

United States Marine Corps
School of Advanced Warfighting
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

FUTURE WAR PAPER

TITLE:

Sharing of intelligence in future military operations

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES

AUTHOR:
LtCol Eldar Berli

AY 2005-2006

Mentor: Dr Brad Meyer

Approved: _____

Date: _____

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 2006		2. REPORT TYPE		3. DATES COVERED 00-00-2006 to 00-00-2006	
4. TITLE AND SUBTITLE Sharing of intelligence in future military operations				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) United States Marine Corps, School of Advanced Warfighting, Marine Corps University, 2076 South Street, Marine Corps Combat Development Command, Quantico, VA, 22134-5068				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 35	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Table of Contents

Disclaimer.....	ii
Executive Summary.....	iii
Preface.....	iv
Introduction.....	1
A future solution for access and sharing of intelligence.....	3
Secrecy and protection of sources.....	7
Collection and analysis.....	8
Organization and cooperation.....	10
Operations concepts.....	13
Conclusion.....	14
End Notes.....	16
Bibliography.....	20

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

EXECUTIVE SUMMARY

TITLE: Sharing of intelligence in future military operations

AUTHOR: Lieutenant-Colonel Eldar Berli, Norwegian Army

THESIS: Effective future military operations require distribution and sharing of intelligence across national lines and on the tactical level that far exceeds today's reality, and to make this happen, the military commander in the field should be given Operational Control (OPCON) of the multinational intelligence assets in his operations area.

DISCUSSION: Intelligence can be shared in a networking fashion between units on all levels within a Multinational Joint Task Force. To effectively achieve unity of effort in a multinational operation, national intelligence cells have to be integrated in the task force. Secrecy of sensitive information can be maintained by separating the source and method from the intelligence product, and also by keeping highly sensitive intelligence separate from the rest by a national line directly to the commander. Raw data can be issued on lower levels without any analysis as the task force largely is developing its own intelligence. The national intelligence cells' main role will be to work for the CJTF commander, but will also need to continue to support their home authorities. The balance between secrecy and openness must in any case shift considerably toward openness from today's reality. Human intelligence will remain very important in the future and it will be done more and more by ordinary troops on the ground, a development which points to the need for multinational integration of intelligence since the operations area will be manned by troops from several nations. Furthermore, for analysis, multinational intelligence will be highly beneficial in the increasingly complex and diffuse environments of the future, where the need for knowledge and skills will exceed what any single nation can provide. The ability to network will be crucial, and this includes access and dissemination of intelligence. Specifically, it is obvious that the intelligence process will have to be pushed down to low-level units. Operations concepts which currently seem to be continued or implemented in the years ahead are all dependent on sharing of intelligence in an extended way to be effective in future wars.

CONCLUSION: Intelligence will remain a national property also in the future, but sharing of intelligence should be the norm and not the exception. The existing culture in the intelligence community will need to change, on all levels from the strategic to the tactical. By giving the CJTF commander OPCON of assets it will be possible to push the intelligence process down to tactical level and utilize intelligence in a networking fashion. There will always be legitimate restraints on the flow of intelligence, but the balance has to be improved between secrecy and sharing. Likely operations concepts in the coming 10-20 years will require increased ability to share information. When put in a coalition or alliance context, it follows that effective future military operations require distribution and sharing of intelligence across national lines and on the tactical level that far exceeds today's reality.

PREFACE

In this paper I have not used classified sources. The unclassified sources are however sufficient to draw conclusions relevant for the theme. The paper is based mainly on U.S. sources and the reasoning and arguments are basically related to American and American/coalition factors but has relevance for all nations participating in multinational operations.

“Quick access to useful intelligence remained a major battlefield problem (in Iraq). Intelligence access is constrained by policies that restricted dissemination and use, especially at the tactical level.”¹ LTG Keith B. Alexander, DCINT

Introduction

Nations go to war for national interests. War, as foreign policy, is based on domestic policy both for small powers and great powers and intelligence is in this context viewed as a national asset and a national property. Intelligence is information, which means power, and is therefore very strictly aligned to national command lines. As an example, U.S. law forbids dissemination through any intelligence channel not exclusively under U.S. control.²

Political and military analysts and commentators generally seem to agree that small wars, counter-insurgency and counter-terrorism are likely to be the normal type of warfare. Such operations require intelligence that is increasingly accessible, rapidly distributed and correct, not hidden, slow and based on one-sided analysis. There is also reason to believe that future wars will bring more use of multinational forces and increasing reliance on human intelligence despite high-tech surveillance measures. New technology can enable other ways of distribution and sharing of intelligence, but implementing it will require a new mentality in the handling of intelligence – from a focus on isolation, mistrust and nationality, to a focus on opportunity, access and multi-nationality. The “Intelligence Community”³ however, seems to be slow to adopt and change in order to meet these concepts. The U.S. intelligence system specifically, has got where it is today largely from the cold war, something that makes it inadequate today and

in the future.⁴ The scope of required changes makes it difficult to believe that it can come overnight. However, it should be possible within a timeframe of 10-20 years.

This paper proposes that effective future military operations require distribution and sharing of intelligence across national lines and on the tactical level that far exceeds today's reality, and that the military commander in the field should be given Operational Control (OPCON)⁵ of the multinational intelligence assets in his operations area. It describes initially a possible future solution on how intelligence should be shared, before moving on to look at why and how this applies to secrecy, collection and analysis, organization and cooperation, and finally modern operations concepts.

