International Journal of Intelligence and CounterIntelligence, 15: 540–564, 2002

0885-0607/02 $12.00 + .00
DOI: 10.1080/08850600290101758

MARTIN RUDNER

The Future of Canada's Defence Intelligence

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 Canada's Military Intelligence. The function of Military Intelligence (MI) is to respond to the tactical, operational, and strategic requirements of the armed forces for mission-relevant information as processed intelligence. Historically and conventionally, MI 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 could not, 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 the future. All projections of future Canadian Forces capabilities are predicated on inputs of substantially new kinds of operational and strategic intelligence and situation-relevant knowledge. These will call for a veritable paradigm shift in Defence Intelligence towards what may be described as a quest for "Information Superiority."

Professor Martin Rudner, Director of the Norman Patterson School of International Affairs at Carleton University, Ottawa, Canada, from 1988 to 1996, is currently Director of the school's Centre for Security and Defence Studies. The author of numerous books on international matters, he is President of the Canadian Association for Security and Intelligence Studies (CASIS), and a frequent commentator on CBC radio and television. Dr. Rudner is also an economic and political advisor to the Canadian International Development Agency (CIDA).

The institutional centerpiece 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 defense, security, and imagery (in cooperation with the CF Photographic Unit) intelligence and counterintelligence (in conjunction with the CF National Counter Intelligence Unit). This includes the provision of strategic and tactical intelligence of 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.

DEFENCE INTELLIGENCE AND THE REVOLUTION IN MILITARY AFFAIRS

Information technology constitutes the core element of the current RMA.[1] 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 underwater warfare; the launching of the HMS *Dreadnaught* and the subsequent transfiguration of the Royal Navy's battle fleet; the German *blitzkrieg* in the early phases of World War II; and the United States Navy's sustained, open ocean operations in the Pacific War. 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.

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. But 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 their capabilities. This trend underscores the imperative for the Canadian Forces to make a robust effort to capitalize on the potential of these new information technologies and achieve the next RMA.

At present, the Canadian Forces have no definitive path to follow to realize the potential of an information technology–based RMA. While exploiting the potential capabilities of information technology represents probably 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 redesign its forces structure, doctrine, weaponry, and equipment procurement in accordance with anticipated mission purposes. Extensive experimentation will be required, 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.

Such an experiment in Defence Intelligence would provide a singular focal point for a coordinated, integrated, and synchronized effort to explore and exploit the attributes of information technology for future CF capabilities development requirements.

Intelligence, Technical Innovation, and Operational Requirements

The purpose of Defence Intelligence is to achieve information superiority for the armed forces it serves. Information superiority in this context entails a capacity for Defence Intelligence to provide real-time, accurate, and relevant battlespace awareness and operational knowledge across a full spectrum of military operations.[2] The element of superiority derives from the synergistic effect of direct national-level intelligence support for the intelligence preparation of 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 interrelated engines of battlefield awareness: (1) a Defence Intelligence capacity to generate and integrate offensive and defense information from a comprehensive array of intelligence sources, surveillance, reconnaissance, and other information-gathering operations; and (2) tied to a C4ISR capability to leverage this Defence Intelligence through to operational commanders in the field.

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

- A robust multisensor information grid 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 followup strikes;[3]
- 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 its own forces.

These new capabilities for Defence Intelligence will enable the armed forces to respond rapidly to any conflict situation or security challenge. For intelligence to translate into information superiority, however, the collected data, facts, and figures must be synthesized so that they 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 United States Army is putting into place the All-Source Analysis System (ASAS) as a central processing facility for the integration, collation, and dissemination of defense intelligence from all available sources for dissemination to field commanders and their staffs down to the battalion level.[4] 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 interoperable with the U.S. and other allied technologies, and capable of offering commanders a common understanding of their mission environment 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.

The Interoperability Requirement for Defence Intelligence

Since the Canadian Forces must be prepared for deployment at any time on missions involving units from other coalition partners, it is important that the CF's 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 the Canadian and U.S. 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 the 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. Not only technological issues 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: 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. Defence Intelligence must synthesize this 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 depend on advanced information communications technologies to achieve horizontal connectivity and dissemination at all levels of training, planning, and operations.

