A-FD-005-005/AF-003

Chemical, Biological, Radiological and Nuclear Defence Operating Concept

National Defence Défense nationale

Canada

Chemical, Biological, Radiological and Nuclear Defence Operating Concept

Chief of Force Development
National Defence Headquarters
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

Produced for the Chief of Force Development
by 17 Wing Winnipeg Publishing Office.
WPO30803

PHOTO CREDIT
Department of National Defence

NDID # A-FD-005-005/AF-003

Library and Archives Canada Cataloguing in Publication

Chemical, Biological, Radiological and Nuclear Defence Operating Concept.

"Produced for the Chief of Force Development by 17 Wing Winnipeg Publishing Office".
Includes bibliographical references.
Available also on the Internet.
Text in English and French on inverted pages.
ISBN 978-1-100-54318-5
Cat. no.: D2-302/2012

1. Military doctrine--Canada. 2. Canada--Military policy. 3. National security--Canada. 4. Canada--Armed Forces. I. Canada. Canadian Armed Forces. Wing, 17 II. Canada. Chief of Force Development III. Title: Concept d'opération en défense chimique biologique, radiologique et nucléaire.

UA600 C44 2012 355'.033571 C2012-980128-3E

Printed in Canada.

1 3 5 7 9 10 8 6 4 2

FOREWORD

I am pleased to present the Department of National Defence (DND) and the Canadian Forces (CF) *Chemical, Biological, Radiological and Nuclear (CBRN) Defence Operating Concept* as a supporting concept to the *Joint Operating Concept* and the *Integrated Capstone Concept*.

An analysis of the *Future Security Environment* and recent incidents around the globe such as the nuclear power plant incident in Fukushima, Japan in 2011, show the potential requirement for CBRN defence capabilities to support all six DND/CF missions outlined in the *Canada First* Defence Strategy.

To provide an effective response, DND/CF must develop adequate CBRN defence force structure and resources, which include properly trained and equipped personnel. To that end, the development of this *CBRN Defence Operating Concept*, which represents the synthesis of strategies, concepts, lessons learned and other products from across the CF and the government, presents, in general terms, the CBRN defence capabilities and structures to meet the requirements identified by the CFDS.

I commend all members of the Defence Team to use the *CBRN Defence Operating Concept*; it is the framework against which force development, generation and employment options will be critically evaluated in support of important decision analysis for the next phase of our collective force development activities.

M.F.R. Lloyd
Rear-Admiral
Chief of Force Development

TABLE OF CONTENTS

1 INTRODUCTION

General

This Operating Concept builds upon the conflict construct outlined in the *Joint Operating Concept* (JOC)[1] and the strategic impacts outlined in the *Integrated Capstone Concept* (ICC).[2] According to the conflict construct stated in the JOC, hybrid conflicts will entail a convergence or fusion of regular or irregular warfare techniques employed by state and non-state actors. In such a situation, no one type of warfare would necessarily predominate because the best synergistic effect is usually achieved by employing a wide range of fighting methods.

Within the range of hybrid conflicts, the proliferation of CBRN weapons continues to be among the most pressing threats to global peace and security. The scientific knowledge to create many CBRN weapons or improvised explosive devices is widely available. Despite efforts to develop and strengthen the existing non-proliferation, arms control verification, and disarmament regimes pertaining to CBRN weapons and material, sensitive CBRN technology, material and expertise continue to fall into the hands of belligerent states and non-state actors. For example, Toxic Industrial Materials (TIMs) are as deadly as some chemical warfare agents and since they can be easily acquired, TIMs are an attractive option for terrorists. Furthermore, accidental releases such as the nuclear power plant failure in Japan in March 2011, or deliberate sabotage pose a threat to the surrounding area/population. Thus, intelligence-led warning and typical preparation time to generate an appropriate response cannot normally be expected. Where a credible CBRN threat exists, an appropriate level of readiness should therefore be adopted to respond to a contingency or incident.

