INTELLIGENCE AND INFORMATION SUPERIORITY IN THE FUTURE OF CANADIAN DEFENCE POLICY

Martin Rudner

OCCASIONAL PAPER
Nº 24 - 2001

INTELLIGENCE AND INFORMATION SUPERIORITY IN THE FUTURE OF CANADIAN DEFENCE POLICY

Martin Rudner

OCCASIONAL PAPER
No. 24, 2001

The Norman Paterson School of International Affairs
Carleton University
1125 Colonel By Drive
Ottawa, Ontario
K1S 5B6
Telephone: 613-520-6655
Fax: 613-520-2889
www.carleton.ca/npsia

This series is published by the Centre for Security and Defence Studies at the School and supported by a grant from the Security Defence Forum of the Department of National Defence.

TABLE OF CONTENTS

ABSTRACT

The force development plans and mission projections for the Canadian Forces (CF) and the ongoing Revolution in Military Affairs (RMA) have far-reaching implications for the future role of Defence Intelligence. It is the function of Military Intelligence to respond to the tactical, operational, and strategic requirements of the armed forces for mission-relevant information as processed intelligence. Historically and conventionally, Military Intelligence focused primarily on the battle space and its operational, tactical and strategic variables: enemy plans, intentions, and order of battle, targeting, damage assessment, and field security. To be sure, that approach addressed certain imminent combat requirements, but was essentially deficient in that its purview was presumptive, hermetic and innately parochial. It did not and indeed cannot address the more comprehensive, multi-disciplinary and knowledge-intensive information requirements of the RMA or for the kinds of missions likely to involve Canadian Forces in future. Projections of future Canadian Forces capabilities are all predicated on inputs of substantially new kinds of operational and strategic intelligence and situation-relevant knowledge. This will call for a veritable paradigm shift in Defence Intelligence towards what may be described as a quest for "Information Superiority."

The study that follows outlines the emergent intelligence requirements for future Canadian Defence Policy, and analyzes their impact on the prospective role of Defence Intelligence in capabilities planning for the Canadian Forces.

ABBREVIATIONS

CF	Canadian Forces
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence
EEZ	extended economic zones
EISAS	Information and Strategic Analysis Secretariat
ELINT	electronic intelligence
HUMINT	human intelligence collection
OOTW	Operations Other Than War
RMA	Revolution in Military Affairs
SCP	Strategic Capability Planning
SIGINT	signals intelligence
TSSU	tactically self-sufficient unit
UN	United Nations

INTELLIGENCE AND INFORMATION SUPERIORITY IN THE FUTURE OF CANADIAN DEFENCE POLICY

Martin Rudner

The force development plans and mission projections for the Canadian Forces (CF) and the ongoing Revolution in Military Affairs (RMA) have far-reaching implications for the future role of Defence Intelligence. It is the function of Military Intelligence to respond to the tactical, operational, and strategic requirements of the armed forces for mission-relevant information as processed intelligence. Historically and conventionally, Military Intelligence focused primarily on the battle space and its operational, tactical and strategic variables: enemy plans, intentions, and order of battle, targeting, damage assessment, and field security. To be sure, that approach addressed certain imminent combat requirements, but was essentially deficient in that its purview was presumptive, hermetic and innately parochial. It did not and indeed cannot address the more comprehensive, multi-disciplinary and knowledge-intensive information requirements of the RMA or for the kinds of missions likely to involve Canadian Forces in future.[1] Projections of future Canadian Forces capabilities are all predicated on inputs of substantially new kinds of operational and strategic intelligence and situation-relevant knowledge. This will call for a veritable paradigm shift in Defence Intelligence towards what may be described as a quest for "Information Superiority."[2]

The institutional centrepiece of Canada's Defence Intelligence capability is the J2 Division at the Department of National Defence (DND). J2, with a staff of approximately 500, is responsible for providing the Canadian Forces with all-source defence, security and imagery (in co-operation with the CF Photographic Unit) intelligence and counter-intelligence (in conjunction with the CF National Counter Intelligence Unit). This includes the provision of strategic and tactical intelligence to CF commanders; support for the CF Photo Unit; the deployment of Intelligence, Geomatics and Imagery detachments for

CF operations; the dispatch of Intelligence Response Teams to support peacekeeping missions; and the provision of Counter-Intelligence force protection to operational missions. Defence Intelligence product is also shared with other components of Canada's security and intelligence community and Government Departments, as well as with selected Allies.

The study that follows outlines the emergent intelligence requirements for future Canadian Defence Policy, and analyzes their impact on the prospective role of Defence Intelligence in capabilities planning for the Canadian Forces.

1. DEFENCE INTELLIGENCE AND THE REVOLUTION IN MILITARY AFFAIRS

Information technology constitutes the core element of the current RMA.[3] The notion of a "Revolution in Military Affairs" denotes a quantum leap in transforming military organizations, strategy, doctrine, equipment, training, operations and tactics, so as to accommodate the adoption of new technologies in order to achieve decisive military results. Conceptually, an RMA is an exercise in technological leadership coupled with military innovation. Historical examples of an RMA in warfare include the revolutionary French Republican *levée en masse*; the invention of the submarine and the evolution of under-water warfare; the launching of HMS *Dreadnaught* and the subsequent transfiguration of the Royal Navy's battle fleet; the German *blitzkrieg* in the early phases of World War Two; and United States Navy's sustained, open ocean operations in the Pacific War. It is pertinent to note that the underlying technologies were readily available to the armed forces of other countries as well, but the combatant that led the way in introducing an RMA effectively transformed its military capabilities so as to achieve a decisive advantage in warfare.

a. Information Technology and the RMA

Over the past decade, the quantum leap in information technology and information processing has prompted a new RMA. The United States led the way in the development of information-based technologies and

utilized these to enhance American military capabilities, including in the development and application of the Global Positioning System and air- and space-based sensors. Be that as it may, the accelerated pace of technological development has not yet culminated in a transformational RMA. In the meantime, as information-based technologies mature and become more readily available, they are being increasingly adapted and deployed by the armed forces of most other countries, and even by irregular forces, to enhance capabilities. This trend underscores the imperative for the CF to make a robust effort to capitalize on the potential of these new information technologies and achieve the next RMA.[4]

There is, at present, no definitive path for the CF to follow to realize the potential of an information-technology based RMA. While information technology represents just one element of the current RMA, it is probably the crucial ingredient. Certainly, the refinement and development of informational technology into a genuine RMA can provide the CF with a unique opportunity to re-design its forces structure, doctrine, weaponry and equipment procurement in accordance with anticipated mission purposes. This will require extensive experimentation both to understand the potential contributions of emerging information technologies and to develop innovative operational concepts to harness these new capabilities. Since large, complex institutions generally find it difficult to deal with experimental ideas and revolutionary concepts, it may be useful to identify a particular component of the organization which could be well-positioned to serve as an executing agency for information-based RMA experimentation. Defence Intelligence, given its role in information operations, could play a key part in the experimentation process and in helping to develop new and innovative concepts of mission-relevant intelligence in the context of an evolving RMA.

Indeed, an experimental approach of this genre would provide a singular focal point – Defence Intelligence – for a coordinated, integrated and synchronized effort to explore and exploit the attributes of information technology for future CF capabilities development.

b. Intelligence, Technical Innovation and Operational Requirements

It is the purpose of Defence Intelligence to achieve information superiority for the armed forces it serves. Information superiority in this context entails a capacity for Defence Intelligence to provide realtime, accurate, and relevant battlespace awareness and operational knowledge across a full spectrum of military operations.[5] The element of superiority derives from the synergistic effect of direct national-level intelligence support for intelligence preparation of the battlespace, coupled with the organic intelligence collection and assessment assets deployed by force commanders.