Intelligence can and will be shared in a networking fashion between units on all levels within a Multinational Joint Task Force (CJTF)⁶. National intelligence cells will be integrated in the task force to ensure unity of effort. Secrecy will be maintained partly by separating the source and method from the intelligence product, partly by issuing raw data at the lower level without any analysis except from within the receiving unit itself, and partly by keeping highly sensitive intelligence separate from the rest by having a national line directly to the commander. There will still be a role to play for national intelligence cells, but their main role will differ from today and the balance between secrecy and openness will shift considerably from today's reality. Human intelligence (HUMINT) will be done more and more by ordinary troops on the ground, a development which points to the need for multinational integration of intelligence since the operations area will be manned by troops from several nations. Furthermore, for analysis, multinational intelligence will be highly beneficial in the increasingly complex and diffuse environments of the future, where the need for knowledge and skills will exceed what

any single nation can provide. The ability to network will be crucial, and this includes access and dissemination of intelligence. Specifically, it is obvious that the “intelligence cycle”⁷ will have to be pushed down to low-level units. Operations concepts which currently seem to be continued or implemented in the years ahead are all dependent on sharing of intelligence in an extended way to be effective in future wars.

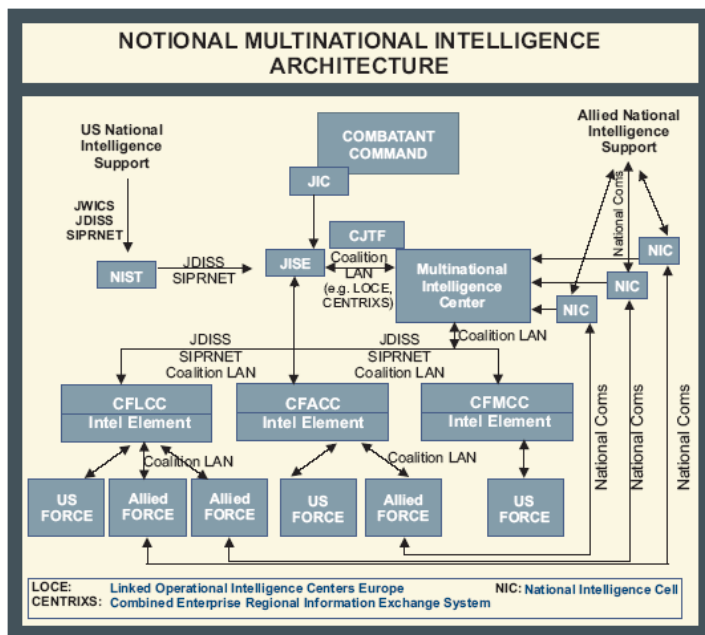
A future solution for access and sharing of intelligence

In the year 2020, when a force consisting of a number of units from different nations and led by U.S. are about to deploy to a theater of operations, all phases of the planning and execution of the campaign will see a much higher level of integration than today. Intelligence is still viewed as national property, but it is also viewed as a resource like, for instance, logistics. Most of the national intelligence assets are therefore subject to “Transfer of Authority” (TOA) to the CJTF commander from the various national intelligence services. Sensors, collectors and analysts are given OPCON to the CJTF commander like any other asset in the force. The CJTF will thus be the “owner” of the intelligence, which facilitates speed and efficiency in the operation. And as the CJTF commander is given operational control of the intelligence assets, he will be able to push the intelligence process further down towards the tactical level - to battalion and even company.

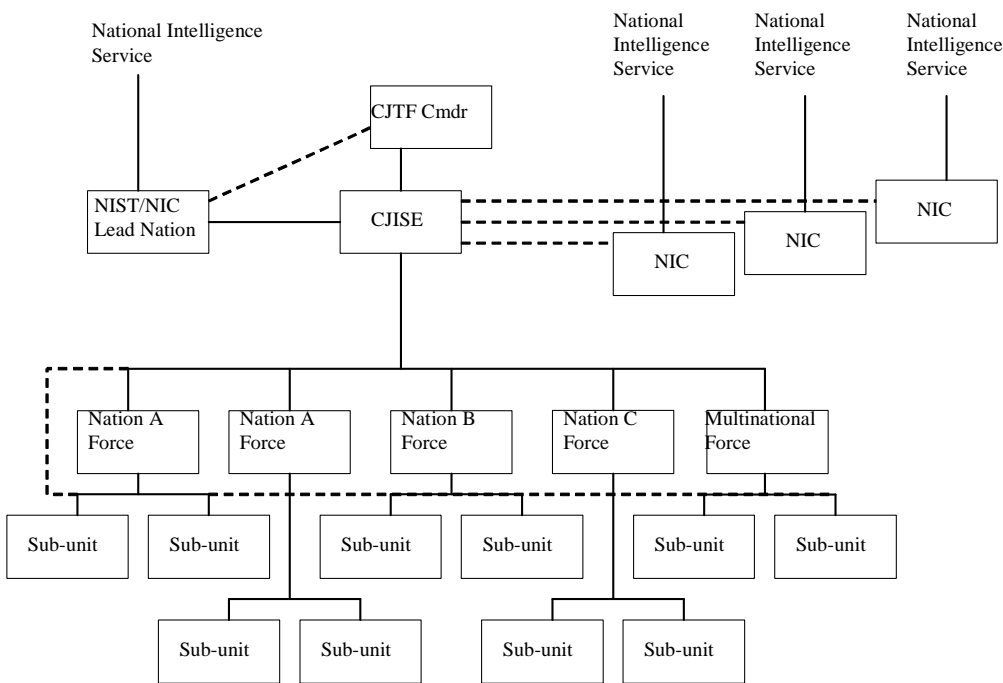
Memorandum of Understanding (MOU) will be worked out before any forces deploy to the theater of operations. For the U.S.A. specifically, there is established one central point to which participating nations’ intelligence services can work out agreements, in contrast to today’s reality where the foreign service has to make agreements with various U.S. agencies.⁸ The command and control for the campaign is

based on a lead nation command and control structure (in contrast to the other normal C2 arrangement, the parallel structure). The principle of lead nation requires integration of national staffs, which by 2020 includes the CJ2, Intelligence. The commander has integrated part of the National Intelligence Cells (NIC) , with their capacity, into his HQ.