To establish a full-spectrum, general-purpose combat capability, DND/CF CBRN activities must be focused on defensive capabilities that enable joint forces to operate in a theatre where the threat and/or risk of a CBRN incident[3] exists.

1 *CF Joint Operating Concept* (Draft), Conflict Construct, (Ottawa: Chief of Force Development, no date), p.6.

2 DND, *Integrated Capstone Concept* (ICC), (Ottawa, Chief of Force Development, 20 October 2009), p.57.

3 CBRN incident – Any occurrence, resulting from the use of CBRN weapons or devices; the emergence of secondary hazards arising from counter-force targeting; or the release of toxic industrial material into the environment, involving the emergence of CBRN hazards or effects. (AJP-3.8) *Allied Joint Doctrine for CBRN Defence* (30 March 2012), p.Lexicon-2. Note: CBRN incidents are either "suspected" or "confirmed" as appropriate to the situation (AJP-3.8) Ibid., p.3-3.

Aim

The aim of this Operating Concept is to provide a framework for force developers, generators and employers to establish an effective CBRN defence Force Protection capability with the requisite capacity to achieve the objectives outlined in the *Canada First* Defence Strategy (CFDS).

Scope

The *CBRN Defence Operating Concept* recognizes both the strategic impacts stated in the ICC and the tactical and operational effects that a CBRN incident would have on CF operations in order to identify the CBRN defence capabilities and capacity required by DND/CF to fulfill its mission. In addition, it provides the CBRN defence principles and basic themes; it is not meant to address particular situations.

Link to the Integrated Capstone Concept

The ICC establishes what DND and the CF will need to consider when developing capabilities for future operations. In its final assessment, the ICC states that "Only by having a comprehensive view of the relationships between the condition sets, domains, and functions can we determine the requirements for being comprehensive, integrated, adaptive, and networked".

- **Comprehensive:** The ICC outlines three different aspects of being comprehensive. It must describe the complete strategic environment with all of the envisioned environmental domains. The problem may have to be continually redefined. Challenges forecasted in the *Future Security Environment* (FSE)[4] must be solved through a multi-disciplinary approach.

- **Integrated:** The term "integrated" is used to expand the meaning of "joint" and "combined" to include other actors and organizations within a Whole of Government (WoG) approach to operations.

- **Adaptive:** The ICC suggests that adaptation is the condition to respond to change and challenges in a positive and effective manner, and is essential for coping with complexities, thereby ensuring resilience and agility.

4 DND, *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends* (Ottawa, Chief of Force Development, 27 January 2009), p.9.

- **Networked:** There are two types of networks: human (or social) networks and technology-enabled networks. The existence of national networks; the nature of social networks; the importance of organizational networks, and the impact of technology on networks are of specific relevance to the DND/CF.

These characteristics are linked to the identified capabilities in this Concept and form a key part in the development of a CBRN defence capacity deemed necessary for the protection of DND/CF members and employees, equipment and infrastructure.

2 THE FUTURE SECURITY ENVIRONMENT

Increasing CBRN Threats

More than a decade into the 21st century, the proliferation of CBRN weapons continues to be among the most pressing threats to global peace and security. The scientific knowledge to create many CBRN weapons or Improvised Explosive Devices (IEDs) is widely available. Despite efforts to develop and strengthen the existing non-proliferation, arms control verification, and CBRN disarmament regimes, sensitive CBRN technology, material and expertise continue to fall into the hands of belligerent states and non-state actors.

In 2008, Defence Research and Development Canada (DRDC) led a CBRN Consolidated Risk Assessment (CRA) working group with representation from the Federal Science and Technology, operational, law enforcement, and intelligence communities. Founded on 45 plausible vignettes, the assessment considered the relative technical feasibility and impact of each scenario. The assessment concluded that, although a CBRN incident involving CF members is assessed a low probability of occurence, the military and political consequences will be high, particularly if it were to occur in Canada.

