"The Fourth Wish"

An Essay on the Need for an Operational Information Management Concept to Improve Situational Awareness in Canadian Military Operations

Captain (N) D.W. Knight
Joint Forces Capabilities
NDHQ
101 Colonel By Drive
Ottawa, Ontario K1A 0K2
CANADA

knight.dw@forces.gc.ca

THE PARABLE OF THE OPERATOR AND THE TECHIE

Between crises, the proverbial Canadian Forces "operator" spent his time contemplating the military of the future. There were so many competing demands, and it was all very complicated. One day, the operator happened upon a magic lamp. When the lamp was rubbed, a genie appeared, endowed with magical skills in information technology (IT). The genie was called "the techie", and he granted the operator three IT wishes. The operator could not believe his good fortune, and he called upon the techie to solve the most vexing of his IT problems – how to use the power of IT to gain the "situational awareness" needed to command and control modern military operations. For his first wish, the operator commanded: "let there be machines to help us collect and display the information we need"! "Yes sir" said the techie, and computers were given to the operator. And it was good, until the operator realized that the computers were not compatible with one another. So the operator called for his second wish: "let all of our computers be interoperable"! And the humble techie readily complied with this wish by creating the concept of the Joint Command and Control Information System. And it was very good. The operator believed that with one more wish he would have the tools for complete situational awareness, and thus he blurted out "let the computers talk to one another so we may share information and build our knowledge"! "Yes sir" said the techie, and the computer systems of all the services and commands were joined in a series of remarkably efficient networks. And the result was brilliant. The jubilant operator shouted: "at last I have situational awareness"! Alas, it was not so. In spite of all the computers, and all the networks, ***something was missing****. Feeling the growing wrath of the operator, the techie scurried back into his bottle, leaving with these words: "You've had your three wishes, and I cannot grant you a fourth. Besides, you now have all the tools required to create the situational awareness you seek – all you have to do is make them work together!" And thus the operator returned to his contemplation, pondering the techie's words and muttering to himself "if only I had just one more wish…"*

Knight, D.W. (2005) "The Fourth Wish". In *Visualisation and the Common Operational Picture (COP)* (pp. KN1-1 – KN1-10). Meeting Proceedings RTO-MP-IST-043, Keynote 1. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

INTRODUCTION

Strategy 2020[1] is a well-articulated and prescient document that portrays how the Canadian Forces must be developed to operate in the new millennium. With the requisite effort by all members of the defence team, this ambitious vision can be made reality. As with all large undertakings, Strategy 2020 must be broken down into constituent parts and accomplished one piece at a time. One of the foundation pieces, or "enablers" of Strategy 2020, is the concept of "situational awareness", the age-old problem of understanding the operating environment so that timely and effective decisions can be made on the employment of military force in operations ranging from disaster relief to high intensity combat. Leveraging on the "command and control"[2] technology advantages enjoyed by western military forces, the Canadian military needs the ability to generate situational awareness for domestic operations, peacekeeping, and coalition operations with allies, especially the United States[3]. Those with a superficial knowledge of military command and control might believe that the challenge of attaining situational awareness has already been met. Those that have been intimately involved in operations in Kosovo, East Timor, Bosnia, Africa, and the Persian Gulf would say otherwise. As operators involved in these conflicts have struggled to push and pull essential operational information through a multitude of networks, changing data formats and crossing security domains along the way, the result has been anything but "situational awareness". If these operators had a fourth technological wish, what would it be?

As a literary device, the "parable of the operator and the techie" serves to describe, in simplistic terms, the many torturous and difficult years that have been dedicated to the development of the military's command and control architecture. While the accomplishments have been magnificent, the details would be too lengthy and dull to recount. The salient point is that information technology and the people that know how to build it, "the techies", have delivered an outstanding command and control capability to the operators of Canadian military – but something is still missing. The missing piece, the one that will join the command and control capabilities to the broader vision of situational awareness required for Strategy 2020, is a clear and workable concept for **managing the operational information** made available by the command and control systems. As military professionals, our "fourth wish" should be for such a concept. Of course in the real world, military forces do not achieve their objectives by making wishes. Thus the aim of this essay is to outline a conceptual action plan for the management of operational information as a stepping stone to "situational awareness".