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's capacity for precision engagement, focused logistics, and full-dimensional protection is exemplary of these transformatory effects.[5] 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 Defence Intelligence's application 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 reengage 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 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, and to psychological operations or information warfare in cyberspace. Moreover, the development of precise, nonlethal 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. But in order to achieve this degree of operational effectiveness, Defence Intelligence must provide the Canadian Forces with an enhanced battlespace situational, and 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 Canadian Forces 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 ensure full-dimension protection for CF personnel and facilities across the threat spectrum, from peacetime through crisis, and at all levels of conflict. Fulfillment of this mission is predicated on a command and control architecture that is built upon information superiority, and which deploys a full array of active and passive measures at multiple echelons. Apart from defending themselves against conventional and unconventional (e.g., chemical or biological) threats, the Canadian Forces also require protective security against ''asymmetric'' attacks on information systems, infrastructure, and other critical assets. The recent experience of United States 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. Peacekeeping and peace-enforcement missions have not been exempt. Full-dimensional protection is called for to allow the CF to safely maintain freedom of action on missions where the operational environment may involve nontraditional, but nevertheless deadly threats.

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.[6] 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.[7] This human resources problem was compounded by substantial reductions in the CF's 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—in both funding and personnel. These ensuing pressures on human resources were doubtless exacerbated by Canada's booming hi-tech economy, which tended to attract some of the same skill-sets needed to staff the new Defence Intelligence functions.

Given the languishing state of human resources in Defence Intelligence, indications are 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 U.S. intelligence community as being required to rectify these human resource deficiencies, and these may also be pertinent to the Canadian Forces:

(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 defense-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, while also responding to new forms of the asymmetric warfare threats. 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 Canadian Forces may be deployed, so that intelligence resources can be effectively directed against potential adversaries, and deal with local societal factors.[8]

(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 United States Defense Intelligence Agency foresees increased teamwork 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, operational commanders clearly 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, Defence Intelligence must necessarily 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.

CF 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, D.C. in April, 1999, aimed at fostering the diffusion of advanced technologies and capabilities as part of an RMA in Alliance forces development.[9] 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.[10] This conceptual device 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 Canadian Forces, as driven by government policy, DND's *Strategy 2020*, and current geopolitical trends.[11]

Canadian Forces Planning Scenarios

The strategic objectives of the Canadian Forces relate to the defense of Canada and the international security goals stipulated by the Canadian government, 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.[12] Given the absence of a major threat, the military capability for Canada's defense will emphasize surveillance of its territory and maritime approaches. The CF will also need to demonstrate a support capability for other government departments or agencies in security-related matters, such as Canadian Forces Information Operations Group support for the Communications Security Establishment;[13] disaster assistance; and aid of the civil power.

Assessments of what international capabilities will be pertinent for the CF's future highlight the broad scope of prospective mission requirements, from combat operations to a wide spectrum of Operations Other Than War (OOTW).[14] These 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 Canadian Forces 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 ''tactically self-sufficient unit'' (TSSU). The TSSU would possess 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 the key to effective mission capabilities. Air, sea, or land TSSUs embody an array of operational and tactical capabilities, and must be supported by a broad range of strategic, tactical, and operational enabling capabilities. Information and Intelligence, included among these enabling capabilities, are also deemed "essential" capabilities.[15]

At the national strategic level, Information and Intelligence enable DND and CF commands to coordinate with other government departments and agencies, and with nongovernmental 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 an 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, geography—to achieve operational objectives with minimal attrition. The Canadian Forces' SCP anticipates that the integral command, and 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 nongovernmental organizations, so as to maximize the overall effectiveness of these OOTW missions.[16]

An underlying principle of Strategic Capabilities Planning is that the TSSU force structure must embody a military capability adequate to make an operational contribution of sufficient relevance to be identified as Canadian.[17] 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. But 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. Strategic Capabilities Planning 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.