Published by Chief of Force Development (CFD) in 2009, *The Future Security Environment 2008-2030 (FSE) Part 1*: *Current and Emerging Trends*[5] notes that "the increasing commercialization of weapons (conventional, CBRN, and novel) will allow some developing nations and non-state actors to acquire inexpensive and sophisticated military capabilities. Hence, Canada and its allies may be confronted by a mixture of conventional, CBRN, and novel technology weapons in the hands of a variety of state and non-state actors, thus necessitating that Canada be able to apply the full spectrum of capabilities, even against non-state actors."[6] It is envisaged that such a threat against both military formations and civilian populations will remain a legitimate and growing concern through 2030. The *FSE Part 2: Future Shocks*[7] draft states that "a CBRN terrorist attack in Canada over the next twenty years, nuclear or otherwise, is a frightening and real possibility".

5 DND, *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends* (Ottawa, Chief of Force Development, 27 January 2009), p.85.
6 Ibid.
7 DND, *The Future Security Environment 2008-2030 Part 2: Future Shocks,* fundamental research (draft) (Ottawa, 17 December 2010), p.28.

The North Atlantic Treaty Organization (NATO) has stated that CBRN proliferation is the greatest threat facing Alliance members over the next 10-15 years.[8] At the November 2010 Lisbon Summit, the NATO Secretary General recommended that allies, among other things, develop their national CBRN defence capabilities.

8 NATO, NATO's Comprehensive Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending Against Chemical, Biological, Radiological, and Nuclear (CBRN) Threats, (1 September 2009), p.1.

3 CURRENT CBRN FORCE PROTECTION CAPABILITY

Concept of Operations

The first line of defence against CBRN effects on operations lies in preventing the proliferation of CBRN weapons. To this end, DND and the CF participate in, and support verification operations under existing international arms control agreements, as well as the development of future agreements and export control regimes. If such proliferation occurs, DND and the CF will participate in attempts to reverse it through either diplomatic means or through military action.

Canada's policy[9] with respect to CBRN weapons and agents is founded upon its obligations under numerous international arms control agreements. DND and the CF will never develop, produce, stockpile or otherwise acquire or retain biological or chemical agents or toxins, except in quantities necessary for defensive research, training, or for other peaceful purposes. DND and the CF will also never develop, produce, stockpile or otherwise acquire or retain or transfer, directly or indirectly, or use chemical weapons. Furthermore, DND and the CF will not use or participate in planning to use biological agents or toxins or receive the transfer of, control over, manufacture or receive assistance in manufacturing, or otherwise acquire nuclear weapons or other nuclear explosive devices. However, DND and the CF will maintain Canada's commitments and obligations as a member of NATO with respect to nuclear consultation and planning.

CBRN defence is a fundamental consideration for all military operations, missions or tasks in which a CBRN threat may be present or develop. Therefore, Canada's interest and intent in preparing for operations where the risk of a CBRN incident exists are solely defensive, as opposed to offensive, in nature.

Special Operations

The CBRN defence capabilities of any CF element committed to operations is the responsibility of the force generating agency.[10] The Canadian Special Operations Forces Command (CANSOFCOM) is comprised of a number of units including the

9 DND, DAOD 8006-0, *CBRN Defence* (Ottawa: VCDS, 25 June 2009).

10 DND, B-GJ-005-311/FP-000, *Canadian Forces Chemical, Biological, Radiological and Nuclear (CBRN) Defence Strategic Doctrine* (Ottawa: 31 March 2005), p.1-3-1.