PROBLEMS WITH THE "INFORMATION PICTURE"

"Situational awareness", or collectively knowing "what is going on", is the key to decision-making and the employment of military forces. From a military perspective, the notion of situational awareness is embodied in the "information picture" seen by the operational commander and shared with others in the operating space. This "picture", which is actually a constantly changing collection of knowledge, assessments, and reference

[1] Defence Strategy 2020 is a paper prepared by the Canadian Department of National Defence. It is available on the internet at http:/www.vcds.dnd.ca/cds/strategy2k/s2k08_e.asp. At related article by Canada's Vice Chief of Defence Staff, Vice Admiral G.L. Garnett, entitled "The Canadian Forces - More Capable in an Unpredictable World", is published in by the Conference of Defence Associations Institute in the 29 June, 2001 edition of "On Track" (Volume 6, No. 2).

[2] The term "command and control" is used in this paper to describe the information technology, sensors, and networks sometimes referred to as "C4ISR", meaning the Command and Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance systems that support military operations.

[3] The US military's approach to the future is embodied in "*Joint Vision 2020"*, produced under the authority of the Chairman of the Joint Chiefs of Staff, US Government Printing Office, Washington DC, June 2000. The integration of command and control technology in joint operations is a major theme of this document.

material, is called the "common operating picture", or COP[4]. For the type of military operations envisioned for Canadian Forces through 2020, there will be a vital linkage between situational awareness, decision-making, and the COP. While the creation of a COP might seem fairly simple for a small group or a single type of force, it is extremely complex when dealing with different types of forces, other government departments, and allies. The underlying challenges of situational awareness are therefore to make sure that information **can** be shared, and that there actually **is** a common operating picture from which to build awareness and base decisions. The problem is that neither of these challenges, which revolve entirely around information management, are being adequately addressed by the leaders of our military, the operators. Instead, responsibility for the COP and it inherent information management problems has been delegated to the "techies", who ultimately have neither the authority nor the operational knowledge to deliver the "information picture".

Military forces are, by their very nature, huge producers and consumers of information. Readiness, transport, logistics, intelligence, plans, combat – all of these real world activities are represented by constant streams of information and reports that crisscross the organization and in turn perpetuate further activity. Virtually all of the activities of the military are now supported by IT, but like many corporate entities, the military has struggled to adapt. In very general terms, military personnel fall into four categories of adaptation to IT[5]:

A) There remains a small, but dwindling core of non-adapters, those who try to limit their interaction with IT. Some of these people, referred to lovingly as "dinosaurs", or "Luddites", have taken refuge in the next category.

B) Most organizations within the military have used IT to **automate their paper trails**. Working within their traditional structures, they have used computers to generate the same papers, reports or briefings they would otherwise have done manually. They are more efficient at churning out paper, but not more effective in executing their work in an IT environment.

C) Some of the more adventurous communities within the military have gone further with automation, but they have done so by developing specialized computer applications within their own narrow fields. Most prevalent in support organizations, these applications are known colloquially as "**information stovepipes**", because they are non-interoperable and tend to isolate information.

D) There are people in the military who realize they must fundamentally change their organizational and work processes to obtain the full benefits of IT, but they cannot, by definition, achieve their goals in isolation. The logic of network computing dictates that they and their organizations cannot achieve their goals in the absence of an **over-arching information management strategy** that would unify the entire Canadian Forces.

From a situational awareness perspective, the impact of this less-than-total adaptation process has been quite substantial. While IT has significantly increased the volume and speed of information flow, "automating the paper trail" has resulted in staffs struggling more than ever before to find, extract, process, and disseminate the essential information required by operational commanders. The technical concept of the Joint Command and Control Information System (JC2IS) has done wonders to help build the interoperable computer network required to build the COP. However, in the absence of a concomitant joint information management concept

[4] Keynote Address by the Principal Deputy Assistant Secretary of Defense (C3I) to the C4ISR Operational and Technical Lessons Learned in Multi-National Operations Technical Exchange Meeting, Tyson's Corner Virginia, 19 October, 1999.

[5] For more information on adapting to information technology, see Shoshana Zuboff, *In The Age f the Smart Machine,* Basic Books, Inc, New York, 1984.

led by operators (the end-users of the COP), the net effect of JC2IS is, and will continue to be, a disparate collection of shapeless information "stovepipes" gathered in a single box with limited interoperability. In effect there is no COP in the CF, at least not in the sense of the COP required for situational awareness. Probably the most revealing insight as to the poor state of the COP, in peacetime or in crisis, is the long line of briefing officers, each with their own stand-alone "PowerPoint"[6] slides, required to brief a Joint Force Commander. The *de facto* COP is created in PowerPoint and exists only for a brief period in the minds of those in the room. Each briefer prepares his "stovepipe" input in isolation, shows it for a few moments of briefing time, and then the graphics are filed away until the next briefing – and thus the closest thing to a COP is filed away too. Just like the old days, but with better IT support! Ultimately the real problem with the COP lies not with "techies", nor technology, but with the operators who should be leading its development.