The operational backbone for information superiority is an advanced technological architecture for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR). Effective information superiority is thus predicated on two inter-related engines of battlefield awareness: a Defence Intelligence capacity to generate and integrate offensive and defensive information from a comprehensive array of intelligence sources, surveillance, reconnaissance, and other information-gathering operations; tied to a C4ISR capability to leverage this intelligence through to operational commanders in the field.

Some of the technological solutions now becoming available to Defence Intelligence can demonstrate the potential for information superiority along five principle dimensions of intelligence collection, processing and dissemination. These technologies, embodied in the evolving C4ISR architecture, include:

- A robust multi-sensor information grid, closely integrated so as to generate synergies among its various components (e.g. imagery, ISR, signals, etc.) and capable of providing dominant awareness of the battlespace.

- A communications grid with adequate capacity, resilience, and network management capabilities to rapidly pass relevant information to commanders and forces and to provide for their communications requirements.

- A sensor-to-combatant grid to enable deployed forces to engage in coordinated targeting, cooperative engagement, integrated air defense, and rapid battle damage assessment and follow-up strikes.[6]

- An information defense capability to protect the globally distributed sensors, communications, and processing networks from interference or exploitation by an adversary.

- An information operations capability to penetrate, manipulate, or deny an adversary's battlespace awareness or unimpeded use of their own forces.

These new capabilities for Defence Intelligence will enable armed forces to respond rapidly to any conflict situation or security challenge. However, for intelligence to translate into information superiority, it is necessary to synthesize the collected data, facts and figures so that it may be processed into actual intelligence, assessed and delivered to intended users on the battlefield, aboard ship or in the air. At the tactical level, the US Army is putting in place the All-Source Analysis System (ASAS) as a central processing facility for the integration, collation and dissemination of Defence Intelligence from all available sources for dissemination to field commanders and their staffs down to the battalion level.[7] Canada's DND is developing a compatible program, the Canadian Electronic Warfare Command and Control Program. Designed as an automated architecture for information processing and distribution, this Canadian program is to be inter-operable with the US and other allied technologies and capable of offering commanders a common understanding of the belligerents and the immediate battlefield in response to tactical and operational requirements. This fusion of information technology and all-source intelligence processing capability will transform the purview of Defence Intelligence, offering it the capacity to achieve a real-time state of information superiority across the full spectrum of operational requirements.[8]

c. The Interoperability Requirement for Defence Intelligence

Since the CF must be prepared for deployment at any time on missions involving units from other coalition partners, it is important that its C4ISR programs and technologies attain a high degree of joint and combined interoperability. The propensity of national governments and services to prefer their own proprietary technological solutions can become an impediment to interoperability among various components of information technology. Current efforts to ensure the compatibility of Canadian and US systems will have to be extended to other prospective coalition partners as well. Canada will have to embark on bilateral initiatives with other prospective partners to determine interoperability requirements and standards needed for compatibility among their respective CC4I systems so that Defence Intelligence can conduct information operations effectively across all mission requirements. It is not just technological issues that will need to be addressed. Some measure of product harmonization will be also called for in order to ensure that the intelligence collected and disseminated is in a format and context appropriate for all coalition commanders.

Interoperability has a second facet, that is the horizontal interface between the growing complexity of the Defence Intelligence data base and the multiplicity of types of sensors, storage and retrieval systems available for information operations. New sensors and assets producing novel types of data are generating changes in the conception and design of information operations. It is incumbent upon Defence Intelligence to synthesize these data through a system that can understand and process the raw inputs into usable information. Dissemination of the intelligence product remains an inherent difficulty. Valuable Defence Intelligence collection and analysis efforts can be undone if the intelligence product is not delivered to the right person at the right time in the right format at the right amounts in the right place. This aspect of interoperability will have to depend on advanced information communications technologies to achieve horizontal connectivity and dissemination at all levels of training, planning and operations.

d. Information Superiority and Mission Effectiveness

By making information superiority not just possible but also mission-relevant, Defence Intelligence can serve as a force multiplier. Indeed,

certain of these force multiplier effects may be of such profound and far-reaching consequence that they engender a real transformation of military doctrine and force structure. The impact of sophisticated C4I systems on the military capacity for precision engagement, focused logistics, and full-dimensional protection are exemplary of these transformatory effects.[9] These enhanced capabilities can demonstrate the effective utilization of information superiority for the conduct of military missions, thus paving the way to a genuine RMA in the Defence Intelligence domain.

The concept of precision engagement denotes the capacity to find, fix, track, and precisely target any military objective worldwide. Precision engagement optimizes the application by Defence Intelligence of information superiority and global situational awareness to provide real-time battlefield awareness and target definition for dynamic command and control. By enabling a more precise delivery and increased survivability for all forces, weapons, and platforms, and the flexibility to rapidly assess the results of the engagement, then to re-engage with precision when and as required, the capacity for precision engagement provides a greater assurance of generating the desired effect against the objective or target. This expanded capability for Defence Intelligence would effectively exploit information superiority across the spectrum of military operations.

The precision engagement concept can actually transcend mere firepower to also address other explicit objectives. Thus, it can relate as well to the achievement of accurate and timely deliveries of humanitarian relief supplies or medical treatment to populations, to psychological operations or information warfare in cyberspace. Moreover, the development of precise, non-lethal weaponry for use on missions where minimizing fatalities and civilian collateral damage is a priority goal will lend further operational significance and flexibility to the concept of precision engagement. The effective utilization of information superiority for precision engagement creates an enabling environment for force commanders to develop innovative strategies, operational principles, and tactical maneuvers. However, in order to achieve this degree of operational effectiveness it will be incumbent upon Defence Intelligence to provide the CF with enhanced battlespace situational, and to ensure that its equipment is fully integrated into the

advanced information systems that support precision engagement.

The concept of focused logistics integrates information superiority and advanced technologies into state-of-the-art logistical practices and doctrine. Focused logistics represent a quantum leap forward through the information interface whereby supply and maintenance information systems are interconnected and embedded with operational information to facilitate precise and more responsive logistical support for rapid unit deployment and operational employment. This connectivity could streamline the logistical tail necessary to sustain more agile rapid reaction forces that can be deployed anywhere around the globe. Although logistics in and of themselves are not a Defence Intelligence function, the development of a focused logistics capability geared to the provision of operational information will permit the CF to accurately track and deploy assets, even while en-route, and would expedite the more timely delivery of essential supplies to meet mission requirements.

An important function of Defence Intelligence is to provide early warning and detailed information about the threats to CF personnel and facilities and to critical national infrastructure. Operationally, this includes notifying commanders about the presence and movements of friendly forces so as to avoid risks of "friendly fire." Apart from early warning of conventional and unconventional (e.g. chemical or biological) threats, the CF also require intelligence directed against so-called "asymmetric" attacks on information systems, infrastructure, and other critical assets (see below). The recent experience of US forces and other allied forces underscores the vulnerability of facilities, assets and even individual personnel to terrorist acts and low-intensity conflict in the course of conducting their mandated missions. As will be discussed below, peacekeeping and peace-enforcement missions have not been exempt from such threats. It is for Defence Intelligence to provide the battlespace awareness and threat assessments that could allow the CF to safely maintain freedom of action on missions where the operational environment may also involve non-traditional but nevertheless deadly threats.

e. The Human Quality of Defence Intelligence

Advanced technologies do not constitute the whole future of Defence Intelligence, even in the information age. As in other applications of information and communications technology, the deployment of new technologies for intelligence collection and dissemination often comes up against the constraints of human resource availability or capability.[10] The considerable investment that has taken place in constantly upgrading the technical means of collecting tactical and operational intelligence has not been matched by similar efforts to improve the human capacity to transform the raw data into useful Defence Intelligence. The experience of some of the most technologically advanced armed forces points to the laggard state of human intelligence collection (HUMINT) and analysis capacity, notwithstanding their enhancements to C4ISR technology over the years.[11] This human resources problem was compounded in the CF by the substantial reductions in personnel levels since the end of the Cold War. As a result, Defence Intelligence, like other components of the CF, was being asked to do more with less – both in funding and in personnel. These ensuing pressures on human resources were doubtless exacerbated by Canada's booming hi-tech economy, which tended to attract away some of the same skill-sets needed to staff the new Defence Intelligence functions.