Technology, the nature of the adversary, the type of operations, and most important, cultural and mental change, has by 2020 made integrated intelligence and operations possible and desirable. Operational Control of national intelligence assets is given to the commander because it is far superior in effectiveness to relationships like General Support, Direct Support, Close Support and Mutual Support⁹ when they are not under the same command (today the intelligence assets are under purely national command). It will in this way gradually be possible and common to establish a unity of command that includes intelligence to support the operation.¹⁰ The notional organization shown here, drawn from Joint Pub 2-01, illustrates the problem of unity of command since the intelligence assets are not integrated.¹¹



In the campaign in 2020, when the nations who have decided to participate also have committed themselves to integrate intelligence assets, the Multinational Intelligence Center will be integrated in the JISE (Joint Intelligence Support Element), while the NICs will continue also to support the home government but not directly their national units in the field as today. The JISE in the CJTF HQ analyzes and disseminates intelligence to recipients in the task force and to national intelligence cells. The following diagram illustrates how communication in principle will flow. The dotted lines are changes to what normally exist today. The CJISE includes parts of the NICs.



This organization comes from lessons learned in operations the last 20 years. The CJTF is organized around the mission, integrating intelligence assets from all participating nations in planning, collection, analysis and dissemination. The dissemination of intelligence will be a combination of “push” and “pull” principle. Even

down at battalion level there will exist a robust intelligence cell with capacity for cultural analysis, interrogation techniques and language skills. At company level there will also be a dedicated intelligence capacity with regional expertise and language skills, to further enhance the speed and quality of intelligence collection, analysis and dissemination on this level. Intelligence will in this way, together with other capacities like psychological operations, civil affairs, information operations, security, and more, constitute a non-kinetic combined arms team at tactical level.

The collection of intelligence is made from numerous sources, where HUMINT plays a dominant role. "Ordinary" units and not specific intelligence units do a large part of collection on the modern battlefield, as has been the case more and more since the end of the cold war. Individual soldiers in the field from all branches will therefore be trained in intelligence work in a much more extensive way than today. The CJTF itself will conduct much of this training, including some training for under-cover operations. The CJTF will largely develop its own intelligence, whether from HUMINT, SIGINT (signal intelligence) or any other form and there will be a need to share it down to low levels between nations for reasons of combat effectiveness and coalition cohesion. The collected information is thus sent to other units at several levels and higher headquarters as well as put in the CJTF's database. Tactical units will make analysis and assessments according to the character of the information. In this lies a paradigm shift in that there are not solely analysts putting information from processed raw data into the network, but there is also raw data put into the network for users. The decision on what is important moves from the collector and analyst to the person who uses it.¹²

Secrecy and protection of sources

National interests will ensure a role for NICs outside the CJTF also in the future. Even though they to a large extent will be integrated in the CJTF HQ, there will continue to be command lines going to the national authorities and national intelligence services for exclusively national interests. For the lead nation one could for instance also imagine a high sensitive piece of information that should be revealed only to the commander and utilized in his plan and execution without revealing specifically what piece of information his decision is built upon. Such a method will pose some new challenges to multinational co-operation, but will make it possible to achieve unity of effort and maximize the total intelligence resources available without revealing really important secrets.

Another way to protect sources and methods is to act in ways that keep them secret. Authorized officers have to make decisions on how to act as to not reveal the source, or risk a compromise to gain an advantage in operations. The decision should be left with the commander or authorized staff officers and not be subject to a rigid compartmentalized system overseen by disclosure officers as today, which facilitates secrecy and not much more. The secrecy problems will be partly overcome by disseminating intelligence with assessments of reliability without revealing the source. What some officers at Joint Forces Staff College wrote in 2003 will be implemented: “Separating the source and method from the ISR (intelligence, surveillance, and reconnaissance) product allows the needed elements of the JIPB (Joint Intelligence Preparation of the Battlefield) to be passed to a wider variety of coalition partners, without having to develop STANAGs¹³ Current joint doctrine offers no clear answer for how to do that. One answer would be to develop intelligence information-

sharing systems using commercial off-the-shelf software and hardware systems to categorize, view, and disseminate uniquely national JIPB information to all coalition partners involved in decision-making.”¹⁴ In this way the problem with systems that are specially designed to fit dissemination of specific national secrets (like the U.S. system SIPRNET) and therefore are unsuitable for extensive coalition sharing, is reduced. Participants in multinational operations are likely to vary, even during a campaign, and the information-sharing systems should therefore be flexible too.

Taking care of secrecy is basically a choice on where to have the balance between situational awareness, a common operational picture and actionable intelligence on one hand, and secrecy and protection of sources and methods on the other. In multinational operations the weight is put so far out on secrecy that it severely hampers operations and effectiveness. Within national lines this may vary between nations, but for the U.S. forces there are obviously also ways to go towards openness and more rapid dissemination.

Collection and analysis

The rapid technological development has made some commentators predict a transparent battlefield where all can be seen and what can be seen can be destroyed. They overestimate how technology in the future can move us from “blindness to total vision of the battlefield” and replace estimates with truth.¹⁵ However, this is not likely to happen. Even though it is possible to see most of the battlefield, you cannot see what is on people’s mind. It is like a chess-player who can see the chessboard and still lose to an expert who can’t see.¹⁶ An increased technology does not automatically lead to increased efficiency – the concept and system are more important. An example outside the

intelligence sphere illustrates this; it takes longer for a U.S. maneuver company or battalion today to get artillery fire than it took in the Korean or Vietnam War.¹⁷ Moreover, the increasing probability that future conflict will involve fights in urban areas, increases the need for human intelligence.¹⁸ Also, in an environment like in Iraq today, HUMINT is usually the most profitable source,¹⁹ as it was in the Somalia operation in the early 1990's.²⁰ These examples indicate that the distinction between operations and intelligence is becoming more blurred in low-intensity conflicts. This suggestion supports the idea that intelligence collection assets should merge, something that also alleviates the sources and methods problem.