THE JOINT OPERATIONAL INFORMATION CONCEPT

Command and control is all about decision-making, the art of "turning ideas into action".[7] In order to make sound and reasonable operational decisions, commanders at all levels require a multitude of information. Readiness reporting, logistics, intelligence, weather, terrain, politics, enemy positions – all of these information elements and a host of others constitute what I call **operational information**; that is, any information needed to support operational decision-making. The thrust of the Joint Operational Information Concept (JOIC) is to ensure that all applicable operational information is provided to a military commander in a single command and control system, when he needs it, and in a format that he can use immediately and share with others quickly. This is a tall order, but one that is entirely achievable, not through the acquisition of more technology, but through the deliberate evolution of information management techniques and procedures.

Figure 1 depicts the "triad" of operational information management. Most people think of a command and control system as a computer, or a network of computers. In fact, computers and communications systems constitute only one part of the command and control system. The foundation of any command and control system is actually the operational information being fed into it. The information is processed through the various computer networks and communications (C4ISR) systems. The magic of command and control occurs when skilled and talented personnel interact with the system to make it really work – to "turn ideas into action". Under the JOIC, the operational information, C4ISR systems, and personnel are all orchestrated under a unifying information management strategy, led by operational commanders, to create the COP.

[6] PowerPoint is the registered trademark of a graphics package produced by Microsoft Corp.

[7] Micheal S. Loescher in "The Rise of Command and Control", *Cyberwar 2.0: Myths, Mysteries, and Reality*, Ed. Alan D. Campen and Douglas H. Dearth, AFCEA International Press, Fairfax, VA, 1998.

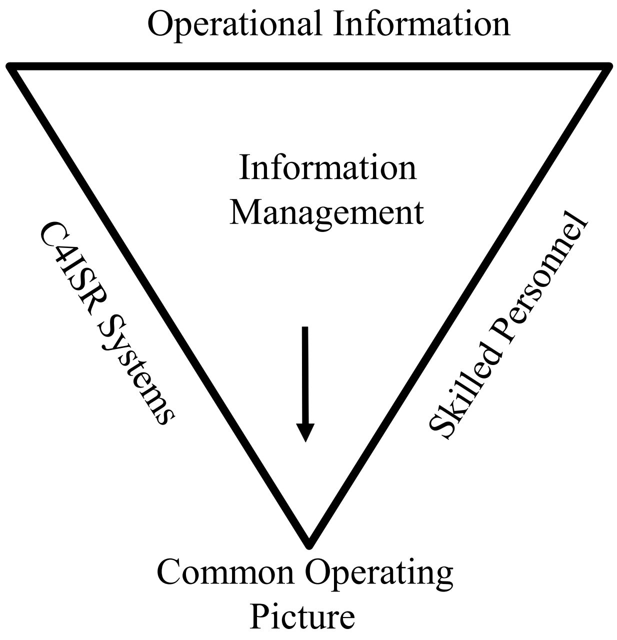

Figure 1: The Information Management Triad.

How is a COP created? Fig 2 shows, in very simple terms, the information flow needed to establish a COP. All incoming operational information falls into two basic categories: **current information** or **background information**. "Current" information, such as unit positions, sensor feeds, and contact reports, is very time-sensitive and must be plotted and viewed immediately on a geo-referenced display for it to be of value. The hardware and software already available through the geo-referenced display component of JC2IS provides a great medium to display unit positional and contact information. "Background" information is all the supporting information relevant to a given problem that fills reference databases, providing depth and context to the current information. Most background information is organized into a variety of databases, many of which are classic "stovepipes", but which are slowly converting to a web-enabled, standards-based, architecture. The goal of the JOIC is to have both current information and background information databases visible and inter-connected on a single screen that will display the COP. The COP is created when **those that are involved in an operation** compare, contrast, and analyze the relevant current and background information together to develop an assessment, or picture, of what is going on in a given situation. Thus a "man-in-the-loop" is essential to the maintenance of the COP. The value of the COP is measured by its content, accuracy and by how frequently it is updated and shared. Based on a good Common Operating Picture, an operational commander can make **sound decisions** and order **effective action** by his forces. A COP that is not seen by all, or that is out of date, is not a COP at all. A COP that is inaccurate or incomplete is dangerous.