Given the languishing state of human resources in Defence Intelligence, there are indications that the recent emphasis on technologies for moving and sharing information has tended to override attention to ensuring the quality of the intelligence product. It is, of course, essential that Defence Intelligence build on the newly available technologies to enhance the quality and relevance of its product, while also responding to new and emerging threats. Four measures have been identified by the American intelligence community as being required to rectify these human resource deficiencies, and these may also be pertinent to the CF[12]:

(1) *Rectifying database inadequacies:* The emphasis since the end of the Cold War on crisis intelligence support and current intelligence support has tended to detract from development of a broad and deep Defence Intelligence database. The long-term goal, as envisaged by the J2 Information Management Centre, would be to transform the very character of the Defence Intelligence database into a web-enabled

knowledge base.

(2) *Fuller interoperability and integration:* Interoperability tends to be more of an organizational, corporate-cultural and budgetary issue than a technical problem. The advanced information and communications technologies now becoming available generally allow for greater degrees of interoperability, especially with international commercial standards. The aim would be to move the intelligence community generally, and Defence Intelligence in particular, away from parochial systems and towards more standardized defence-wide operational systems.

(3) *Comprehensive threat awareness:* The Post Cold War era has presented Defence Intelligence with the challenge of having to continue dealing with traditional force-on-force threats whilst also responding to new forms of the asymmetric warfare threats. This challenge must be met in a systematic, organized, resource-efficient way. The resources of the intelligence community will be called upon to maintain a high-level of global situational awareness in order to identify these asymmetric threats as they arise and understand their strengths and vulnerabilities. Faced with asymmetric threats, Defence Intelligence will have to develop an understanding of the local political cultures of areas where CF may be deployed, so that intelligence resources can be effectively directed against potential adversaries and also deal with local societal factors.[13] This would involve very close collaboration between Defence Intelligence and the national intelligence and foreign affairs communities on the one hand, and operational forces on the other, in defining the character of asymmetric threats and in determining how to support our own plans and missions.

(4) *Revitalizing and reshaping the human resource base of Defence Intelligence:* As information operations and the types of threat become more varied and complex, Defence Intelligence will have to develop new skills, expertise, and knowledge management capabilities. Supporting information warfare, for example, will require different types of expertise than supporting conventional combat. Advanced technologies will demand commensurate abilities. Improvements in information collection and dissemination will have to be matched by improvements in the interpretation and management of information.

For its part, the American Defence Intelligence Agency foresees increased team work with academia and in mining open source information. Social science and humanities subjects like history and international languages will become more relevant to intelligence requirements for prospective missions in less familiar regions and societies. Yet, it is clear that operational commanders require not more information, but more pertinent information tailored to their specific operational needs. Effective intelligence preparation of the battlespace, or whatever other operational environment is being addressed, is predicated on a robust system of information management which can provide real-time access to pertinent intelligence in the format best designed to address the specific requirements of operational commanders. To ensure a future capacity to deliver mission- relevant intelligence of high quality, it will be necessary for Defence Intelligence to invest in the development of its human resource potential so as to match improved technological capabilities with parallel enhancements to information interpretation and information management.

2. CANADIAN FORCE DEVELOPMENT, FUTURE MISSIONS AND INTELLIGENCE REQUIREMENTS

Force planning is always a complex task. Recent, dramatic changes in the global security environment and the relentless pace of innovation in military technologies render the challenge of formulating a coherent long-range plan for future forces development all the more formidable. The Defence Capabilities Initiatives, launched at NATO's 50th anniversary Summit in Washington DC in April, 1999, aimed at fostering the diffusion of advanced technologies and capabilities as part of an RMA in Alliance forces development.[14] Canada's own *Strategy 2020* confirmed this RMA-centered focus. Accordingly, the Canadian Forces have shifted from the traditional threat-based approach of the past to a new, capabilities-based paradigm for future force development. This new paradigm is embodied in the Strategic Capability Planning (SCP) strategy, adopted in 2000.

The SCP process draws on current policy considerations to propose a notional Concept of Operations that forecasts the type(s) of force

structure indicated by prospective deployments and mission goals.[15] This conceptual devise offers planners a mechanism for assessing projected capability developments, starting with the derivation of a common framework of capabilities, the Canadian Joint Task List. Although this process is only in its beginning phases, preliminary assessments have assigned relatively high value to Information and Intelligence capabilities among the anticipated "capability goals" of the CF as driven by Government policy, DND *Strategy 2020* and current geo-political trends.[16]

a. Canadian Forces Planning Scenarios

The strategic objectives of the CF relate to the defence of Canada and the international security goals as stipulated by the Government of Canada, including crisis prevention, confidence-building, humanitarian or conflict intervention missions. Current planning assumes that the CF will not be expected to be prepared for every possible military contingency, and that resources for capability development remain limited except in instances of evident emergency.[17] Given the absence of a major threat, the military capability for the defence Canada will emphasize surveillance of our territory and its maritime approaches. As well, the CF will need to demonstrate a capability to support for other Government departments or agencies in security-related matters, such as Canadian Forces Information Operations Group support for the Communications Security Establishment[18]; disaster assistance; and aid of the civil power.

Assessments of what international capabilities will be pertinent for the future of the CF highlight the broad scope of prospective mission requirements, from combat operations to a wide spectrum of Operations Other Than War (OOTW).[19] These latter operations can embrace such activities as intra-state conflict-peace-support and peacekeeping missions. The CF do not have today, and will not likely acquire, the capability to operate by themselves in international conflict situations. The Concept of Operations currently being considered envisages that the CF will operate internationally as "task tailored" components alongside other international or coalition partners in a Combined Force. Accordingly, the future capabilities of the CF would be structured around operationally-autonomous, task-tailored modular groups, the so- called tactically self-sufficient unit (TSSU). This TSSU

structure would possessing the operational capability and interoperability to integrate with a Combined Force, while allowing for wide flexibility in deployments.

The future scenarios being contemplated as part of the Strategic Capabilities Planning exercise thus stipulate that the CF must be capable of operating alongside allied or coalition partners in international operations, while retaining an autonomous capability to function domestically. Moreover, the notion of capability is treated as involving more than just combat capabilities; indeed, force planners seem to accept that enabling capabilities, including an effective command and control system, intelligence, and responsive logistics, are key to effective mission capabilities. Air, sea or land TSSUs embody an array operational and tactical capabilities and must be supported by a broad range of strategic, tactical and operational enabling capabilities. Information and Intelligence are included among these enabling capabilities, but are also deemed to be "essential" capabilities.[20]

At the national strategic level, Information and Intelligence enable DND and the CF command to coordinate with other Government departments and agencies and with non-governmental organizations in responding to emergent crises. Tactical level Information and Intelligence capabilities encompass all the knowledge resources required by commanders to plan and act effectively, with economy of effort and security. Surveillance and reconnaissance are intrinsic to this capability. Information and Intelligence capabilities at the operational level are designed to provide force commanders with sufficient battlespace awareness, including detailed intelligence on opposing forces, friendly forces, weather and geography, to achieve operational objectives with minimal attrition. The CF's SCP anticipates that the integral command, Information and Intelligence capabilities of TSSUs will also be usable in the event of disasters or on humanitarian operations to coordinate military activities with those of civil agencies and non-governmental organizations so as to maximize the overall effectiveness of these OOTW missions.[21]