Increasing HUMINT requirements will put a heavy burden on human resources. This will in turn lead to a more need-to-share attitude, which will open the way for increased intelligence sharing in the future. Today's rigid system of intelligence sharing, even within national lines in U.S. forces, contributes to a weak interest in HUMINT and general intelligence. In Iraq today, U.S. Marine Corps is not building a robust intelligence capability by training troops in collection.²¹ There are no courses for troops in the Marine Corps and even officers are not properly educated in this field. (As an example, there is no intelligence focus neither in the U.S. Army's nor the Marine Corps' staff colleges.) Making intelligence they collect more rapidly accessible throughout the force at the low level will increase the interest in intelligence training and improve dissemination.

Cultural IPB (Intelligence Preparation of the Battlefield) is challenging and requires experts to be of high quality. The U.S. military runs several programs for cultural knowledge today, but they are dispersed, under-funded and not easily accessible.²² Coalition partners can provide very insightful collection, analysis and

assessments and should in the future be integrated in the continuous IPB process.

Furthermore, multi-nationality in operations will enhance the possibilities to use the indigenous population and their military forces in intelligence work. U.S. forces in Iraq today do not train and use Iraqi security forces for intelligence work even though Iraqi soldiers are far more effective than their US counterparts at establishing contact and collecting information from the local population.²³ This situation will likely be improved when the focus on secrecy is better balanced with the need for actionable intelligence.

Multi-nationality will help in seeing things from different perspectives, as they will bring a variety of background to the Combined JISE. This will help preventing “mirror imaging”, which is a term describing the tendency to attribute to other leaders or groups the same basic reasoning, psychology and values as one’s own. Foreign officers can provide the role of devil’s advocates more easily than internal intelligence-officers. They are more likely to avoid mirror imaging, wishful thinking, group thinking, and the underestimation of novel dangers, because they will not suffer from what Richard Posner claims: “The best officers (from one’s own nation) will be reluctant to volunteer for an assignment that may impede their promotion prospects by setting them at odds with their colleagues, Those who are appointed will for the same reasons tend to pull their punches.”²⁴ These potential benefits of multi-nationality are not utilized today.

Organization and cooperation

There has been some changes within handling of intelligence the last years, especially in the U.S.A. However, there are still some counter-productive attitudes towards the users of intelligence, and a tendency to over-classify reports and studies with

a passion for secrecy.²⁵ It is obvious that a mentality change and a cultural revolution in the intelligence community are needed. The change has to come also on the strategic level since intelligence on all levels of war are closely interrelated. A multilevel security system does not exist today to facilitate dissemination under current concept, but joint and multi-national forces can request intelligence products as necessary. Today, numerous agreements exist between nations, mostly bilateral agreements, for mutual sharing of intelligence. However, even an “old” alliance such as NATO does not have its own intelligence system. NATO has some capacity for assessments and analysis, but does not have collectors. The alliance must rely, or ask, member-nations to provide data, information, assessments and intelligence. The disadvantage of this is obvious. For instance, in the SFOR operation “Joint Endeavour” launched in 1995 in Bosnia, NATO had to request specific information from the national intelligence cells in the theater and the nations’ intelligence agencies. The responses varied a lot in quality and the nations were generally slow to respond - sometimes answers were not given at all.²⁶ In UN operations, the intelligence situation is even worse. So far, the United Nations have relied on Military Information Officers with access only to unclassified sources as intelligence collectors.²⁷ The multinational disaster relief effort after the Tsunami in December 2004, illustrated the problem in multinational ad-hoc cooperation when several participating nations were too reluctant to share information that could have helped the operation.²⁸ In short, today’s system and concept for utilizing intelligence does not work well. It causes problems for military operations and illustrates the need for changes.

In the Cold War, when information could have enormous impact on the entire struggle and where the existence of any participating nation was at stake, it was only

natural that decisions concerning use and dissemination of intelligence were to be made at the highest level. There are of course still such high level decisions to be made today, but in war and conflicts where our existence is not at stake in the same way and where military forces are more likely to try to solve a low-intensity conflict somewhere else, like it was for instance in Somalia in the 1990s, it should be natural to push a lot more of the intelligence activities and decisions down and let almost everything known be shared with any of the forces participating. The organizational form where information must go up and down the hierarchy from the different subunits, integrated at the top, converted into directives and then go back to the subunits was preferable in the reality of the Cold War. But a different organization, which requires high competence and initiative at lower levels, is likely to be more suitable in an environment as expected in future conflicts. This will require multinational co-operation in a networking fashion. Accordingly, national approaches to the “need-to-know” principle have to be abandoned or loosened up. Strict application of such a principle is incompatible with a networking environment.

Another common problem today is that collectors and other intelligence officers act as if they “own” information while it really is the Government’s property, and they control access to the information that they generate. This is counterproductive to an efficient dissemination and use of intelligence and supports a solution where the commander owns the information on behalf of all participating nations. And these nations have of course access to the same information through their respective NICs in the theater. The idea of giving the commander OPCON of “foreign” NIC has already been tried with success in the operations in Kosovo, which proves that it is possible.²⁹ By taking the “ownership” away from the collectors and giving the national intelligence

assets to the multinational commander in the field, we also get rid of much of the trade of intelligence products, which is an inefficient mode of transacting and because people with good analytical skills but little information will have little to trade.³⁰

Operations concepts

Maneuver warfare is an operational concept where high tempo is central. An intelligence process that takes place at battalion and company level will help increase speed. Besides, most tactical intelligence is time sensitive anyway. By establishing command relationships, or task organizing intelligence assets, to directly support subordinate commanders it will be possible to disseminate some information before it has been fully analyzed and make information management in general more effective.

We see today an increasing interest in Distributed Operations (DO), not least in the U.S. Marine Corps in response to unconventional warfare threats. The Marine Corps underscores the importance of “individual Marines and small units in generating intelligence for their own use, as well as for their higher headquarters. Tactical intelligence will drive distributed operations,...Of particular importance is the realization that the human dimension manifested in small units may be the only way to make positive identification of our adversary and gain an insight into his likely intent.”³¹ A DO-unit should have the capability to utilize information and intelligence rapidly in deliberate actions, and be able to analyze and make assessments in order to complement intelligence achieved from other/higher elements and technological means. It is essential that tactical level units are authorized to act on intelligence from their own level.