Intelligence Capabilities for OOTW Missions

For nearly a half-century, the predominant international deployment of the CF has been for peacekeeping and peace-enforcement operations, except for the Gulf War and Kosovo air campaign. Experience indicates that peace support operations require Information and Intelligence capabilities that can differ in significant respects from those of traditional conflictual situations. These Operations Other Than War (OOTW), though varying considerably in their scope and purpose, 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.[18]

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 traditional 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 its experience in Somalia, Haiti, and Bosnia, the U.S. 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 nongovernmental organizations.[19]

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, 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 CF Information and Intelligence capabilities must 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.[20] To effectively perform these functions, Defence Intelligence will have to interact with the information-gathering capabilities of local authorities and nongovernmental organizations. The implication 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 Defence Intelligence. Its 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, optimized for responses to empirical facts and things, and not the subtleties of context, is the essence of the "sensor-to-shooter" process. While this sensor-to-shooter capability should be retained, particularly for force protection, an enhancement is required 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]

DEFENCE INTELLIGENCE AND MISSION REQUIREMENTS

The Arctic: Global Warming and the Security of Northern Canada

The development of CF capabilities as regards the defense 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 Canada's 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 times of continued high, and rising, oil and natural gas prices. Along with expanded economic activity will come increased human settlement, and greater 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 enhanced 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 the nation'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 Canadian Forces 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. The intensification of commercial interests should also warrant an expanded requirement for Arctic economic intelligence, particularly 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 the future, underwater mining) and related shipping warrant particular attention.

The prospective intensification of commercial activity in the Arctic will be accompanied, almost invariably, by an expansion of transnational crime. Specific risks exist in the North of transnational criminality trafficking in contraband, perhaps even in nuclear materials which are mined in northerly regions, that could significantly affect Canada's security. Were this to be the case, Defence Intelligence may also be tasked with 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 Canadian Forces 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 Canadian Forces 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 Canadian Forces 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.

The Intelligence Challenges of Peace Support Operations

Peace support 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 peace operations include a large element of improvisation, 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.[21] 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 North Atlantic Treaty Organization (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 that 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.

The UN Rethinks Intelligence

UN peace missions display considerable ambivalence about Information and Intelligence.[22] The UN considers itself an essentially neutral, multilateral organization, thus ''intelligence systems'' were not countenanced as part of UN–mandated peace operations, ostensibly due to their covert, sinister connotations.[23] 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.''[24]

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. Toward this end, the Panel 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."[25] 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, to 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."[26] As implemented, EISAS consists of three component units: a Strategic Analysis Service, a Peace-Building Unit, and an Information Management Service. Its prescribed functions include 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, the 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, strategic information—or intelligence—has clearly now acquired a new legitimacy within the framework of UN peace support planning. This newfound 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.

NATO'S New Roles

Since the end of the Cold War, NATO, for its part, has undertaken peace support operations in the Persian Gulf, Somalia, and in the former Yugoslavia.[27] 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.[28] 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 at a time when this mission is becoming salient on the Alliance agenda.

NATO does not possess an intelligence collection and analysis capacity of its own. 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. A fundamental principle of NATO intelligence-sharing is that none of it can be shared with nonmember countries or any international organization composed of nonmember countries. This basic rule also applies to peace support missions involving NATO in partnership with other countries and organizations, notwithstanding operations 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 U.S. military often discriminates even among 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 U.S. users, and are not generally shared even with other NATO countries on the same NATO-led missions. But Canadian Forces have reportedly 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, 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.[29] Nevertheless, NATO insists that it cannot countenance any sharing of Alliance intelligence products with nonmember countries or with international organizations 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-tiered, differentiated apparatus, with a top tier consisting of U.S.

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 has 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. Thus, in 1992, General Lewis Mackenzie, commander of UN Forces in Bosnia, found that the deficiencies of intelligence prevented the forces under his command from responding to hostile fire from positions ostensibly under UN control, and complained "there was no way we could know—we had absolutely no intelligence."[30] Since ad hoc coalitions with non-NATO partners have become characteristic of peace and humanitarian missions, Canada, as a NATO member, intimate U.S. ally, and frequent coalition partner with nonmembers, 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 must 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. But, 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 Canadian Forces 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. Clearly, Canadian Forces commanders on peace missions will henceforth demand greater attention to the scope, depth, and relevance of Defence Intelligence.

