Ministry of Defence

Chemical, Biological, Radiological and Nuclear (CBRN) Defence

Allied Joint Publication 3.8(A)

Development, Concepts and Doctrine Centre

NATO STANDARD

AJP-3.8

ALLIED JOINT DOCTRINE FOR CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR DEFENCE

Edition A Version 1

MARCH 2012

NORTH ATLANTIC TREATY ORGANISATION

ALLIED JOINT PUBLICATION

Published by the
NATO STANDARDIZATION AGENCY (NSA)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION

NATO STANDARDIZATION AGENCY (NSA)

NATO LETTER OF PROMULGATION

30 March 2012

1. AJP-3.8 Edition A Version 1 – Allied Joint Doctrine for Chemical, Biological, Radiological, and Nuclear Defence is a non classified publication. The agreement of nations to use this publication is recorded in STANAG 2451.

2. AJP-3.8 Edition A Version 1 is effective on receipt. It supersedes AJP-3.8, which shall be destroyed in accordance with the local procedures for the destruction of documents.

Cihangir AKSIT, TUR Civ
Director, NATO Standardization Agency

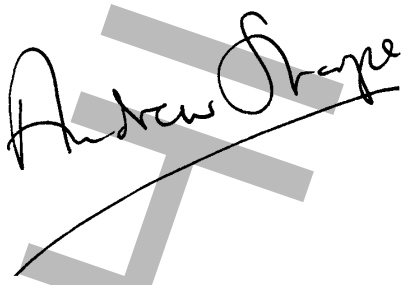
INTENTIONALLY BLANK

ALLIED JOINT PUBLICATION – 3.8(A)

ALLIED JOINT DOCTRINE FOR
CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR DEFENCE

Allied Joint Publication – 3.8(A) (AJP-3.8(A)), dated March 2012,
is promulgated in the United Kingdom as national doctrine

As directed by the Joint Force Commander and Chiefs of Staff



Director Concepts and Doctrine

Adopting NATO Doctrine

NATO underpins the defence of the UK and our allies, while also providing deployable, expeditionary capabilities to support and defend our interests further afield. As a founder member of the Alliance, the UK plays a full part in NATO with a range of permanent commitments, and the ability to assign further capability in times of crisis. European Security and Defence Policy specifies that NATO doctrine should be used in European Union-led military operations.

DCDC has, since its inception, played a leading role in producing NATO doctrine. We hold custodianship for ten NATO AJPs and participate actively in producing all others. However, until now, most NATO doctrine has been mirrored by equivalent, but different, UK Joint Doctrine Publications (JDPs). This has caused a dilemma for our Armed Forces who are most frequently committed to operations as part of NATO-based coalitions. It has also distracted DCDC effort away from playing an even greater role in the improvement of NATO doctrine.

With defence budgets reducing across Europe, the need to achieve maximum coherence and interoperability within, and between, our closest allies and partners has only increased. NATO is the institution best placed to help us achieve this. To that end, in July 2012, the Chief of the Defence Staff and the Permanent Under Secretary issued clear direction on how the UK's contribution to NATO could be further improved, stating that:

> 'We should use NATO doctrine wherever we can, and ensure coherence of UK doctrine with NATO wherever we cannot.'

In response, DCDC has undertaken a systematic study of the differences between NATO and UK joint doctrine to assess the risks in transition and determine:

- where a NATO AJP can be adopted in direct replacement of the JDP equivalent;
- where UK caveats or supplements are necessary in the form of 'green pages/paragraphs';
- what UK keystone publications are required to explain the UK strategic approach; and
- which NATO doctrine cannot replace the UK equivalent (i.e. the JDP must endure).

Where AJPs are adopted in lieu of a UK JDP, they will have a split cover (like this publication) with both DCDC and NATO livery and publication numbers. Some publications will have only the NATO approved text. Others will include UK text, diagrams, vignettes and even photographs, all with a green background or border to distinguish it. These additions will be made to explain a particular UK approach to operations, to aid understanding or to increase appeal/interest. No NATO text (against a white background) will be altered or removed.

This bold move will re-enforce the UK's commitment to NATO and give our Armed Forces greater interoperability within the coalition than ever before. It should also enable DCDC to take a far more active role in the production of NATO doctrine, to the benefit of the alliance as a whole.