Canadian Joint Incident Response Unit (CJIRU) that has the mission to provide specialized, timely and agile CBRN defence response to the Government of Canada (GoC);[11] CANSOFCOM is the force generating agency for this specialized capability. CJIRU purposely is a high-readiness unit capable of a wide range of specialized operations specifically designed to support Other Government Departments (OGDs) (domestic) and specialized support to CF operations (international). With this as background, CJIRU's mandate is to:

- Respond to CBRN incidents in conjunction with other elements of the National Chemical, Biological, Radiogical, Nuclear and Explosives (CBRNE) Response Team;
- Provide an agile integral part of the CANSOFCOM Immediate Response Task Force (IRTF); and
- Provide specialized support to CF expeditionary operations.

To further define these, domestically, CJIRU is the only fully dedicated CF contribution to the National CBRNE Response Team, an interagency National CBRNE Response Team comprised of the RCMP, Public Health Agency of Canada (PHAC) and the CF (CANSOFCOM-CJIRU). DND scientific support is provided to CJIRU and the National CBRNE Response Team on an *ad hoc* basis. Additionally, CJIRU is an integral part of CANSOFCOM's Immediate Response Task Force, which is mandated to respond to domestic counter terrorism. Lastly, CJIRU has a mandate to contribute to overseas operations, specifically supporting any deployed Special Operations Task Force(s) but, also has responsibility to support CF deployments until other Force Generators can ramp up to fulfill the role.

Domestic Operations

The DND/CF may become involved in a major domestic operation in support of law enforcement agencies, as was the case during Operations PODIUM and CADENCE in 2010. It may also be requested to support a WoG response to a CBRN incident in Canada. In either case, the DND/CF will be requested to provide support through the Minister of Public Safety. This support may include unique CBRN military expertise and resources, intelligence, and/or DND scientific support. The nature of the support would be mission specific and be based on either the requirements of the supported law enforcement agency or the request from

11 DND, *Canadian Special Operations Forces Command – An Overview* (Ottawa: CANSOFCOM, 2008), p.8.

provincial authorities for DND/CF support in the event of consequence management activities. While it is clear that DND/CF CBRN force protection capability primarily exists to support the CF, these same assets could potentially be requested to support civilian authorities in a CBRN consequence management role.

Without extensive preparation, as was the case with Operations PODIUM and CADENCE, the ability of the CF to provide specialist capabilities and military CBRN expertise to civilian authorities in response to a CBRN incident is very limited. Without a national consequence management framework, the DND/CF's ability to support these types of incidents remains limited. The key lessons learned from these recent operations suggest the requirement to complete the CBRN defence equipment modernization program and improve CF-wide CBRN defence training and readiness. The lack of trained CBRN defence advisors and of a standing conventional capability was also noted.

Expeditionary Operations

A CBRN threat may exist or may develop into a hazard in any CF expeditionary operation. The capability to survive a CBRN incident must be integral to our Forces, as Canada cannot rely on its allies for CBRN defence support. A high standard of individual training, readiness, and equipment is therefore essential for all three services.

Although they share the same requirements for their personnel, each of the three services has unique collective CBRN defence requirements, and as a result each has evolved different training and readiness postures, and operating procedures. The Navy has built CBRN protection (i.e. citadels and pre-wet systems) into its platforms, at least on the major warships, and has well-established Standard Operating Procedures (SOPs) for CBRN defence. Ships are also able to move out of a contaminated area reasonably quickly. The Air Force may be able to operate from airfields a long distance from the actual area of operations and therefore, from the potential CBRN threat. Aircrew may still, however, find themselves having to extract themselves from a contaminated airfield. Similarly, the Army may be required to extract itself from a contaminated environment where defensive capabilities across the three levels of Integral, Close and General Support are required.

Current CBRN Defence Limitations

Post-Operations Reports from Operations PODIUM and CADENCE have highlighted the significantly reduced state of CBRN defence in the CF. These reports indicated that:

- General knowledge of CBRN defence matters is lacking across the rank structure;
- CBRN defence readiness is poor due to a lack of equipment and training; and
- There is a lack of qualified CBRN defence staff.