Assuming future wars will be multinational, it follows that also the DO concept requires a change as this paper proposes.

The current operations in Afghanistan and Iraq shows that intelligence is not shared effectively neither between multinational units nor within national command lines on the tactical level. Also, indigenous forces are not given sufficient intelligence.³² The problem of organizing intelligence assets to support tactical missions is not new. In 1974, a U.S. Army study concluded that they had not achieved integration from all sources into single products. In an effort to fix this problem, the Army turned typically to a technological solution, an automation of handling the intelligence.³³ But the problem still exists and shows there must be a change in concept if this is to be resolved.

NATO is currently working on concepts that will have influence on intelligence-sharing. It introduces an effects based approach to operation.³⁴ Within this concept, and as part of the aim of achieving decision superiority, the information management and organization must ensure that the information exchanged is linked to the operational needs. And this will require more open information sharing posture³⁵ and a tight relationship between operations and intelligence.

Conclusion

Future wars will require multinational forces that can operate integrated in unpredictable and fluid environments with sharing of intelligence across national chains of command. Intelligence will remain a national property also in the future, but operations will probably show that sharing of intelligence should be the norm and not the

exception. The existing culture in the intelligence community will need to change, on all levels from the strategic to the tactical.

The participating nations will transfer authority of some of their national intelligence assets to the CJTF commander. By giving him OPCON of assets it will be possible to push the intelligence process down to tactical level and utilize intelligence in a networking fashion. The NICs will partly integrate with the CJTF's JISE. At the same time there will continue to exist a role for NICs within national command lines to handle highly sensitive information and provide national authorities with information.

Protection of sources and methods can be handled by separating the product from sources and methods. Also, for some information, raw data can be issued on lower levels and let the receiver do the analysis. Very sensitive and important intelligence can be separated from the main stream of intelligence and led directly to the commander for him to act upon without revealing what information it is based on. There will always be legitimate restraints on the flow of intelligence, but the balance has to be improved between secrecy and sharing. When task forces increasingly are developing their own intelligence, it is natural that also sharing of it will be normal within the force.

Likely operations concepts in the coming 10-20 years, as maneuver warfare, distributed operations, effect based operations and networking, will all require increased ability to share information. When put in a coalition or alliance context, it follows that effective future military operations require distribution and sharing of intelligence across national lines and on the tactical level that far exceeds today's reality.

¹ Melanie M.H. Gutjahr, The Intelligence Archipelago – The Community’s Struggle to Reform in the Globalized Era, (Washington D.C.: Joint Military Intelligence College, 2005), p 137.

² Kenneth Allard, Somalia Operations, (Fort Lesley J. McNair, Washington D.C.: National Defense University, 1995), p 75.

³ The ”Intelligence Community” (IC) is according to Joint Pub 2-01 a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of US national security. However, in this paper by ”the Intelligence Community” we mean the professional intelligence arm of nations.

⁴ The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Report to the President of the United States March 31, 2005, (Washington D.C.: U.S. Government Printing Office), p 353.

⁵ OPCON is the authority delegated to a commander to direct forces assigned so that the commander may accomplish specific missions or tasks which are usually limited by function, time, or location; to deploy units concerned, and to retain or assign tactical control of those units. It does not include authority to assign separate employment of components of the units concerned. Neither does it, of itself, include administrative or logistic control. (This is a NATO definition from <http://www.nato.int/docu/stanag/ajp44/ajp-44.pdf>.)

⁶ The term “Combined” is more and more replaced by “Multinational” as a military term. However, “CJTF” seems to be maintained as the abbreviation for Combined (Multinational) Joint Task Force.

⁷ The term “intelligence cycle” is now in “revision of Joint Publication 2-01, dated 20 November 1996 replaced by the term “Intelligence process” which is defined as the process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback.

⁸ MajGen Jan Blom, NoA, Norwegian Defense Attaché in Washington D.C. and former Chief of Norwegian Intelligence Service, interview 2 Mar 2006.

⁹ For description of these for supporting relationships, see: U.S. Joint Staff, Joint Publication 2-01, Joint and National Intelligence Support to Military Operations, 7 October 2004, http://www.fas.org/irp/doddir/dod/jp2_01.pdf, p II-2.

¹⁰ See U.S. Department of the Navy, HQ U.S. Marine Corps, Washington, D.C. U.S. Marine Corps MCDP 1-0 Marine Corps Operations, (Washington, D.C. 2001), p 1-12 for thoughts on unity of command vs unity of effort.

¹¹ U.S. Joint Staff, Joint Publication 2-01, Joint and National Intelligence Support to Military Operations, 7 October 2004, http://www.fas.org/irp/doddir/dod/jp2_01.pdf, p IV-20.

¹² This view or idea is supported by for instance Major David W. Pendall, U.S. Army, Persistent Surveillance and Its Implications for the Common Operating Picture, (Fort Leavenworth, Kansas: U.S. Army Combined Arms Center - Military Review, Nov-Des 2005), p45, and Carol Haave, Deputy Undersecretary of Defense for Counterintelligence and Security, in Melanie M.H. Gutjahr, The Intelligence Archipelago – The Community’s Struggle to Reform in the Globalized Era, (Washington D.C.: Joint Military Intelligence College, 2005), p 142.

¹³ NATO Standardization Agreements

¹⁴ Jon Engle, USAF; Bernie Harvey, USAF; Charles King, USA; Kevin Sherman, USN. NDU Papers: Joint Critical Analysis – Intelligence: In a Rut, With Some Vectors Out, (Joint Forces Staff College, 2003), p 17.