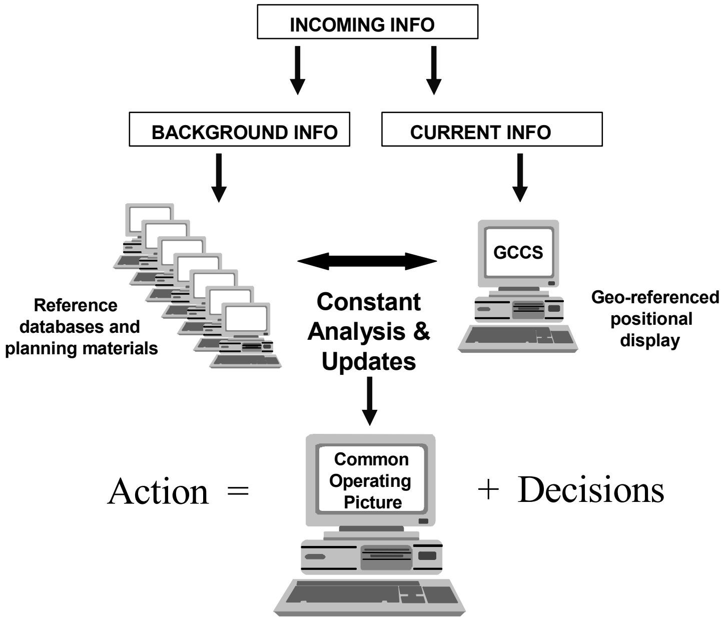
INCOMING INFO
BACKGROUND INFO
CURRENT INFO
Reference databases and planning materials
Constant Analysis & Updates
GCCS
Geo-referenced positional display
Action =
Common Operating Picture
+ Decisions

Figure 2: The Flow of Operational Information.

By way of illustration, here is how the information flow described above might be used in a notional scenario:

> *"There is a revolution in a far off land, and many foreign nationals, including a number of Canadian citizens, are caught in a dangerous situation. An ad hoc coalition force is brought together at short notice to carry out a Non-combatant Evacuation Operation (NEO). Canada contributes a joint force contingent to the coalition operation.*
>
> *The Canadian contingent commander takes a quick look at his Command and Control System to see what is known about current friendly and enemy force dispositions as the sensor feeds begin to flow. The country in question has been thoroughly studied over the years, so there is a vast array of background intelligence, environmental data, and infrastructure information readily accessible in the reference databases. Own force readiness and capabilities, to include critical deficiencies, are quickly reviewed, as are the assigned rules of engagement, logistics factors, and political constraints. In conjunction with coalition partners, a threat assessment and an estimate of the situation are quickly conducted. A set of options is developed and shared with subordinate forces and higher HQs, with everyone collaborating on the computer network to bring the necessary expertise to bear on the problem. The Coalition Commander selects the best option and starts planning, drawing on readily available templates and advice from coalition partners. Information gaps are identified and filled as quickly as possible. Material deficiencies are rectified and forces are augmented as the situation permits. Detailed orders are issued, indications and warning criteria are established, sensors are tweaked, and contingency plans are made.*
>
> *As the operation commences, commanders at all levels are focused on the Common Operating Picture. As events unfold, they are displayed on the plot. Enemy defenses are suppressed and*

> *enemy leadership is rendered "blind" through well-targeted information operations. Urgent queries are run against the reference databases to support urgent decisions and rapidly changing operational activity. All forces involved act with speed and precision, concentrating their combat power effectively and decisively. Higher HQ, coalition partners, and subordinate forces are able to keep abreast of the overall situation by unobtrusively viewing the COP. Selected elements of the COP are extracted in softcopy form and used to inform political leadership, the media and the public. Everyone involved in the operation is doing what they are trained to do, and they are using the same weapons, sensors, and information systems they have been trained to use…*
>
> *Hopefully the operation succeeds. In any event, the COP, will be cited as a major strength in the operation. The positional display worked well because the operators use it all the time, and it is fed with data from trusted and reliable sources. The reference databases were helpful because they were filled with relevant, well-organized and detailed information that could be accessed quickly. The interface between the current and background information was smooth and efficient, allowing the operators to rapid-fire queries, display output information as desired, and develop the best decision-making picture possible. Common data formats and compatible network configurations allowed essential information to flow freely between coalition members. Finally, behind the scenes in each of the headquarters elements, there was* ***someone*** *who made sure the COP worked..."*