It is an underlying principle of SCP that the TSSU force structure must be embody a military capability adequate to make an operational

contribution of sufficient relevance to be identified as Canadian.[22] Examples of TSSU can include a naval Task Group formed of various ships capable of sea control over a limited area, or even a singleton *Halifax* class frigate which possesses sufficient weaponry, sensors and command and control capability to contribute to a maritime embargo or surveillance operation on its own. A land TSSU may have different characteristics if deployed as a Battle Group on a peace enforcement operation or as a Canadian Brigade Group in a war-fighting operation, however both contexts require approximately the same C4ISR capability. Air TSSUs may likewise vary in composition and unit strength according to the conflict situation and mission objectives, as between fighter, airlift, and surveillance capabilities. SCP presumes a basic TSSU competence in intelligence collection, analysis and dissemination, although the precise array of Information and Intelligence capabilities will be determined according to operational requirements and mission objectives.

b. Intelligence Capabilities for OOTW Missions

Over the past (nearly) fifty years peacekeeping and peace-enforcement has become a highly visible, nationally sacrosanct mission for the CF. Experience indicates that peace support operations require Information and Intelligence capabilities that can differ in significant respects from those of traditional conflictual situations. Although these OOTW have varied considerably in their scope and purpose, they appear to demonstrate some common operational threads apropos Information and Intelligence. The lessons learned may help derive some more clearly defined intelligence planning principles for peace support operations and other OOTW missions than is currently enjoined by traditional operational doctrine.[23]

Information and Intelligence capabilities for peace support and other OOTW missions must relate to operational situations of far greater complexity and indeed ambiguity compared to the tradition combat operations for which these systems were designed. For one thing, in OOTW situations the potential adversaries (and their forces) are usually ambiguous, and often obscure and elusive as well. For another, the intentions of belligerents are typically volatile, and may not always be indicated by the positioning and activity of military or paramilitary

forces. In such circumstances, highly sophisticated technical means of intelligence collection may be less relevant than the balanced application of all Information and Intelligence capabilities, and especially HUMINT. Moreover, the conventional principles of offensive, target-oriented tactical and operational intelligence may have to be modified in order to achieve a nuanced and accurate assessment of the OOTW situation. Based on their experience in Somalia, Haiti and Bosnia, the US Military Intelligence community discerned the following imperatives for future OOTW Information and Intelligence capability planning:

(1) Intelligence support to force protection as the foremost priority;
(2) Human intelligence (HUMINT) as the paramount requirement;
(3) Technical means of collection to be utilized reservedly and appropriately to ensure synergy and balance with HUMINT;
(4) The architecture for Information and Intelligence to be modified so as to incorporate both political and military factors in every assessment, and to sustain interoperability and commonality with coalition partners and non-governmental organizations.[24]

The intelligence architecture of the CF in operational contexts will generally be subordinated to Allied – and especially American – systems in terms of Information and Intelligence capabilities, particularly sophisticated sensors, processors, automated analysis tools, and supporting dissemination networks. While sophisticated sensors, imagery and signals technologies may well serve as force multipliers in peace support operations, experience indicates that they are generally of more limited operational effectiveness than in conventional combat situations. Similarly, high-capacity information processors and analysis tools tend to be of more limited applicability in OOTW contexts. This is principally because the bulk of information collected (predominantly HUMINT) in these more ambiguous situations must be treated to qualitative analysis (characterization of intent) that does not easily lend itself to machine-formatted data fields or reporting. Certainly, the future development of the CF Information and Intelligence capabilities must certainly retain a capacity to interface with these advanced technologies. However, it would be distinctly advantageous and appropriate for Canadian Defence Intelligence to focus its own endogenous efforts on developing complementary talents,

perspectives and HUMINT-centered capabilities.

Future OOTW scenarios suggest that Canada's Information and Intelligence architecture will be impelled to accommodate, process, and effectively deal with substantial HUMINT input of military, political and increasingly also economic/humanitarian bearing.[25] To effectively perform these functions, Defence Intelligence will have to interact with the information-gathering capabilities of local authorities and non-governmental organizations. The implications for the future is clear: the more complex and dynamic the OOTW context, arguably the more HUMINT oriented the supporting intelligence architecture must become.

This inclusion of HUMINT may pose certain conceptual challenges for the architecture of Defence Intelligence. The current architecture is shaped by an automated analytical process designed to input data, apply logical algorithms to it, and then produce an artificial real-time intelligence-based result for dissemination to forces in the field. This design is optimized for responding to empirical facts and things, and not the subtleties of context. It is the essence of the so-called "sensor-to-shooter" process. While this sensor-to-shooter capability should be retained, in particular for force protection, it requires enhancement to accommodate more subtle, context-based HUMINT apropos situations where complexity of the mission environment is much greater. Defence Intelligence architecture will have to be modified (and soldiers trained) to incorporate assessment of both a political and military context with every analysis, adding a very important human dimension to powerful, but limited, technology-based systems.[12]

3. DEFENCE INTELLIGENCE AND MISSION REQUIREMENTS

a. The Arctic: Global Warming and the Security of Northern Canada

The development of CF capabilities as regards the defence of Canada's Arctic sovereignty and security would be profoundly affected by trends in Global Warming. Changing climatic conditions that diminish the sea ice and permafrost could cause a far-reaching and dramatic transformation of the Canadian Arctic security environment. A warmer

Arctic would, in effect, open Canada's northern borders and adjacent waters to circumpolar maritime transport, commercial fisheries and seal hunting, and the expanded exploitation of natural resources, especially in a scenario of continued high and rising oil and natural gas prices. Along with expanded economic activity will come increased human settlement and expanded exposure of Canada's northland to external regional and international contacts and risks, as well as potential threats. As these trends evolve, the CF are likely to be tasked with vastly expanded surveillance and security responsibilities to safeguard the Arctic dimensions of Canada's sovereignty, protect extended economic zones (EEZ) in the Arctic Ocean, and defend Canadian security concerns, including this country's environmental security.

The enhanced Information and Intelligence capabilities likely to be required in response to a warming Arctic may involve both the strategic and tactical levels of future CF development. At the strategic level, Canada already possesses important SIGINT collection facilities at Alert. Additional Information and Intelligence capabilities may be required to monitor, assess and predict actual trends in climate change. As well, the intensification of commercial interests should warrant an expanded requirement for Arctic Economic intelligence, in particular in relation to international investments and planned activities in neighboring circumpolar regions. Given the fragility of the Arctic environment, it may be prudent to undertake surveillance of such economic activities to warn against encroachments on Canadian sovereignty, interests, sea lanes, and environmental security concerns. Offshore oil and gas drilling (and, in future, underwater mining) and related shipping warrant particular attention in this regard.

The prospective intensification of commercial activity in the Arctic will accompanied, almost invariably, by an expansion of transnational crime. There are specific risks in the north of transnational criminality trafficking in contraband affecting the security of Canada, perhaps even in nuclear materials which are mined in northerly regions. Were this to be the case, Defence Intelligence may be tasked with also supporting national efforts in the Arctic directed at international crime and counter-proliferation targets.