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.[31] According to current threat assessments, the greatest menace confronting Canada's critical infrastructure derives from potential asymmetric warfare threats.[32] Indeed, the tight interface with United States systems in many key areas of advanced technology implies that Canada's critical national infrastructure may be in double jeopardy, because Canadian systems are unlikely to escape collateral damage from asymmetric attacks on the United States. The risk that the 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, though not new, represents a contemporary example of low-intensity conflict, through which, as put by the 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.[33]

Canadian society, having become more ''open'' in the wake of globalization, coupled with the information revolution in computing and telecommunications and the increasing privatization of governmental functions, 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 the critical national infrastructure. Not only is the defense domain under implied threat from asymmetric information warfare, so are the telecommunications networks, computer systems, and data-transferring capacities that constitute the sinews of contemporary government,

commerce, culture, and social services. Asymmetric adversaries to a peace support operation might even engage in strategic information warfare 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 networks, 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 increasingly 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.[34]

Asymmetric information warfare is not only a threat to critical national infrastructure, it is also an intelligence challenge. The focus on potential disruption scenarios has tended to ignore other very cogent applications of information operations in asymmetric warfare, and particularly in intelligence-gathering, counterintelligence, and disinformation.[35]

The implied threats to Canada's critical national infrastructure and to the security of its 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 defense 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.[36]

Defence Intelligence support for operations against asymmetric threats would necessarily imply a transformation of the traditional strictly military purview. Defence Intelligence must 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.

THE FUTURE OF DEFENCE INTELLIGENCE: A THREE-DIMENSIONAL FUSION

Strategic Capabilities Planning for the future of the Canadian Forces is likely to set in motion a transformation of Defence Intelligence, augmenting its traditional combat-related functions with a wider ranging Information and Intelligence architecture capable of addressing emergent operational requirements, including peace support, Arctic defense, and asymmetric threats to national critical infrastructure. Without question, 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. Canadian Forces 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 defense agenda. Were Defence Intelligence to eschew this transformation, Canadian Forces could then either find themselves deprived of information superiority and thus impeded operationally, or become even more dependent on allied intelligence resources which may or may not always be accessible.

Therefore, Information and Intelligence capabilities for peace support, Arctic, and other OOTW missions must 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 nongovernmental organizations. By creating an enabling environment for information superiority, a transformed Defence Intelligence architecture could significantly augment Canadian Forces 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 achieving a three-tier fusion of Defence Intelligence capabilities:[37]

(1) The first tier of capabilities fusion would aim to enhance the technical capabilities of Defence Intelligence, while scaling up its capacity to accommodate, analyze, and relate to HUMINT sources. 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, nongovernmental organizations, and consulting industry. Political, social, cultural, and economic information would be synthesized into an enhanced intelligence preparation of the battlespace or other operational environment facing CF commanders. The achievement of fusion between technical and HUMINT capabilities would pave the way to a transformatory RMA in the Defence Intelligence domain.

(2) A second tier of capabilities fusion should aim at blending 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 CF's projected missions point to an increasing fusion of strategic, tactical, and operational intelligence support. The 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 combining 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 that the architecture of Canadian Defence Intelligence retains horizontal interoperability with (a) allies, as they develop ever more sophisticated Information and Intelligence assets; (b) the emergent UN architecture for Strategic Information and Analysis; and, (c) 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 nonmember 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, scope, and nature of international conflict pose new and heightened challenges for Defence Intelligence. Though perhaps less dangerous in some respects, the events of 11 September 2001 showed dramatically that this is a rather more uncertain world. Defence Intelligence must transform its architecture and enhance its capabilities in order to support the Canadian Forces in dealing with these uncertainties and challenges.

REFERENCES

[1] 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*, Vol. 75, No. 2, 1996; Stephen Blank, ''Preparing for the Next War: Reflections on the Revolution in Military Affairs,'' *Strategic Review*, Vol. 24, Spring 1996; Lawrence Freedman, ''Britain and the Revolution in Military Affairs,'' *Defence Analysis*, Vol. 14, No. 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).