¹⁵ See for instance Robert R. Leonard, The Principles of War for the Information Age, (Novato, California: Presidio Press Inc., 2000), p 19; and Bill Owens, Lifting the Fog of War, (New York: Farrar, Straus and Giroux, 2000), p 100-102.

¹⁶ Analogy proposed by Paul Van Riper in lecture for U.S.M.C. School of advanced Warfighting (SAW) 16 Aug 2005; “Laying a Foundation about Future War”.

¹⁷ Paul Van Riper in lecture for SAW-class 16 Aug 2005; Class “Laying a Foundation about Future War”.

¹⁸ FY00 Army/USMC Battle Lab MOUT ACTD Program Description, cited in: Center for Army Lessons Learned: Newsletter No. 99-16 Urban Combat Operations, (Fort Leavenworth, Kansas: U.S. Army TRADOC, 1999), p 2-2.

¹⁹ LtCol Andrew Milburn, USMC, unpublished paper: “Bn Level Collection Methods in OIF – II”.

²⁰ Kenneth Allard, Somalia Operations, (Fort Lesley J. McNair, Washington D.C.: National Defense University, 1995), p 74.

²¹ LtCol Andrew Milburn, USMC, Interview Feb 24.

²² Andrea Jackson and Montgomery McFate, An Organizational Solution for DOD's Cultural Knowledge Needs, (Fort Leavenworth, Kansas: U.S. Army Combined Arms Center - Military Review, Jul-Aug 2005), p 18.

²³ LtCol Andrew Milburn, USMC, Interview Feb 24.

²⁴ Richard A. Posner, Preventing Surprise Attacks, Intelligence reform in the Wake of 9/11, (Lanham, Maryland: Rowman & Littlefield Publishers Inc, 2005), p 124.

²⁵ These statements are supported for instance by:

- The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Report to the President of the United States March 31, 2005, (Washington D.C.: U.S. Government Printing Office), p 546.
- Richard A. Posner, Preventing Surprise Attacks, Intelligence reform in the Wake of 9/11, (Lanham, Maryland: Rowman & Littlefield Publishers Inc, 2005), p 113 and 121.
- Ralph Peters, Beyond Terror, (Mechanicsburg, Pennsylvania: Stackpole Books, 1999) p 196, 197.

²⁶ Interview with LtCol Tohmas Brevick in Allied Transformation Command, Norfolk, VA, U.S.A.

²⁷ MajGen Jan Blom, NoA, Norwegian Defense Attaché in Washington D.C. and former Chief of Norwegian Intelligence Service, interview 2 Mar 2006.

²⁸ David J. Dorsett, Tsunami! Information Sharing in the Wake of Destruction, (Fort Lesley J McNair Washington D.C.: National Defense University Press – Joint Force Quarterly 4th quarter 2005), p 15.

²⁹ MajGen Jan Blom, NoA, Norwegian Defense Attaché in Washington D.C. and former Chief of Norwegian Intelligence Service, interview 2 Mar 2006.

³⁰ See Richard A. Posner, Preventing Surprise Attacks, Intelligence reform in the Wake of 9/11, (Lanham, Maryland: Rowman & Littlefield Publishers Inc, 2005), p 113.

³¹ U.S. Department of the Navy, HQ U.S. Marine Corps, Washington, D.C. A Concept for Distributed Operations, (2005),p VII.

³² For Iraq: LtCol Andrew Milburn, USMC, Interview Feb 24.

³³ Kenneth Allard, Command, Control, and the Common Defense (Revised Edition), (Fort Lesley J. McNair, Washington D.C.: National Defense University, 1996), p 147-148.

³⁴ North Atlantic Treaty Organization (NATO), Concepts for Alliance Future Joint Operations (Final Draft 25 Aug 05), p 1.

³⁵ North Atlantic Treaty Organization (NATO), Concepts for Alliance Future Joint Operations (Final Draft 25 Aug 05), p 21.

BIBLIOGRAPHY

Alberts, Garstka, Hayes & Signori, Understanding Information Age Warfare, Air University Papers, http://www.au.af.mil/au/awc/awcgate/ccrp/alberts_uiaw.pdf.

Allard, Kenneth, Command, Control, and the Common Defense (Revised Edition), Fort Lesley J. McNair, Washington D.C.: National Defense University, 1996.

Allard, Kenneth, Somalia Operations, Fort Lesley J. McNair, Washington D.C.: National Defense University, 1995.

Air War College (AWC), Gateway to Information Operations, <http://www.au.af.mil/au/awc/awcgate/awc-info.htm>.

Air War College (AWC), Gateway to Intelligence, <http://www.au.af.mil/au/awc/awcgate/awc-ntel.htm>.

Arquilla, John and Ronfeldt, David, Networks and Netwars, RAND, 2001.

Bell, Wendell, Foundations of Future Studies, New Brunswick, New Jersey: Transaction Publishers, 1997.

Beyerchen, Alan., Clausewitz, Nonlinearity and the Unpredictability of War, International Security, 1992/93 – reprint in School of Advanced Warfighting 2005, Selected Readings for SAW 7410.

Birtle, Andrew J., U.S. Army Counterinsurgency and Contingency Operations Doctrine 1860-1941, Washington, D.C.: Center of Military History United States Army, 1998.

Blom, Jan, MajGen, NoA, Norwegian Defense Attaché in Washington D.C. and former Chief of Norwegian Intelligence Service, interview 2 Mar 2006 .

Boardman, Jill L., (Lockheed Martin Information Technologies); Shuey, Donald W. (Department of the Air Force). Combined Enterprise Regional Information Exchange System (Centrixs): Supporting Coalition Warfare World-Wide, USCENTCOM MACDILL AFB, Florida, 2004:
<http://www.au.af.mil/au/awc/awcgate/ccrp/centrixs.pdf>.

Bowden, Mark., Black Hawk Down, New York: Penguin Books Ltd, 2000.

Brevick, Tohmas, LTC, NoA, ACT. Interview 1 Oct 2005.