At the tactical level, the impact of global warming on the Canadian

Arctic may generate increased demands for expanded Information and Intelligence capabilities on the part of the CF in the northlands and adjacent waters. In particular, were the Northwest Passage and other northerly sea lanes to open up to regular commercial shipping, fishing and sealing, the CF would have to deploy more extensive reconnaissance, electronic intelligence (ELINT), and direction-finding capabilities in order to fulfill the assigned maritime surveillance, search and rescue missions. Any expansion of economic activity in the environmentally fragile Arctic will almost certainly result in this CF surveillance capability being extended to the provision of environmental early warning and disaster support to the Canadian Coast Guard. Similarly, Defence Intelligence could also find itself tasked with supporting law enforcement (e.g. against transnational criminal targets) and protective security, especially for critical infrastructure in the vast and vulnerable north.

b. The Intelligence Challenges of Peace Support Operations

Peace operations, whether undertaken for classic peacekeeping missions or more contemporary preventive action, peace enforcement or peace-building objectives, demonstrate their own distinctive requirements for Information and Intelligence. Although there tends to be a large element of improvisation in peace operations, they seem to be guided by three salient principles: the importance of impartiality and transparency of policies; the exercise of control by an accepted international authority; and the need to ensure effective military and political command and control in an otherwise complex multilateral operating environment.[26] Experience indicates that the place of Defence Intelligence in peace operations tends to vary according to whether these missions were mandated under United Nations (UN) or NATO auspices. Since peace support may be expected to remain a major and indeed preeminent international commitment for the CF for the foreseeable future, it is appropriate the development of force capabilities and doctrine be closely attuned to the attributes of the international operational framework(s) within which these operations are likely to be conducted.

UN peace missions display considerable ambivalence about Information and Intelligence.[27] In as much as the UN considers itself

an essentially neutral, multilateral organization, "intelligence systems" were not countenanced as part of UN mandated peace operations, ostensibly due to their covert, sinister connotations.[28] So far as the UN was concerned, intelligence was equated with espionage, and therefore considered a betrayal of the "trust, confidence and respect" deemed necessary for effective UN peacekeeping. Reflecting this view, Canadian military doctrine rejected the term "intelligence" as being "negative and covert", insisting instead that peacekeeping operations rely on a more principled access to "information" that was "impartial, trustworthy and overt."[29]

The operational consequences of this aversion to intelligence were highly problematic for CF on UN peace support operations. Thus, in 1992, General Lewis Mackenzie, commander of UN Forces in Bosnia, found the deficiencies of intelligence prevented the forces under his command from responding to hostile fire from positions ostensibly under UN control, complaining "there was no way we could know – we had absolutely no intelligence."[30]

Be that as it may, a review of UN peacekeeping operations undertaken at the behest of the Secretary-General and published in August 2000 proposed a radical reconfiguration of the role of intelligence in the framework of UN peace and security. The Report of the Brahimi Panel determined that UN peace operations require a more robust military doctrine and a realistic mandate, including a preparedness to apply military force as appropriate to achieve mission objectives. Towards this end, the Report concluded that "United Nations forces for complex operations should be afforded the field intelligence and other capabilities needed to mount an effective defence against violent challengers."[31] To put these capabilities in place, the Report recommended that the Secretary-General establish an Information and Strategic Analysis Secretariat (EISAS), to be administered jointly by the Departments of Political Affairs and Peacekeeping Operations, and which would serve as an information gathering and analysis unit to support the UN's Executive Committee on Peace and Security.

By way of response, the Secretary General decided to establish an Information and Strategic Analysis Secretariat within the Department of Political Affairs, solely, as "the focal point for the application of

modern information systems and technology to all parts of the UN system engaged in peace and security activities."[32] As implemented, EIAS consists of three component units: a Strategic Analysis Service, a Peace-Building Unit, and an Information Management Service. Its prescribed functions included creating and maintaining an integrated database on peace and security issues, disseminating that knowledge within the United Nations system, generating policy analyses, providing early warning of impending crises, and formulating long-term strategies for the UN Executive Committee of Peace and Security. Thus, this new Information and Strategic Analysis Secretariat combines a strategic intelligence function along with policy planning functions. While this duality of functions may become problematic in and of itself, it is clear that strategic information – or intelligence – has now acquired a new legitimacy within the framework of UN peace support planning. This new found acceptability of Information and Analysis at the strategic policy level will doubtless resonate downwards to the development of Defence Intelligence capabilities – to gather, process and disseminate "strategic information" – also at the tactical and operational levels of UN peace mission planning.

Since the end of the Cold War NATO, for its part, has undertaken so-called "peace support" operations in the Gulf, in Somalia and in the former Yugoslavia.[33] These activities were not only "out of theater", but also engaged NATO forces in an entirely new genre of missions – for the Alliance, as such – aimed at conflict prevention, peacemaking, peacekeeping, humanitarian aid, peace enforcement and peace building.[34] As a result of recent experience, especially in Bosnia, NATO military planning for peace support operations now prepares itself for a continuum of contingencies in which low-intensity monitoring may escalate into high-intensity peace enforcement. Moreover, NATO has also recognized that the intelligence requirements for peace support missions extend beyond Defence Intelligence as narrowly defined to also embrace the pertinent political, social, cultural, and economic dimensions of intelligence. Contingency planning for peace enforcement generates a powerful imperative for robust Information and Intelligence capabilities at the very outset of NATO-led peace support operations. Perceptions of impartiality and intelligence sharing will perforce be affected by this war preparedness. The Alliance's approach to peace support may well serve to undercut

the effectiveness of the intelligence function, which may in turn constrain NATO's leadership role in peace support just a time when this mission is becoming salient on the Alliance agenda.

NATO, as an organization, does not possess an intelligence collection capability of its own, and has but a limited capacity for analysis. Ordinarily, all of NATO's intelligence requirements are met from intelligence products supplied by member countries for the exclusive use of the Alliance itself and for its constituent governments. It is a fundamental principle of NATO intelligence sharing that none of the intelligence supplied to the Alliance can be shared with non-member countries or to any international organization composed of non-member countries. This fundamental principle applies also on peace support missions involving NATO in partnership with other countries and organizations, notwithstanding operational requirements for intelligence sharing.

While providing some intelligence input into NATO, the United States tends to rely on its own very sophisticated C4ISR capabilities to acquire high-quality imagery, SIGINT, and other elements of information superiority to support American forces engaged in NATO-led peace support missions. The American military often discriminates even between allies in allowing access to these intelligence products, so as to protect classified capabilities or methodologies. Thus, some of the highest value components of information superiority are reserved for US users and are not generally shared even with other NATO countries on the same NATO-led missions. However, the CF reportedly have enjoyed privileged access to this intelligence.

NATO military planning is, of course, cognizant of this tension between the security principle governing access to Alliance intelligence, on the one hand, and the operational principles of transparency and integrated command and control, which imply intelligence sharing among partners and international authorities involved in peace support coalitions, on the other.[35] Nevertheless, NATO insists that it cannot countenance any sharing of Alliance intelligence products with non-member countries or with an international organization of which they are a part. As a result, the intelligence architecture for NATO-led peace support missions has

tended to assume the characteristics of a three tier, differentiated apparatus, with a top tier consisting of US forces and their most intimate allies who share access to American ISR capabilities to the fullest; a second tier composed of other NATO allies who may obtain Information and Intelligence made available through the Alliance, but which may exclude access to some reserved American-generated products; and a third tier consisting of all other country or international components. This compartmentalization of the NATO intelligence architecture militated against the effective command and control of peace support operations involving the Alliance, and sometimes produced grave deficiencies in the availability of tactical and operational intelligence even to Canadian participants. Since ad hoc coalitions with non-NATO partners have become characteristic of peace and humanitarian missions, Canada, as a NATO member, intimate US ally and frequent coalition partner with non-members may well find itself on the fault lines between the three tiers of intelligence compartmentalization.