[2] Douglas Dearth, ''Information War: Rethinking the Application of Power in the 21st Century,'' *Military Intelligence Professional Bulletin*, Vol. 23, No. 1, January–March 1997; Lt. Col. Michael Flynn, ''Intelligence Must Drive Operations: How Intelligence Can Clear the Fog of War,'' *Military Intelligence*, Vol. 26, No. 1, January–March 2000.

[3] For a report on Israeli Military Intelligence initiatives in response to asymmetric warfare in the form of the ''Aqsa Intifada'' in order 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.

[4] Lt. Col. Gregory Fritz and Lt. Col. Michael Montie, ''All Source Analysis System,'' *Military Intelligence*, Vol. 23, No. 3, July–September 1996.

[5] Douglas Dearth, ''Information War''; Gregory Fritz and Michael Montie, ''All Source Analysis System.''

[6] Lt. Col. Robert Adolphe, Jr., ''Intelligence: The Human Dimension,'' *Military Intelligence*, Vol. 25, No. 1, January–March 1999.

[7] 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*, Vol. 4, No. 1, Autumn/Winter, 1993; Thomas Fields, ''Thinking About Defense HUMINT for the Future,'' *Defense Intelligence Journal*, Vol. 6, No. 1, Spring, 1997; Jeffrey Richelson, ''From MONARCH EAGLE to MODERN AGE: The Consolidation of U.S. Defense HUMINT,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 10, No. 2, Summer 1997; Lt. Col. Michael Pick, ''CI and HUMINT in Multinational Operations: The Lessons of Vigilant Blade 97,'' *Military Intelligence*, Vol. 25, No. 1, January–March 1999.

[8] Cf. Major John Chenery, ''Transnational Threats 101: Today's Asymmetric Battlefield,'' *Military Intelligence*, Vol. 25, No. 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.

[9] Directorate of Strategic Analysis, Policy Planning Division, Policy Group, *Strategic Overview 2000* (Ottawa: Department of National Defense, September 2000), pp. 118–120.

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

[11] Ibid., Table 5.1 and Para.5.; DND, Directorate of Defense Analysis, *Military Assessment 2000*.

[12] *Strategic Capability Planning for the Canadian Forces*, Chapter 4.

[13] See 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).

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

[15] Ibid., Para. 4.7.

[16] Ibid., Para. 4.8.

[17] Ibid., Para. 4.6.

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

[19] See H. Allen 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; Michael 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. 41–42; 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.

[20] H. Allen Boyd, "Joint Intelligence Support of Peace Operations"; David Rababy, "Intelligence Support During a Humanitarian Mission," pp. 41–42; Alastair Duncan, "Operating in Bosnia," pp. 12–15, 20.

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

[22] Paul Johnston, "No Cloak and Dagger Required: Intelligence Support to UN Peacekeeping," *Intelligence and National Security,* Vol. 12, No. 4, October 1997; Hugh Smith, "Intelligence and UN Peacekeeping," *Survival*, Vol. 36, No. 3, Autumn 1994; see also, A. Walter Dorn, "The Cloak and the Blue Beret: Limitations on Intelligence in UN Peacekeeping," *International Journal of Intelligence and CounterIntelligence*, Vol. 12, No. 4, Winter 1999–2000, pp. 414–447.

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

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

[25] 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].

[26] *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, Part 2, paras. 11 and 12.

[27] *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.

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

[29] *NATO, Peacekeeping, and the UN*, pp. 22–23.

[30] General Lewis Mackenzie, former UN commander in Bosnia, speaking in a BBC Radio Interview on 11 February 1994. Cited in John Nomikos, ''Intelligence Requirements for Peacekeeping Operations,'' ff. 12.

[31] 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]

[32] Cf. Kevin O'Brien and Joseph Nusbaum, ''Intelligence Gathering on Asymmetric Threats,'' *Jane's Intelligence Review*, Vol. 12, No. 10, October 2000, Part 1, pp. 50–55.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Cf. Col. Lawrence Arrol, ''The Intelligence Fusion Family,'' *Military Intelligence*, Vol. 22, No. 3, July–September 1996.