Bureau of Justice Assistance, National Criminal Intelligence Sharing Plan,
http://it.ojp.gov/topic.jsp?topic_id=93.

Center for Army Lessons Learned: Newsletter No. 99-16 Urban Combat Operations, Fort Leavenworth, Kansas: U.S. Army TRADOC, 1999.

Clark, Wesley K., Winning Modern Wars, New York: Public Affairs, 2003.

Clausewitz, Carl Von, (ed. And transl. By Michael Howard and Peter Paret) On War, Princeton, New Jersey: Princeton University Press, 1984.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Report to the President of the United States March 31, 2005, Washington D.C.: U.S. Government Printing Office.

Cooney, J.J., Drug Interdiction Along the U.S: Southwest Border: U.S. Counterdrug Policy, History and Future Implications, Paper submitted to School of Marine Corps War College, 1998.

Coram, Robert, Boyd – The Fighter Pilot Who Changed the Art of War, United States of America: Little Brown and Company, 2002.

Cowieson, Keith, “Beyond Certification – Operation Iraqi Freedom”, on the HQ ARRC- Journal web: http://www.rrc.nato.int/journal/summer03/iraqi_freedom.htm.

Deptula, David A., Effects-Based Operations: Change in the Nature of Warfare, Arlington, Virginia: Aerospace Education Foundation, 2001.

Dobson, Robert K Jr., The Distributed Operations Hurdles, Quantico, Virginia: Marine Corps Gazette, Oct 2004.

Dorsett, David J., Tsunami! Information Sharing in the Wake of Destruction, Fort Lesley J McNair Washington D.C.: National Defense University Press – Joint Force Quarterly 4th quarter 2005.

Engle, Jon, USAF; Harvey, Bernie USAF; King, Charles USA; Sherman, Kevin USN. NDU Papers: Joint Critical Analysis – Intelligence: in a rut, with some vectors out, Joint Forces Staff College, 2003:
http://www.jfsc.ndu.edu/current_students/documents_policies/documents/jca_cca_awsp/Joint_Critical_Analysis-Intel-In_A_Rut_with_Some_Vectors_Out.doc.

Engler, Alan, USAF, Glodowski, Al, USAF; Lee, Rocky, USN. Coalition Operations: Politically Necessary Yet Operationally Challenging, Joint Forces Staff College, Joint and Combined Warfighting School – Senior Class 04-1S, 8 mar 04.

Federation of American Scientists (FAS), Congressional Research Service Reports on Intelligence and Related Topics, Intelligence Policy, <http://www.fas.org/sgp/crs/intel/index.html>.

Gebhardt, James F., Eyes behind the Lines: US Army Long Range Reconnaissance and Surveillance Units, Fort Leavenworth, Kansas: Combat Studies Institute Press, 2005.

Giambastiani, Edmund, “Operation Iraqi Freedom Lessons Learned, on the web:
<http://www.iwar.org.uk/pipermail/infocon/2003-October/000673.html>.

Goulding, Vincent J Jr., Distributed Operations, Quantico, Virginia: Marine Corps Gazette, Apr 2005.

Greer, James K., Colonel, U.S. Army, Operation Knockout: Counterinsurgency in Iraq, Fort Leavenworth, Kansas: U.S. Army Combined Arms Center - Military Review, Nov-Des 2005.

Gutjahr, Melanie M.H., The Intelligence Archipelago – The Community’s Struggle to Reform in the Globalized Era, Washington D.C.: Joint Military Intelligence College, 2005.

Hanlon, Edward Jr., Distributed Operations: The Time Is Now, Quantico, Virginia: Marine Corps Gazette, July 2004.

Holzer, Robert D., Wolf PAC: Distributed Operations Experiment, Washington: The Officer <http://proquest.umi.com/pqdweb?index=10&did=793387591&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=POD&ROT=309&VName=POD&TS=1128093674&clientId=32176>.

Institute for Intergovernmental Research: The National Criminal Intelligence Sharing Plan, <http://www.iir.com/giwg/ncisp.htm>.

Jackson, Andrea and McFate, Montgomery, An Organizational Solution for DOD’s Cultural Knowledge Needs, Fort Leavenworth, Kansas: U.S. Army Combined Arms Center - Military Review, Jul-Aug 2005.

Knox, MacGregor and Murray, Williamson. Thinking about Revolutions in Warfare, Dynamics of Military Revolution – reprint in School of Advanced Warfighting 2005, Selected Readings for SAW 7410.

Lackey, Sue A., Initial Look at Distributed Operations Reveals Potential and Problems, Washington, D.C.: Sea Power, Dec 2004,

[http://proquest.umi.com/pqdweb?index=12&did=795394401&SrchMode=1&sid=1&Fmt=4&VInst=PROD
&VType=PQD&RQT=309&VName=PQD&TS=1128093773&clientId=32176](http://proquest.umi.com/pqdweb?index=12&did=795394401&SrchMode=1&sid=1&Fmt=4&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1128093773&clientId=32176).

Latimer, Jon, Deception in War, London, Great Britain: John Murray, 2001.

Leonard, Robert R., The Principles of War for the Information Age, Novato, California: Presidio Press Inc., 2000.

Lynn, John A., Patterns of Insurgency and Counterinsurgency, Fort Leavenworth, Kansas: U.S. Army Combined Arms Center - Military Review, Jul-Aug 2005.

MacIntyre, Douglas J., More on Distributed Operations, Quantico, Virginia: Marine Corps Gazette, July 2005.

Mahaffey, John and Skaar, Trond, Dissemination of ISR Data with Network-Enabled Capabilities in a Coalition Environment, Bonn, Germany: Military Technology, 2005,
[http://proquest.umi.com/pqdweb?did=892209751&sid=3&Fmt=4&clientId=32176&RQT=309&VName=P
QD](http://proquest.umi.com/pqdweb?did=892209751&sid=3&Fmt=4&clientId=32176&RQT=309&VName=PQD).

Mattis, LtGen James N., Lecture for School of Advanced Warfighting class of 2006, Quantico Feb 10 2006.