In order to ensure an effective response to the requirements for Information and Intelligence in the context of UN or NATO-led peace and humanitarian missions, future Canadian TSSU capability development will have to seek a closer interoperability and fusion in the production and dissemination of Defence Intelligence. Interoperability with allies and prospective coalition partners will remain a *sine qua non* for the operational integration of C4ISR capabilities on peace support missions. However, technical interoperability will not suffice. Structural impediments confronting both the UN and NATO systems, which prevent the effective deployment of Defence Intelligence capabilities in a coherent, integrated manner for peace support must likewise be addressed. To enable the CF on UN or NATO-led peace support operations to achieve information superiority, the future development of Information and Intelligence capabilities for Canadian TSSUs will have to promote a more balanced integration of technical and HUMINT sources, along with a closer fusion of the strategic, tactical and operational dimensions of Defence Intelligence. It seems clear that CF commanders on peace missions will demand greater attention to the scope, depth and relevance of Defence Intelligence.

c. Intelligence Responses to Threats to Critical National Infrastructure

Lessons learned from the Ice Storm of 1998 and the Y2K exercise highlighted the vulnerabilities of Canada's critical national infrastructure to disruption.[36] According to current threat assessments, the greatest menace confronting Canada's critical infrastructure derives from potential asymmetric warfare threats.[37] Indeed, the tight interface with American systems in many key areas of advanced technology implies that Canada's critical national infrastructure may be in double jeopardy, in so far as Canadian systems are unlikely to escape collateral damage from asymmetric attacks on the United States. The risk that critical national infrastructure can be threatened by physical or electronic means in asymmetric warfare is of great concern to Canadian and American security and intelligence authorities. Such an attack on vital commercial, military and government information and communications systems could have damaging consequences vastly disproportionate to the effort expended to undertake it.

Asymmetric warfare is not new, but represents a contemporary example of low-intensity conflict, through which, as put by United States Defense Intelligence Agency, "weaker adversaries attempt to advance their interests while avoiding a direct engagement with (our) military on our terms." Threats deriving from terrorist activity, paramilitary adversaries, militant action groups, organized crime, or complex emergencies, all denote asymmetric challenges to a more conventionally powerful military or law enforcement authority. Asymmetric adversaries typically attack vulnerabilities. At the strategic level, asymmetric threats exploit the fears of the civilian population to weaken support for the democratic process, undermine confidence in government, or compromise its alliances and partnerships. At the tactical level, asymmetric adversaries can try to coerce governments into changing policy directions or actions, by launching attacks that are difficult for the authorities to confront and prevent, like attacks, both physical and electronic, on critical national infrastructure. To be able to anticipate, analyze and respond to such asymmetric threats, a greater appreciation and understanding of the circumstances that give rise to asymmetric attacks must become prevalent in the intelligence community.[38]

As Canadian society has become more "open" in the wake of globalization coupled with the information revolution in computing and telecommunications and the increasing privatization of governmental functions, it also becomes more vulnerable to cyber-based asymmetric warfare. Adversarial organizations or individuals with hostile or malicious intent could utilize cyber-weaponry to wage asymmetric information warfare to deny, disrupt or destroy the capabilities of our critical national infrastructure. It is not only the defence domain that is under implied threat from asymmetric information warfare, but so are the telecommunications networks, computer systems and data-transferring capacities that constitute the sinews of contemporary government, commerce, culture and social services. There is even a threat that asymmetric adversaries to a peace support operation might engage in information warfare strategically to cause large-scale disruptions in Canada and its coalition partners. Targets could include the most information intensive sectors of their national economies – notably the telecommunications network, financial and banking systems, the electric power grid, and national transportation web. Asymmetric information warfare could have potentially devastating consequences for Canada and other societies that are increasing reliant on information systems as a core component of their critical national infrastructure, especially if combined with terrorist assaults or attacks with weapons of mass destruction.[39]

Asymmetric information warfare is not only a threat to critical national infrastructure, it is also an intelligence challenge. The focus on potential disruptions scenarios has tended to ignore other very cogent applications of information operations in asymmetric warfare, and in particular intelligence gathering, counterintelligence and disinformation.[40]

The implied threats to Canada's critical national infrastructure and to the security of our intelligence community invoke a requirement for enhanced intelligence capabilities to warn against asymmetric dangers and to support countervailing operations. Although the primary responsibility for providing intelligence support for dealing with asymmetric threats may rest with the Canadian Security Intelligence Service (CSIS), Defence Intelligence cannot eschew involvement due

to the vulnerability of the defence sector, the risks to OOTW and other peace missions, and the close interface between the military and critical national infrastructures. While technological assets (such as SIGINT and Satellite imagery) may certainly be helpful in dealing with these threats, experience demonstrates the particular value of HUMINT and open source intelligence for monitoring and assessing asymmetric adversaries.[41]

Defence Intelligence support for operations against asymmetric threats would necessarily imply a transformation of the traditional strictly military purview. Defence Intelligence would have to achieve a more syncretic fusion between political intelligence and traditional military concerns, while also fostering a closer horizontal interoperability with CSIS as well as other components of Canada's civilian intelligence community, if it is to contribute effectively to intelligence support against asymmetric threats. Fusion and horizontal interoperability seem to be the only practical courses of action, since compartmentalization will otherwise militate against realization of the full potential of Canada's Information and Intelligence capabilities. For Defence Intelligence, fusion and horizontal interoperability represent force multipliers in response to asymmetric threats.

4. THE FUTURE OF DEFENCE INTELLIGENCE: A THREE DIMENSIONAL FUSION

The present analysis suggests that SCP for the future of the CF will set in motion a transformation of Defence Intelligence, building on its traditional combat related functions while augmenting these with wider ranging Information and Intelligence architecture capable of addressing emergent operational requirements, including peace support, Arctic defence, and asymmetric threats to national critical infrastructure. There is no question that Defence Intelligence must retain and enhance its combat support function. However, SCP projections for an accelerating RMA coupled with the projected development of more extensive OOTW capabilities will redound upon the purview of Defence Intelligence. The CF will require expanded Information and Intelligence support to operate effectively and achieve mission objectives in the OOTW environment that looms large on Canada's

security and defence agenda. Were Defence Intelligence to eschew this transformation, then the CF could either find themselves deprived of information superiority and thus impeded operationally, or else becoming even more dependent on allied intelligence resources which may or may not always be accessible.[42]

As we have seen, Information and Intelligence capabilities for peace support, Arctic, and other OOTW missions have to relate to operational situations of far greater complexity and ambiguity than traditionally has been the case for Defence Intelligence. The more complex and volatile the OOTW context, arguably the more HUMINT oriented the supporting intelligence architecture must become. OOTW scenarios suggest that Canada's Defence Intelligence architecture will have to accommodate, process, and effectively deal with substantial HUMINT input of military, political and economic parameters. To effectively perform these functions, Defence Intelligence will have to interact with the information-gathering capabilities of local authorities and non-governmental organizations. By creating an enabling environment for information superiority, a transformed Defence Intelligence architecture could significantly augment CF capabilities for such mission relevant objectives as precision engagement, focused logistics, and full-dimensional protection.

To implement this transformation, the future direction of SCP for Information and Intelligence capabilities planning should aim at a achieving a three tier fusion of Defence Intelligence capabilities[43]:

(1) The first tier of capabilities fusion would aim to enhance the technical capabilities of Defence Intelligence whilst scaling up its capacity to accommodate, analyze and relate to with HUMINT sources. A closer integration of Canada's current Imagery, ISR, and even SIGINT capabilities could generate valuable synergies. In a context of scarce resources and increasingly urgent requirements, the creation of a single focal that generates synergy among these technical means would produce a more efficient and robust system of military intelligence collection.[44] Among the HUMINT sources that should be addressed is the vast knowledge base of international, area and country studies, political and cultural anthropology, vested in Canada's interdepartmental community, universities and research institutions,

non-governmental organizations, and consulting industry. Political, social, cultural and economic information would be synthesized along with combat intelligence into an enhanced intelligence preparation of the battlespace or other operational environment facing CF commanders. This could, in turn, be fused with an automated architecture for intelligence processing and distribution, through the Canadian Electronic Warfare Command and Control Program. This achievement of fusion between technical and HUMINT capabilities would pave the way to an transformatory RMA in the Defence Intelligence domain.