DCDC welcomes feedback on this or any other subjects relating to joint doctrine. Please address correspondence to the DCDC Doctrine Coordinator at: The Development, Concepts and Doctrine Centre, Ministry of Defence Shrivenham, SWINDON, Wiltshire, SN6 8RF

Record of Changes

Change No.	Date Entered	NATO Effective Date	By Whom Entered (Signature; Rank, Grade or Rate: Name or Command)

INTENTIONALLY BLANK

Record of Reservations

CHAPTER	RECORD OF RESERVATIONS BY NATIONS

INTENTIONALLY BLANK

Record of Specific Reservations

NATION	SPECIFIC RESERVATIONS
BGR	1. The standardization document wil not be implemented in the part related to detection, sampling and identification of biological agents. CBRN units from the declared forces will perform their tasks in the area of detection of biological agents related only to fast manual antibody-based analysis. 2. Para 0312 Collective Protection will be implemented only from the declared forces in part of implementation of requirements and procedures for occupation and use of COLPRO that are provided from the lead nation during their participation in NATO led operations. Till acquisition of COLPRO which will fulfil ATP-70 requirements, Bulgarian Armed Forces will use their existing COLPRO systems.
CZE	Army of the Czech republic will not implement article 0317, letter c, dealing with "Clearance Decontamination". Further CZE has reservations concerning Chapter 3 of the Allied publication. Especially Section 3"CBRN Infromation Management" does not contain information on capabilities and functions of "CBRN reach Back and Fusion System" as stated in MC 0590"NATO CBRN Reach Back and Fusion Concept".
LUX	(1) For lack of specialized capabilities, Luxemburg will not apply section 6, “Medical countermeasures and support” ; (2) For lack of specialized capabilities, Luxemburg will not apply Annex A, paragraph A02, “Threat and Hazard Evaluation”.
NLD	The NLD disagrees with the content of Chapter 3, pt0301(2) and Chapter 3, pt0305c. NLD will regard "Information management" as "Warning & Reporting" and will keep this as a seperate enabler instead of "Information management". NLD will use "CBRN Information Management" in the broader context of Command & Control, including intelligence dissemination and Reach Back, although the latter as a national asset only.
GBR	As noted in the Record of Specific Reservations for AJP3-14 *Allied Joint Doctrine for Force Protection* the UK does not support the NATO definition of Force Protection (paragraph 0102 a). The UK definition, given in JDP3-64 *Joint Force Protection* is as follows: *The coordinated measures by which threats and hazards to the Joint Force are countered and mitigated in order to maintain an operating environment that enables the Joint Commander the freedom to employ Joint Action.*

	The UK considers the scope of CBRN defence to be wider than that given in paragraph 0103, including support to both political activity to reduce the CBRN threat cooperatively and actions to counter, as well as mitigate, the threat in a non-permissive environment. The UK considers this to be part of the 'prevent' activity discussed in NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending against CBRN Threats and believes that the definition of CBRN defence in NATO doctrine will need to be widened to encompass this. Within the UK, the component of CBRN defence titled 'Detection, Identification and Monitoring' (paragraph 0301 a (1)) is referred to as 'CBRN Sense'. The component titled 'CBRN Information Management' (paragraph 0301 a (2)) is titled 'CBRN Knowledge Management'. The UK agrees with the listed constituents of each component, but believes that the UK titles are more accurate descriptions of their role. The UK has introduced an additional CBRN dress state (dress state Zero Charlie) in addition to those given in Table C5, which is equivalent to the NATO CBRN Dress State Zero). For the UK, dress state Zero now means that a CBRN respirator need not be carried at all times, reflecting the reality of current operations.