Maxey, Demetrius F., An Opinion on Distributed Operations, Quantico, Virginia: Marine Corps Gazette, Apr 2005.

McIvor, Anthony D. (editor), Rethinking The Principles of War, Annapolis, Maryland: Naval Institute Press, 2005

Milburn, Andrew, LtCol, USMC, (Currently student at School of Advanced Warfighting. Former U.S military advisor Iraqi Army 2004-2005), Interview Feb 24.

Mucklow, Steven A., Network Centric Warfare: Is the Navy on the Right Course?, Unpublished paper. School of Advanced Warfighting, 1999.

Murray, Williamson and Millet, Allan R. (ed), Military Innovation in the Interwar Period, New York: Cambridge University Press, 1996.

Nagl, John, LTC, USA, Lecture at SAW 8 Oct 2005.

O'Hanlon, Michael, Technological Change and the Future of Warfare, Washington, D. : Brooking Institution Press, 2000.

Owens, Bill, Lifting the Fog of War, New York: Farrar, Straus and Giroux, 2000.

Pendall, David W., Major, U.S. Army, Persistent Surveillance and Its Implications for the Common Operating Picture, Fort Leavenworth, Kansas: U.S. Army Combined Arms Center - Military Review, Nov-Des 2005.

Peters, Ralph., Beyond Terror, Mechanicsburg, Pennsylvania: Stackpole Books, 1999.

Peters, Ralph., Fighting for the Future, Mechanicsburg, Pennsylvania: Stackpole Books, 2002.

Reuters Foundation, EU set to agree on intelligence sharing next week, 02 Sep 2005, Reuters news article: <http://www.alertnet.org/thenews/newsdesk/L0285251.htm>.

Posner, Richard A., Preventing Surprise Attacks, Intelligence reform in the Wake of 9/11, Lanham, Maryland: Rowman & Littlefield Publishers Inc, 2005.

Rekkedal, Nils M., Moderne Krigskunst (English transl: Modern Art of War), Oslo, Norway: Forsvarets Stabsskole, 2003.

Scales, Robert H. Jr., Future Warfare Anthology, Carlisle Barracks, Pennsylvania: U.S. Army War College, 2000.

Scales, Robert H. Jr., Strengthening U.S. Land Forces: Ten Principles for the Future, Yellow Smoke – reprint in School of Advanced Warfighting 2005, Selected Readings for SAW 7410.

Smith, P.E., Maneuver Warfare: The Only Joint Warfighting Philosophy, Paper submitted to Marine Corps War College, 2003.

Soybel, Phyllis L., A Necessary Relationship, The development of Anglo-American Cooperation in Naval Intelligence, Westport, Connecticut : Praeger publishers, 2005.

STINET search site: <http://stinet.dtic.mil>, several results searching for “Intelligence-sharing” and “Information-sharing”.

Thomas, Troy S., Beneath the Surface – Intelligence Preparation of the Battlespace for Counterterrorism, Washington D.C., Joint Military Intelligence College, 2004.

Tjostheim, Inge; Innset, Bjorn; Haarberg, Johan; Haavoll, Harald, Introduksjon til Nettverksbasert Forsvar (Transl to English: Introduction to Networkbased Defense), Oslo, Norway: Forsvarets Stabsskole, 2001.

Trahan, James R., Cultural Intelligence Preparation of the Battlefield, Paper submitted to School of Advanced Warfighting, 1996.

U.S. Air Force, Pamphlet 14-210 USAF Intelligence Targeting Guide, 1998.

U.S. Army Command and General Staff College, Modern warfare, A French View of Counterinsurgency, USAC&GSC, Fort Leavenworth, Kansas, 1985. First published in France in 1961 with the title “La Guerre Moderne”.

U.S. Department of Defense, Loyola, Military Intelligence Links

<http://www.loyola.edu/dept/politics/milintel.html>.

U.S. Department of Defense, Pentagon Has 'MAJIIC' Idea For Intelligence Sharing

http://www.defenselink.mil/news/May2005/20050519_1224.html, and updating at:

<http://www.msnbc.msn.com/id/8171576>.

U.S. Department of the Navy, HQ U.S. Marine Corps, A Concept for Distributed Operations, Washington, D.C., 2005.

U.S. Department of the Navy, HQ U.S. Marine Corps, MCDP 1-0 Marine Corps Operations, Washington, D.C., 2001.

U.S. Department of the Navy, HQ U.S. Marine Corps, MCDP 2 Intelligence, Washington, D.C., 1997.

U.S. Joint Staff, Joint Publication 2-01, Joint and National Intelligence Support to Military Operations, 7 October 2004, http://www.fas.org/irp/doddir/dod/jp2_01.pdf.

U.S. Joint Staff, Joint Publication 5-00.2 Joint Task Force Planning Guidance and Procedures, 13 January 1999, http://www.dtic.mil/doctrine/jel/new_pubs/jp5_00_2.pdf

U.S. Headquarters Department of the Army. FMI 3-07.22 Counterinsurgency Operations, Washington, D.C., 2004.

U.S. Marine Corps MAGTF Staff Training Program MSTP Pamphlet 2-0.3. Collection Management, Quantico, Virginia, 2003.

U.S. Marine Corps MAGTF Staff Training Program MSTP Pamphlet 6-7. C2 Support to MAGTF Intelligence, Quantico, Virginia, 2000.

U.S. Marine Corps. Small Wars Manual, Manhattan, Kansas: Sunflower University Press, Quantico, Virginia, 1940.

Van Riper, Paul: Lecture for SAW-class 16 aug 2005; Class “Laying a Foundation about Future War”.

Van Riper, Paul and Scales, Robert H. Jr. Preparing for War in the 21st Century, Reprint from Parameters, 1997.

Wheeler, John H. Symptoms and Systems: Intelligence and information for future urban “OOTW”, Paper submitted to School of Advanced Warfighting, 1998.