The limitations that became evident during Operations PODIUM and CADENCE are equally applicable to expeditionary operations. There is a basic need to address overall situational awareness, training and readiness, equipment deficiencies, and both the capability and capacity of the CF to operate under the threat of a CBRN attack and if attacked, to survive, recuperate and if necessary, resume operations.

4 FUTURE CBRN DEFENCE CAPABILITY AND CAPACITY

Canada First Defence Strategy

To achieve the objectives outlined in the CFDS, the CF will provide the GoC with a joint force that defends the nation, delivers strategic effect and projects leadership abroad. The CF will be capable of executing multiple Lines of Operations (LOO) domestically and internationally, and may be required in some instances to execute these simultaneously. In addition, the CF must retain the capability to conduct routine domestic operations in Canada, across the North American continent with North American Aerospace Defence Command (NORAD), and have the capacity to support a major domestic effort such as Operation PODIUM and Operation CADENCE 2010.

The CF must be ready with an expeditionary force to undertake an operation in response to a crisis for a short period, which may be of a Humanitarian Operations and Disaster Relief (HODR) character, such as Operation HESTIA. This force will deploy to a low intensity, and normally to a permissive environment (by exception a non-permissive environment) to conduct limited spectrum operations for a short period of time. At the same time, the CF must be prepared to participate in a major international operation with a joint force for an extended period of time in a non-permissive environment up to medium intensity. In step with strategic warnings, a phased readiness approach will permit the CF to build combat power over time, gradually increasing to full spectrum operations.

Domestically, the CFDS "Excellence at Home" paragraph states that one of the three capabilities that the military will maintain is the capacity to "Assist civil authorities in responding to a wide range of threats – from natural disasters to terrorist attacks."[12] The threat of an intentional or accidental CBRN release, as a potential condition of the operating environment across the spectrum of CF roles and missions, validates CBRN defence as an enabling capability for the protection of our Forces should the CF be called upon during a CBRN incident.

It is understood that the impact on operations could range from immediate to delayed effects and consequences, and from local to theatre-wide coverage. A force, suitably protected against CBRN hazards, will be able to continue operations despite the incident. However, the lack of a suitable defensive capability will potentially preclude

12 DND, *Canada First Defence Strategy* (CFDS), (Ottawa: 12 May 2008), p.7.

a CF contribution to that operation. A force not enabled with a basic CBRN Force Protection capability unnecessarily risks significant casualties and mission failure.

Governance

In June 2009, the Defence Administrative Orders and Directives (DAOD) 8006 series addressing CBRN defence were issued under the authority of the Vice Chief of the Defence Staff (VCDS). The DAOD 8006 series addressed CBRN requirements and responsibilities in the CF structure that evolved from CF Transformation 2005-6. They apply to DND and the CF and cover policy, operations, training, capability development and sustainment. The DAOD 4002 series provides a comprehensive overview of Nuclear Technology Regulation and Control and Nuclear and Ionizing Radiation Safety. DAOD 4007-5 guides the Initial Response by Firefighters to Hazardous Materials Incidents or CBRN Incidents. In addition to the DAODs, this *CBRN Defence Operating Concept* provides the necessary framework for DND and CF force developers, generators and employers to establish the requisite CF CBRN defence capabilities to be employed either domestically or on expeditionary operations. This Operating Concept will be followed with the production of a *CF CBRN Force Employment Concept* (FEC) under the guidance of the Strategic Joint Staff (SJS), which will further enable DND and the CF to address the CBRN defence needs identified by CFDS.

Advice and Coordination

CBRN defence is a highly specialized enabling capability of Force Protection that requires staff with a full understanding of all technical aspects of employment and deployment of the CBRN defence capability in support of CF operations.

The SJS issues strategic direction on CBRN defence issues affecting DND and the CF, and acts as primary advisor to the Chief of the Defence Staff (CDS). The Directorate CBRN Defence (D CBRN D) is the Technical Authority for CBRN defence matters to the SJS (less Special Operations Forces (SOF) specific) including joint capability requirements, program coordination, doctrine, tactics, techniques and procedures. D CBRN D is the primary advisor to the Director of Staff (DOS) SJS for non-SOF roles for strategic guidance. The appropriate designated force employer will coordinate and advise on activities at the operational level.

