduit, content and cognitive), Ibrugger's definition of warfare (i.e., form, objective, forces/systems), and a broad definition of information warfare as an integrating warfare concept, it was determined affirmatively that information warfare should be considered a warfare area of its own. It has a distinct form of warfare, objectives and forces. However, it is not a radically new warfare area, but instead an evolution of traditional command responsibilities required to respond to the evolving information space. A distinction is made between particular tactical activities of traditional warfare areas, and the holistically interconnected activities in the information space. In this information age there are few, if any, isolated actions that will not have ramifications in the information space.

While the battles for information conduits and content are relatively easy to understand, given the extent of the information space, they can also be over-whelming. It is the third information domain, the cognitive, that provides the context to make these battles tractable. We have argued that the context can be provided by the concept of narrative dominance, which then provides a means to determine appropriate objectives in the conduit and content areas of the information space. We define narrative dominance as establishing our narrative as the dominant set of ideas for the conflict area, and have argued that under this context it is then easier to see how concepts such as information dominance and Effects Based Operations apply and should be implemented.

It is further argued here that specialized personnel and systems are needed to assist command teams to understand the information space, the state of the narrative, how to predict the effect of an operation upon those narratives, and how to integrate the tools at hand into operations that will achieve the objective of blue narrative dominance.

References

1. Director General Naval Force Development, Concept for Maritime Information Warfare, June 2015.
2. Blakely, D. Information as war: the RCN comes to grips with a new battle space. Crowsnest. Summer 2017, 12 July 2017. http://www.navy-marine.forces.gc.ca/en/news-crowsnest/crowsnest-view.page?doc=information-as-war-the-rcn-comes-to-grips-with-a-new-battle-space/j46ylklz. [Accessed 5 Sept 2017.]
3. Buchan, G. (1996), Information War and the Air Force: Wave of the Future? Current Fad?, RAND Corporation, Santa Monica CA.
4. Libicki, M.C. 1995. What Is Information Warfare, CCRP, http://www.dodccrp.org /html4/books_downloads.html [Accessed Jan 2015].
5. United States Air Force (1998), Information Operations, (Document 2-5) US Department of Defense.
6. Ibrugger, L. 1998. The Revolution in Military Affairs. NATO Parliamentary Assembly report. http://www.naa.be/publications/comrep/1998/ar299stc-e.html [Accessed 3 February 15].
7. Rowley, J. 2007. The wisdom hierarchy: representations of the DIKW hierarchy, Journal of Information Science, 33 (2), 163-180.
8. Ackoff, R.L. 1989. From data to wisdom, Journal of Applied Systems Analysis, 16 (1), 3-9.
9. Brookes, B.C. (1980), The foundations of information science Part I. Philosophical aspects, Journal of information science, 2 (3-4), 125-133.
10. Raber, D. (2003), The Problem of Information: An Introduction to Information Science, Lanham, Maryland, and Oxford: The Scarecrow Press, Inc.
11. Kuebl, D. 2007. Introduction: “Brother Can You Spare Me a DIME”, Information Warfare: Separating Hype from Reality. Ed. L. Armistead. Potomac Books, Washington.
12. http://www.answers.com/Q/What_is_a_dominant_narrative [Accessed 17 Mar 2015].
13. Jonas, E., Schulz-Hardt, S., Frey, D. and Thelen, N. (2001), Confirmation bias in sequential information search after preliminary decisions: an expansion of dissonance theoretical research on selective exposure to information, Journal of personality and social psychology, 80 (4), 557.
14. Smith, E.A. 2002. Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis and War. CCRP Press Nov 2002. ISBN1-893723-08-9

15. U.S. Navy Information Dominance Roadmap, 2013-2028. March 2013. http://www.public.navy.mil/fcc-c10f/Strategies/Information_Dominance_Roadmap_March_2013.pdf. [Accessed 14 Sepember 2017].
16. U.S. Navy Information Dominance Roadmap 2013-2028: Synchronizing Navy's information and operational environments to fight and win. Deputy Chief of Naval Operations for Information Dominance., http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=4676 [Accessed 3 Nov 2014]
17. Knight, R. and McIntyre, M. (2005), An operational framework for battle in network space, In Proceedings of 10th International Command and Control Research and Technology Symposium, McLean, VA.
18. Porche, I.R., Paul, C., York, M., Serena, C.C., Sollinger, J.M., Axelband, E., Min, E.Y. and Held, B.J. 2013. Redefining Information Warfare boundaries for an Army in a Wireless World. Rand Monograph 1113, Rand Corporation.
19. Ventre, Daniel. Cyberwar and Information Warfare. Wiley, London. 2011. ISBN: 9781848213043.

AUTHOR BIOGRAPHY

MARK G. HAZEN is a senior scientist in the Maritime Decision Support Section at Defence R&D Canada – Atlantic Research Centre. He has an MSc in Mathematics from Carleton University and 31 years of experience in defence research using modeling and simulation to support operations and capability development. He has led projects in a wide variety of maritime warfare areas ranging from anti-ship missile defence to C2 for harbour force protection. His current research interests are in the area of naval command support, predictive situational awareness, planning support systems, human-in-the-loop command and control experimentation, and distributed simulation.

ANTHONY W. ISENOR is a scientist in the Maritime Decision Support Section at Defence R&D Canada – Atlantic Research Centre. He has an MSc in Physical Oceanography from Dalhousie University. He has led projects dealing with technologies for trusted Maritime Domain Awareness (MDA), is past member of the NATO research group on Semantic Interoperability (i.e., IST-075) and current member of NATO IST Exploratory Team 097 on Cloud Computing Technologies for C2. He has extensive experience with vocabularies and systems that support MDA.

FRANCINE DESHARNAIS is the Head of the Maritime Decision Support (MDS) Section at Defence R&D Canada – Atlantic Research Centre. She has an MSc in Physics from Université du Québec à Montréal and has led the MDS Section since 2008. She is the senior advisor to the Canadian Maritime Information Warfare program, is Lead for Maritime Information Warfare under The Technical Cooperation Panel (TTCP) Maritime Group, and is the Canadian Principal Panel Member on the NATO Information Systems Technology Panel.

TANIA RANDALL is a scientist in the Maritime Decision Support section of Defence R&D Canada – Atlantic Research Centre. She has an MSc in Mathematics from Dalhousie University and her main research interests are in the area of interface design and concepts to support decision making. She has lead activities in naval fires support command and control, as well as task analyses and information requirements for naval planning team personnel at the ship and task group levels. She is currently engaged in activities related to decision support for the naval operational planning process, including identification and visualization of course of action criteria and metrics, and the exploration of novel interface concepts and technologies.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Atlantic Research Centre
Defence Research and Development Canada
9 Grove Street
P.O. Box 1012
Dartmouth, Nova Scotia B2Y 3Z7
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Characteristics of Information Warfare: The Battle for the Narrative

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Hazen, M.G.; Isenor, A.; Desharnais, F.; Randall, T.

5. DATE OF PUBLICATION (Month and year of publication of document.)

December 2017

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

14

6b. NO. OF REFS (Total cited in document.)

19

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

External Literature (P)

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Atlantic Research Centre
Defence Research and Development Canada
9 Grove Street
P.O. Box 1012
Dartmouth, Nova Scotia B2Y 3Z7
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

01da; 01db

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2017-P136

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11a. FUTURE DISTRIBUTION (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Any limitations on further dissemination of the document, other than those imposed by security classification.)

12. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

13. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

information warfare; narrative