The above scenario represents "situational awareness" in action, demonstrating many of the supporting elements of the JOIC. This scenario certainly does not reflect today's reality. In today's reality, geo-referenced positional displays are not worked at the joint level each day. Geo-referenced positional displays are not inter-operable, and are usually used in a single service context, leaving a Joint Force Commander to look at a variety of displays to interpolate the COP in his head. The reference databases exist, but they are not necessarily well populated with information that is relevant to operators. Furthermore, most of the "stovepipe" reference databases are not yet accessible by operators, and the operational information contained in these databases is formatted and shaped to suit the producers, not the users. In the absence of standard data formats, linked networks, and practical "cross domain" security policies, feeding information to higher HQs, subordinate units, coalition partners, and the media is very difficult and time-consuming. Finally, there is no smooth interface between current and background information that facilitates the iterative process of building the COP. As noted earlier, the COP is really not a COP at all. I contend the main reason for the deficiency in the operational information flow is the lack of leadership and management effort dedicated to making it work. As soon as an operator takes charge of the COP, the real COP that is the product of operational information management, it will be made to work. The JOIC is all about making the transition from the current reality to the COP required for situational awareness.

MAKING THE TRANSITION

The most effective means of making the transition between the inefficient information management techniques of today and those that will be required in 2020 would be to start some form of a JOIC now, and build on it through incremental improvements. One method might be to form a parallel ops centre team in an operational HQ environment, perhaps manned by some innovative individuals with the requisite operations experience and some computer savvy. Another method would be take an existing Joint HQ team, give them the required technology, and mandate them to produce and share all of their operational information in a "paperless" environment. I am inclined to believe that the latter method, if rigorously pursued, would yield the best results simply because of the day-to-day imperatives imposed by "real" operational responsibilities. Perhaps some combination of the two approaches would also work. In either case, there would be many common elements. As a means of demonstrating the implementation of the JOIC, I would propose the following ten "common" steps as an initial guide:

1) **Chose a leader** – From amongst the operators in the staff organization, appoint a "leader" for the common operating picture. This could be the Chief of Staff, the J3, or a separate staff officer[8] in a new billet. In any case, the selected leader must be empowered to act for the Commander in shaping the operational information environment on the command and control system.

2) **Designate a single command and control system as the focal point** – In the Canadian context, the selected communications network would be at the Secret level and the target command and control system would be JC2IS, including related systems in the army, navy and air force. All databases supporting JC2IS would either be formatted for positional display or be web-enabled. Metadata standards compatible with our US allies would be applied and enforced.

3) **Ensure all info sources point at the command and control system** – This would be a high level order from the DCDS level to ensure that all organizations designated as operational information providers make their databases interoperable with JC2IS. While this order has already been given with respect to connectivity and technical compliance, a similar order has not be given to govern data standards and information content. By this order, all operational information would be made available "on-line", visible to higher and lower HQ elements on the network.

4) **Organize the Commander's operational info requirements and displays** – Starting with the Commander's daily brief, shape all of the required operational information into a format for management and display. Work backward from this format to instruct information providers as to how to prepare and update their information. When assembled on the web in the correct order, briefings should be clear and comprehensive enough for anyone to understand, regardless of whether they are actually present at a formal delivery. By making information providers conform to a format, they will be forced to adjust their databases and procedures to support the requirement. Putting the Commander's daily briefing "on-line" is just the first step on the road to building the COP. Over time, through experience and feedback, the operational information environment required for the COP will grow. Eventually the predilection with briefings can be made to disappear, and information can be updated more frequently as operational requirements demand.

5) **Assign specific operational information production duties** – Almost everyone in the military, particularly at the operational HQ level, has information reporting responsibilities. Formalize these responsibilities and turn them into specific tasks, with reporting schedules and content requirements clearly assigned. Instead of using daily message reports, have the same information entered into a database and made visible through a web browser. Timings and level of detail can be adjusted to meet operational requirements, but the discipline of routine reporting must first be instilled. Just as a military phone directory lists names, duties and phone numbers, a list of information production authorities could be produced. As "on-line" information production flourishes, cross-links between organizations and the cross-pollination of operational information will grow exponentially. As the population of well-organized data grows, more effort can be invested in the aggregation and analysis of information to derive the really valuable knowledge that will become available.