Capability and Capacity

CBRN defence is the enabling capability that permits general purpose, combat capable forces to operate in a theatre where the threat and/or risk of a CBRN incident exists, and if attacked, to survive and, if necessary, recuperate and resume operations. An effective CBRN defence program and capability requirements are based on the five Enabling Components: Detection, Identification and Monitoring; Information Management; Individual and Collective Protection; Hazard Management; and Medical Countermeasures and Support.

From a structural perspective, CBRN force protection is applied across three levels of capability. The first is executed at the personal level (e.g. respirators, detectors) to ensure individual survival and to continue to support the operation. This is recognized as Integral Support. Next, there is a requirement to maintain or restore operational tempo within a short period, but which is beyond simple survival skills, and is normally conducted at the sub-unit or unit level (e.g. reconnaissance and surveillance, hazard avoidance). This is a Close Support function. Finally, there are additional functions such as thorough vehicle/equipment decontamination, sampling and identification which may be undertaken by the unit or attached specially trained elements. These functions are commonly referred to as General Support.

Further, an effective CBRN defence program would meet the following capability objectives:

- Provide CBRN situational awareness to all levels of command;
- Provide CBRN-related decision support to commanders and staff;
- Operate with the OGDs, civilian authorities and other agencies in domestic operations where a CBRN risk exists;
- Operate with the USA and other allies in domestic and defence of North America operations where a CBRN risk exists; and
- Operate with allies in international operations where a CBRN risk exists.

A detailed list of the capabilities necessary to meet these capability objectives is at Annex A.

CBRN trained, equipped and ready forces, as explained in Section Three, should be maintained to provide the necessary CF CBRN defence capabilities. Although no CF

CBRN defence assets would be dedicated to support civilian authorities, DND/CF assets could be requested during a domestic CBRN incident.

Services' and Operational Commands' Own Unique Requirements

While CBRN defence is a common function, there are differences in tasks and capabilities required across the three services that often require unique responses. CBRN defence staffs for each of the services and operational commands address their own unique requirements.

- **Maritime Forces**. The CBRN threat to ships and submarines at sea is very different from when in port or during littoral operations. Ships and submarines at sea are difficult chemical and biological targets, and the major warships have a high level of collective protection built into their platforms with the citadels and pre-wet systems. However, the onboard hangar for the embarked helicopter is not part of the citadel, and the pre-wet system may not sufficiently decontaminate the ship and aircraft. Naval elements are at their most vulnerable when in port. Littoral operations put maritime elements increasingly at risk when operating close to shore or transiting a narrow passage such as a canal.

- **Air Forces**. The threat to Air Force (AF) elements is focused primarily on the airfields and facilities that support air operations. Most chemical and biological agents will be dispersed close to the ground and remain at low altitudes. Only tactical helicopter elements are likely to face significant chemical and biological hazards away from the base or, in the case of maritime helicopters, when the Navy is conducting littoral operations. AF elements may use alternate facilities when primary bases become contaminated. This would minimize the challenge of decontaminating aircraft contaminated in an airfield attack since the capability for the decontamination of aircraft is very limited and weathering becomes the primary aircraft decontamination means.

- **Land Forces**. Land Force (LF) elements face all aspects of the CBRN threat due to their land-centric operating environment. They could face a direct attack on combat elements, together with strategic biological, persistent or non-persistent chemical, radiological, and possibly nuclear attack directed at any elements of the force. In domestic operations, the LF could operate in support of the local authorities. It is anticipated that CANSOFCOM and Canadian Army (CA) resources will assume the primary responsibility to provide DND/CF support

to civilian authorities following a CBRN incident given their readiness postures and force structures. The Army responsibilities for the generation of specialized CBRN capabilities are still being defined. Capacity will continue to define what can be accomplished on operations and the Army will continue to work to ensure that risks are defined and that progress is made toward defining clear capability requirements and managing risk while the resources to build those capabilities are found.