(2) A second tier of capabilities fusion should aim at fusing the strategic, tactical and operational levels of Defence Intelligence into a holistic, vertically integrated and interoperable Information and Intelligence system. During the 1990s, considerable emphasis was placed on interoperability and dissemination issues. The projected missions for the CF point to an increasing fusion of strategic, tactical and operational intelligence support. The future challenge is to achieve a high quality of information management that broadens and deepens analytical capabilities at all three levels of Defence Intelligence. This vertical interoperability should build on a fusion of technical and HUMINT assets while ensuring the relevance and responsiveness of the Information and Intelligence system to the requirements of field commanders.

(3) The third tier of capabilities fusion should focus on ensuring the future architecture of Canadian Defence Intelligence retains horizontal interoperability with allies, as they develop ever more sophisticated Information and Intelligence assets; with the emergent UN architecture for Strategic Information and Analysis; and with other prospective international partners on peace and humanitarian missions. While respecting the need to protect the classified elements of intelligence, a particular effort could be made to find ways to achieve a functional horizontal interoperability for the dissemination of Information and Intelligence products, duly "sanitized", between NATO and other non-member coalition partners on peace support operations

All of this translates to a broader purview for Defence Intelligence than was hitherto the case. However, as with most DND and CF

organizations during the past decade, Defence Intelligence has seen its numbers and budget cut. Since the end of the Cold War, the uncertainties arising from the changing context and scope of international conflict pose new and heightened challenges for Defence Intelligence. It may well be a less dangerous world in some respects, but it is a rather more uncertain world. It is for Defence Intelligence to transform its architecture and enhance its capabilities in order to support the CF in dealing with these uncertainties.

ABOUT THE AUTHOR

Martin Rudner is Director of the Centre for Security and Defence Studies at The Norman Paterson School of International Affairs, Carleton University. He is also Professor at the School and teaches several courses, including on Intelligence and Security.

LIST OF OCCASIONAL PAPERS

1. Aliya and the Demographic Balance in Israel and the Occupied Territories (1992)
   James W. Moore

2. A New Germany in a New Europe (1992)
   John Halstead

3. Does the Blue Helmut Fit? The Canadian Forces and Peacekeeping (1993)
   Ian Malcolm

4. Yugoslavia - What Went Wrong? (1993)
   John M. Fraser

5. The Origins and Future Demise of the Democratic People's Republic of Korea (1994)
   Charles K. Armstrong

6. Contesting an Essential Concept: Dilemmas in Contemporary Security Discourse (1994)
   Simon Dalby

7. Ethnic Conflict and Third Party Intervention: Riskiness, Rationality and Commitment
   David Carment, Dane Rowlands and Patrick James

8. Conflict Prevention and Internal Conflict: Theory and Policy, A Workshop Summary (1995)

9. David Mitrany, the Functional Approach and International Conflict Management (1995)
   Lucian Ashworth and David Long

10. Dealing with Domestic Economic Instability: U.S. Foreign Policy and the Rally Effect, 1948-1994 (1996)
    Athanasios Hristoulas

11. Modelling Multilateral Intervention in Ethnic Conflict: A Game Theoretic Approach (1996)
    David Carment and Dane Rowlands

12. The Interstate Dimensions of Secession and Irredenta: A Crisis-Based Approach (1996)
    David Carment

13. The Functional Approach, Organization Theory and Conflict Resolution (1996)
    Craig N. Murphy

14. Using a Culturally-Specific Process of Mediation and Dispute Resolution to Promote International Security (1997)
    Roger Hill

15. Exploring Canada's Options on 'Global' Issues (1997)
    Evan H. Potter and David Carment

16. Canadian Foreign Policy: From Internationalism to Isolationism? (1997)
    Jean-François Rioux and Robin Hay.

17. Making the Impossible Possible: The PLA's Cross-Strait Operations in the 21st Century (1999)
    Jianxiang Bi

18. Water Balances in the Eastern Mediterranean: A Workshop Summary (1999)
    Ozay Mehmet.

19. Conditions of Influence: A Canadian Case Study in the Diplomacy of Intervention (1999)
    John B. Hay

20. Information Warfare: Media-Military Relations In Canada (1999)
    Michael Croft, Sharon Hobson, and Dean Oliver

21. Twisting Arms and Flexing Muscles: Perspectives on Military Force, Humanitarian Intervention and Peacebuilding - Report on a Workshop (2000)
    Natalie Mychajlyszyn

22. Canada's Communications Security Establishment: From Cold War To Globalization. (2000)
    Martin Rudner

23. From Rhetoric to Policy: Towards Workable Conflict Prevention at the Regional and Global Level - Report on a Workshop (2000)
    David Carment, Abdul-Rasheed Draman and Albrecht Schnabel

24. Intelligence And Information Superiority in the Future of Canadian Defence Policy (2001)
    Martin Rudner

Ordering Information:

- Please send a cheque or money order for $12.00 to (made out to **The Norman Paterson School of International Affairs**) to Elizabeth James, NPSIA, Carleton University, 1125 Colonel By Drive, Ottawa, ON, K1S 5B6. If the item is to be picked up in person, the cost is $10.00

ENDNOTES

[1]. For a similar assessment of the ongoing transformation in the purview of Military Intelligence in the Canadian context, see Commander D.W. Knight, "A Decision Point in the Future of Military Intelligence," presented at the CASIS 2000 Conference of the Canadian Association for Security and Intelligence Studies, Ottawa, 29 September 2000.

[2]. For an insightful analysis of Canadian military intelligence requirements and its prospective capabilities as regards information superiority see Commander D.W. Knight's CJCS Strategy Competition Essay, "The Fourth Wish" (mimeo).

[3]. Cf. VCDS, *Strategic Capability Planning for the Canadian Forces*, June 2000 (mimeo.), esp. Para 2.11; Department of National Defence, Directorate of Strategic Analysis, Policy Planning Division, Policy Group, *Strategic Overview 2000* (Ottawa: National Defence, September 2000), "RMA and the DCI", pp. 118-122. There is an extensive literature on the Revolution in Military Affairs and its pertinence for intelligence and information. Salient contributions to the literature include: Elliot Cohen, "A Revolution in Warfare," *Foreign Affairs* 75:2 (1996); Stephen Blank, "Preparing for the Next War: Reflections on the Revolution in Military Affairs," *Strategic Review* 24 (Spring 1996); Lawrence Freedman, "Britain and the Revolution in Military Affairs," *Defence Analysis* 14:1; Tierry Gongora and Harald von Reikhoff, eds., *Towards a Revolution in Military Affairs? Defence and Security at the Dawn of the 21st Century* (Westport, CT: Greenwood Press, 2000).

[4]. Knight, "The Fourth Wish".

[5]. Douglas Dearth, "Information War: Rethinking the Application of Power in the 21st Century," *Military Intelligence Professional Bulletin*, 23:1 (January-March 1997); Lt. Col. Michael Flynn, "Intelligence Must Drive Operations: How Intelligence Can Clear the Fog of War," *Military Intelligence*, 26:1 (January-March 2000).

[6]. For a report on Israeli Military Intelligence initiatives in response to asymmetric warfare in the form of the so-called Aqsa Intifada to achieve an all-source integration of intelligence collection coupled with a real-time dissemination of intelligence products down to battalion level, see "Report: New Intelligence Thwarting Palestinian Attacks," *The Jerusalem Post*, 10 January 2001.