[8] In a presentation by VAdm A.K. Cebrowski to the US Naval War College Foundation (Senate Chambers, Washington DC, 5 April 2000), the Admiral suggested that, in the emerging "network centric warfare" environment, the lines between different types of operations officers and specialists in the fields of information warfare, intelligence and cryptology would begin to blur. Thus it would be possible for such specialists to be assigned the lead in information management.

6) **Use the command and control system every day –** If the command and control system is going to be used in a crisis, then it should be used by operators every day, all the time. This daily use would include support to deployed operations, which will always be the most demanding on the system. Through the establishment of an information environment that operational commanders at all levels view each day, a natural focal point will be available in times of crisis.

7) **Leaders must actually use the command and control system –** A command and control system will only work if the leaders it supports actually use it. Commanders are busy, and they need to focus their talents on issues, people, and decision-making. However, regular scrutiny of the command and control system, even if only during daily briefings, provides feedback and incentive to information providers. The assigned leader for the COP needs to be particularly active in this regard, providing constant direction, encouragement, and constructive criticism to producers.

8) **Ensure full participation and compliance** – The leader must ensure that all contributors of operational information disseminate their products on the network, in the required format, and with the required content. Information producers must be rewarded for timeliness, accuracy, and clarity in their reporting, and punished if they fail to meet expected standards. If high standards are set and enforced for all on a routine basis, the discipline required to build a true COP will be available when it is needed most.

9) **Reorganize as required to shape the information environment** – The existing staff organization may not be the ideal one for supporting the COP in a modern IT environment. By developing the COP incrementally as suggested above, new and more effective processes and personnel assignments will come to the fore. Leaders will have to recognize when changes are required, and not be afraid to act accordingly to improve the operational information flow. Eventually, common procedures will begin to evolve across staffs at all levels.

10) **Don't wait for magic technical solutions** – Above all, don't wait for the "Techies" to invent the ideal command and control system. Work with available resources and improve incrementally. Use day-to-day work experiences and information products as the basis for articulating very specific IT requirements. Share "best practices" with other organizations, and encourage personnel to try new ways of facilitating the information flow.

FINAL THOUGHTS

To be sure, Canada and its military allies have access to the finest information gathering systems in the world, the most sophisticated computer networks, and a dedicated workforce of remarkably skilled and talented personnel. With one exception, all of the required components are available to achieve the kind of situational awareness envisioned in 2020. The missing piece is a comprehensive information management strategy that would unite the other components in a joint effort to create the Common Operating Picture. The Joint Operational Information Concept seeks to provide that missing piece.

Taken in the context of other military operations and activities, operational information management is certainly not the greatest issue facing modern military forces. That being said, to borrow a phrase often used by army personnel, the management of operational information is the "long pole in the tent" of situational awareness – an issue that must be resolved before the real work can get done. Vice Admiral Cebrowski, President of the US Naval War College, has referred[9] to information management as a precondition for

[9] *Ibid*

success in future operations, but also as an activity that should eventually fade into the background as we get good at it. Indeed, the Admiral referred to information management in the current context as an impediment to command and control, hindering quick and efficient access to essential information. In keeping with these thoughts, the real goal of the JOIC is not information management itself, but rather the removal of impediments to effective command and control caused by poor information management. If pursued aggressively, the operational information management problem will be solved, and the JOIC can fade into the background where it belongs.

Is the Joint Operational Information Concept outlined in this paper the best way to solve the information management problem and build the COP? Perhaps not, but the JOIC is certainly superior to the existing alternative, which is to wish for an information management miracle! As has been the case in other fields of military innovation, the first and most important step is leadership. Having purchased the computer networks and set the goal of situational awareness, it is time for our operational leaders to step forward and take the lead in the JOIC. Wishing for a magic technical solution is not an acceptable substitute for action – certainly not when all the tools required to build a real Common Operating Picture are already at hand. Neither the COP nor the information management strategy outlined in the JOIC will ever be perfect, but they should always represent the best that can be done with the resources available. Strategy 2020 is a grand vision, and situational awareness is a viable supporting concept. With a concerted effort in information management, one of the barriers to attaining situational awareness will be broken down. So let us stop wishing, and start working.