- **Special Forces**. Just as each Force Generating agency is responsible for maintaining its own integral CBRN defence and force protection capabilities,[13] CANSOFCOM is the Force Generator of this capability for Special Operations Task Forces that are employed in support of domestic and international operations. CANSOFCOM has very defined responsibilities for the generation of these specialized capabilities. Capacity will continue to define what can be accomplished on operations and CANSOFCOM will continue to work to ensure that risks are defined and that there is the required level of continuity where required.

Training and Education

The essential aim of any and all CBRN defence operations is the survival of personnel should CBRN incidents occur. For this reason, CBRN defence survival skills are taught in basic training and maintained as a general military skill throughout one's employment in the CF. All soldiers, sailors and air personnel therefore require training in the use of CBRN Individual Protective Equipment (IPE). This training should be conducted regularly to ensure proficiency in CBRN defence survival skills. The CF must ensure that a common standard of training and practice is maintained, regardless of the level of commitment of each organization.

Advanced individual training is the responsibility of the CF Fire and CBRN Academy (CFFCA) and for the RCN the CBRN sections of the Damage Control divisions on each coast. Due to the nature of its mission and mandate, the CJIRU will conduct much of its own training. DRDC, through the Scientific Advisor for Personnel Protection, Director General DRDC Suffield, will provide advice and guidance on the requirements for specialized knowledge and advanced training.

13 DND, B-GJ-005-311/FP-000, *Canadian Forces Chemical, Biological, Radiological and Nuclear (CBRN) Defence Strategic Doctrine*, (Ottawa: 31 March 2005), p.1-3-1.

5 CONCLUSION

CBRN defence capability can be critical to the success of a CF domestic or expeditionary operation where a potential CBRN risk exists. For this Operating Concept to add to the overall effectiveness of the CF and to the concepts presented in the *Integrated Capstone Concept,* CBRN defence capabilities must be responsive to the evolving threat, and their capacities sustained to meet a broad range of current and future threats within currently allocated resources. In today's volatile operating environment, a "just-in-time" approach to equipping and training the CF to face such threats may increase the risk that the CF will not have the necessary CBRN defence capabilities to respond to an evolving threat. At the same time, it could reduce the CF's ability to provide adequate specialized CBRN defence capabilities to assist civilian authorities, if requested to support a domestic CBRN incident.

This Operating Concept guides CF CBRN defence capability and capacity by addressing the statement in FSE *Part 1* which advises that "Canada be able to apply the full spectrum of capabilities, even against non-state actors".[14] It is a key component of the *Joint Operating Concept* and provides the necessary and comprehensive framework for DND and CF force developers, generators and employers to establish an effective CF CBRN force protection capability employable in either domestic or expeditionary operations.

Lastly, this *CBRN Defence Operating Concept* will further enable DND and the CF to respond to CFDS requirements.

14 DND, *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*, (Ottawa: Chief of Force Development, 27 January 2009), p.70.

ANNEX A – OUTLINE OF CBRN DEFENCE CAPABILITIES

General

As stated in the aim, this Operating Concept is designed to provide a framework for force developers, generators and employers to establish an effective CBRN defence force protection capability for the CF's joint forces, in domestic and expeditionary operations. This Annex outlines the capabilities necessary to accomplish the CBRN defence mission and mandate.

Detection, Identification and Monitoring (DIM)

The CBRN DIM system must be capable of providing systematic observation of aerospace and surface areas as well as examining objects to determine the presence of CBRN hazards.

It should be capable of passive and/or active operation and capable of detecting while on the move. It must be capable of being locally or remotely controlled. Sensors may be unattended but they all must be networkable.