[7]. Lt. Col. Gregory Fritz and Lt. Col. Michael Montie, "All Source Analysis System," *Military Intelligence*, 23:3 (July-September 1996).

[8]. Knight, "The Fourth Wish" proposes various scenarios to achieve this.

[9].Dearth, "Information War"; Fritz and Montie, "All Source Analysis System."

[10]. Lt. Col. Robert Adolphe, Jr., "Intelligence: The Human Dimension," *Military Intelligence*, Vol. 25, No. 1 (January-March 1999).

[11]. Robert Ackerman, "Military Intelligence Looks Within: A Re-examination of Goals and Capabilities is Forcing the Community to Focus on Human Assets," *SIGNAL Magazine 2000* (October 2000); see also Donald Ullman, "HUMINT in the Military," *American Intelligence Journal*, 14:1 (Autumn/Winter 1993); Thomas Fields, "Thinking About Defence: HUMINT for the Future," *Defence Intelligence Journal*, 6:1 (Spring 1997); Jeffrey Richelson, "From MONARCH REAGLE to MODERN AGE: The Consolidation of US Defense HUMINT," *International Journal of Intelligence and Counterintelligence* 10:2 (Summer, 1997); Lt. Col. Michael Pick, "CI and HUMINT in Multinational Operations: The Lessons of Vigilant Blade 97," *Military Intelligence* 25:1 (January-March 1999)

[12]. See also Knight, "A Decision Point in the Future of Military Intelligence" for a somewhat different argument but in a parallel direction.

[13]. Cf. Major John Chenery, "Transnational Threats 101: Today's Asymmetric Battlefield," *Military Intelligence* 25:1 (January-March 1999); see also the report of the commission investigating the attack on the USS Cole, cited in "Panel on Cole Attack Urges Increased Spending on Intelligence," *The New York Times*, 10 January 2001.

[14]. Directorate of Strategic Analysis, Policy Planning Division, Policy Group, *Strategic Overview 2000*, Ottawa: Department of National Defence, September, 2000, pp. 118-120

[15].VCDS, *Strategic Capability Planning for the Canadian Forces* (June, 2000). *Mimeo*.

[16].*Strategic Capability Planning for the Canadian Forces*, Table 5.1 and Para.5.; DND, Directorate of Defence Analysis, *Military Assessment 2000*.

[17]. *Strategic Capability Planning for the Canadian Forces*, Chap. 4

[18].*Vide.* Martin Rudner, *Canada's Communications Security Establishment: From Cold War to Globalization*, Occasional Paper No. 22 (Norman Paterson School of International Affairs, Carleton University, 2000)

[19]. *Strategic Capability Planning for the Canadian Forces*, Para. 3.6.

[20].*Strategic Capability Planning for the Canadian Forces*, Para. 4.7.

[21].*Strategic Capability Planning for the Canadian Forces*, Para. 4.8.

[22].*Strategic Capability Planning for the Canadian Forces*, Para. 4.6.

[23]. Col. H. Allen Boyd, "Joint Intelligence Support of Peace Operations," *Military Intelligence*, Vol. 24, No. 4 (October-December, 1998).

[24]. *Vide.* Boyd, "Joint Intelligence Support of Peace Operations"; U.S. Army, Headquarters, XVIII Airborne Corps Deputy Chief of Staff for Intelligence

Briefing "Joint Intelligence Operations: Operation RESTORE DEMOCRACY," U.S. Army Worldwide Intelligence Conference, Fort Huachuca, Arizona, January 1995; Pick, "CI and HUMINT in Multinational Operations: The Lessons of Vigilant Blade 97"; David Rababy, "Intelligence Support During a Humanitarian Mission," *Marine Corps Gazette* (February 1995), pp. 41-2; Alastair Duncan, "Operating in Bosnia," *RUSI Journal* (June 1994), pp. 12-15; Thomas Wilson, "Joint Intelligence and UPHOLD DEMOCRACY," *Joint Forces Quarterly* (Spring, 1996), pp. 57-58; Raymond Leach, "Information Support to UN Forces," *Marine Corps Gazette* (September 1994), p. 49.

[25] Boyd, "Joint Intelligence Support of Peace Operations"; Rababy, "Intelligence Support During a Humanitarian Mission," pp. 41-2; Duncan, "Operating in Bosnia," pp. 12-15.

[26] *NATO, Peacekeeping, and the UN*, Berlin Information Center for Transatlantic Security, Germany, 1994, p. 53.

[27] Paul Johnston, "No Cloak and Dagger Required: Intelligence Support to UN Peacekeeping," *Intelligence and National Security* 12:4 (October 1997); Hugh Smith, "Intelligence and UN Peacekeeping," *Survival* 36:3 (Autumn 1994)

[28] International Peace Academy, *Peacekeeper's Handbook* (New York: Pergamon Press, 1984), p. 39.

[29] Canadian Forces Publication 301(3), *Peacekeeping Operations, 1992*, Section 618, Para.1e.

[30] General Lewis Mackenzie, former U.N. Commander in Bosnia, speaking in a BBC Radio Interview on 11 February 1994. Cited in Nomikos, *Intelligence Requirements for Peacekeeping Operations*, ff. 12.

[31] United Nations, *Report of the panel on UN Peace Operations*, A/55/305 - S/2000 801, 21 August 2000.
[URL:www.un.org/peace/reports/peace_operations.

[32] *Resource Requirements for the Implementation of the Report of the Panel on UN Peace Operations. Report of the Secretary-General.* United Nations General Assembly, A/55/507, 27 October 2000, pt. 2, paras. 11 & 12.

[33] *NATO, Peacekeeping, and the UN*, pp. 22.23. NATO involvement in Peace Support missions was approved by its Military Committee, the Alliance's highest military organ, but has not yet been endorsed or even discussed as a policy matter by the legislatures of member states.

[34] John Nomikos, *Intelligence Requirements for Peacekeeping Operations*, Research Institute on European and American Studies Working Paper, Athens, Greece, October, 2000.

[35] *NATO, Peacekeeping, and the UN*, pp. 22-23.

[36] Critical national infrastructure is defined as "those systems and assets,- both physical and cyber - so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety:" Critical Infrastructure Assurance Office: *Critical Infrastructure Glossary of Terms and Acronyms* (n.d). [URL: www.ciao.gov/CIAO_Document_Library_Glossary/critical_ infrastructure_glossary_C.htm]. The Canadian Senate Special Committee on Security and Intelligence described critical infrastructure as "both physical and cyber-based systems essential to the day-to-day operations of the economy and government," Report of the Special Senate Committee on Security and Intelligence, *Emerging Issues*, Chap. III (January, 1999). [URL: http://parl30.parl.gc.ca/36/parlbus/commbus/senate/come/secu-e/repsecuinjan99part3-e.htm]

[37] *Cf.* Kevin O'Brien and Joseph Nusbaum, "Intelligence gathering on asymmetric threats," *Jane's Intelligence Review*, 12:10 (October 2000), Pt. 1, pp. 50-55.

[38] O'Brien and Nusbaum, "Intelligence gathering on asymmetric threats," pp. 52-3.

[39] O'Brien and Nusbaum, "Intelligence gathering on asymmetric threats," pp. 53-5.

[40] O'Brien and Nusbaum, "Intelligence gathering on asymmetric threats," pp. 53-5.

[41] O'Brien and Nusbaum, "Intelligence gathering on asymmetric threats," pp. 53-5.

[42] Knight, "A Decision Point in the Future of Military Intelligence."

[43]. Cf. Col. Lawrence Arrol, "The Intelligence Fusion Family," *Military Intelligence* 22:3 (July-September 1996).

[44].Knight, "The Fourth Wish."