It must be capable of detecting biological hazards, chemical hazards, and all levels and types of radiation, including when shielded, in liquid, solid and vapour forms.

The system must be capable of discriminating between local background activity and CBRN threat activity, airborne CBRN agents and airborne TIMs.

CBRN reconnaissance and survey system must be capable of:

- Verifying the hazard prediction area;
- Surveying to determine the extent of liquid and particulate CBRN hazard; and
- Operating in built-up areas.

CBRN identification system must be capable of:

- Identifying CBRN agents;
- Stating the concentration of the identified hazard;
- Indicating the greatest risk; and
- Providing spectral data.

CBRN monitoring system must be capable of:

- Monitoring contaminated areas; and
- Operating in built-up areas.

Information Management (IM)

The IM system must be capable of:

- Warning troops endangered by CBRN hazard in near real time;
- Making a rough estimate of CBRN hazard area in near real time;
- Making an accurate hazard prediction;
- Determining the source of contamination;
- Distinguishing between an instantaneous hazard release and a continuous hazard release;
- Applying changing weather conditions to an existing hazard prediction area;
- Providing CBRN situational awareness applicable at strategic, operational and tactical levels;
- Providing CBRN-related decision support to commanders and staff at each level of command;
- Providing guidance for planning and execution of CBRN defence in all phases of operations at each level of command;
- Reaching back to Canada for specialized analysis and advice; and
- Providing the means to manage the CBRN defence resources.

Physical Protection

Individual Protective Equipment (IPE) must be capable of:

- Providing protection for the whole body for identified CBRN hazards; and
- Providing protection without significantly degrading performance.

Collective Protection (COLPRO) must be capable of:

- Providing fixed facility and transportable COLPRO;
- Providing mobile COLPRO integral to sea, land and air platforms;
- Providing protection within existing splinter-proof shelters; and
- Providing COLPRO tailored for the functions to be performed within the facility.

Material Protection must provide CBRN defence equipment with the capability to:

- Continue to function in CBRN hazard conditions;
- Be capable of self-decontaminating; and
- Be capable of being protected by sacrificial coating.

Hazard Management

CBRN defence Contamination Control system must provide the capability to:

- Limit the spread of CBRN contamination; and
- Contain CBRN hazards.

CBRN defence Post-Incident Hazard Management system must:

- Decontaminate to levels required in the situation;
- Decontaminate personnel;
- Decontaminate mission critical platforms;
- Decontaminate small and large sensitive equipment;
- Decontaminate terrain vital to mission accomplishment; and
- Be capable of evacuating CBRN decontamination effluent.

Medical Countermeasures (Med CMs) and Support

For CBRN defence, DND/CF must be capable of providing safe, effective, licensed medical countermeasures to potentially exposed personnel. Further, the system must be capable of safely evacuating casualties from CBRN contaminated areas and evacuating CBRN casualties through uncontaminated areas. In addition, the system must provide:

- Prophylactic protection before exposure;
- First aid self-treatments against CBRN agents; and
- First Aid treatment of casualties in a CBRN environment.

ANNEX B – REFERENCES

B-GJ-005-311/FP-000, *Canadian Forces Chemical, Biological, Radiological and Nuclear Defence Strategic Doctrine*, 2007.

Canada First Defence Strategy (CFDS), 2008.

Canadian Special Operations Forces Command – An Overview, 2008.

CF Joint Operating Concept (Draft), 2011.

Defence Administrative Orders and Directives 4002-0 (2000), 4002-1 (2000), 4007-5 (2006), 8006-0, 8006-1, 8006-2, 8006-3 (2009).

The Future Security Environment (FSE) *Part 1: Current and Emerging Trends*, 2009.

The Future Security Environment (FSE) *Part 2: Future Shocks* (Draft), 2010.

Integrated Capstone Concept (ICC), 2010.

NATO's Comprehensive Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending Against Chemical, Biological, Radiological, and Nuclear (CBRN) Threats, 2009.