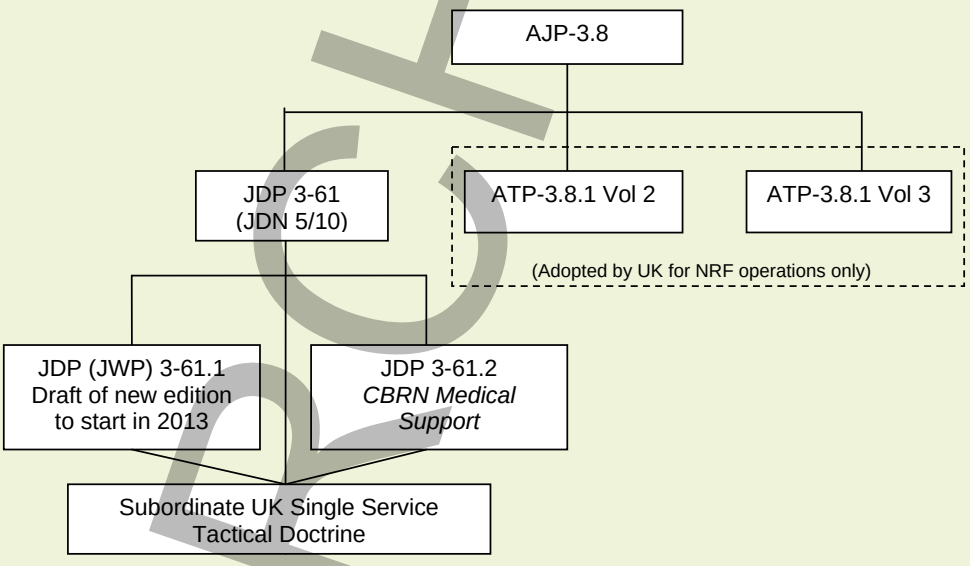
UK Preface

AJP 3.8 and the UK's CBRN Doctrine Hierarchy

Allied Joint Publication (AJP)-3.8 *Allied Joint Doctrine for Chemical, Biological, Radiological and Nuclear Defence* provides the highest level of Allied and UK doctrine for CBRN defence. In the Allied Joint Doctrine Architecture, AJP-3.8 provides the environmental context for the three subordinate volumes of ATP-3.8.1. Although the UK has ratified Volume 1, which contains operational level guidance, it has not been adopted. Because of the unique composition of the UK's Counter-CBRN capability and the subtly different national approach towards CBRN at the operational level, this guidance is provided within the UK's Joint Doctrine Publication (JDP) 3-61 *Counter-CBRN: the Military Contribution*.

NATO policy categorises all CBRN defence activity within the three 'pillars' of prevent, protect and recover. AJP-3.8, in its current form, only deals with the 'protect' pillar while JDP 3-61 provides UK guidance regarding prevent and recover activities. Work on a revised edition of AJP-3.8 that will address all three pillars will commence in 2013.

Despite the differences at the operational and tactical levels, it must be emphasised that the UK's CBRN Defence doctrine hierarchy is fully integrated with, and aligned to, the NATO Doctrine Architecture. Furthermore, UK CBRN doctrine, at all levels, is NATO STANAG compliant.



INTENTIONALLY BLANK

Preface

1. Purpose and Scope

a. Allied Joint Publication (AJP)-3.8 provides North Atlantic Treaty Organization (NATO) strategic and operational commanders with fundamental principles for the planning, execution, and support of NATO operations for which the threat and/or risk of intentional or accidental use of chemical, biological, radiological, and nuclear (CBRN) substances are either assessed or exist. These CBRN defence principles provide a foundation for and guide the joint force in identifying required CBRN defence capabilities. The application of these CBRN defence principles will enable the joint force commander to take appropriate countermeasures before, during and after a CBRN incident or in the framework of operations aiming at preventing the proliferation of weapons of mass destruction (WMD) and defending against CBRN threats.

b. AJP-3.8 does not cover offensive actions to nullify, eliminate, or disable CBRN weapons or their delivery systems, however, the principles and capabilities described here may be employed by commanders during countermeasure operations designed to prevent CBRN incidents. They may also be used as part of the overall response to manage the consequences of a CBRN incident.

c. AJP-3.8 describes military capabilities developed according to alliance forces requirements. These military capabilities could be employed in reinforcement of or in addition to insufficient or non-existing civilian capabilities in case of CBRN incidents.

d. Although AJP-3.8 is intended for use by NATO forces, the doctrine is equally applicable to operations conducted by a coalition of NATO and non-NATO nations within the framework of a NATO-led combined joint task force or for European Union-led operations using NATO assets and capabilities.

e. Even if the primary goal of CBRN Defence is to protect against effects and recover from the consequences of a CBRN incident, the CBRN defence capabilities can provide an effective military contribution to preventing WMD proliferation. Thus, the AJP-3.8 will be a transitional document, which will be followed by a rapid development of successor doctrine that will incorporate the 3 pillars *(Prevent, Protect and Recover)* described in the 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 and the Comprehensive NATO CBRN Defence Concept.

2. Structure

a. AJP-3.8 consists of four chapters supported by four annexes as follows:

(1) Chapter 1, "Fundamentals of CBRN Defence," provides an overview of the strategic context and fundamentals of CBRN defence;

(2) Chapter 2, "CBRN Threats and Hazards," examines the spectrum of CBRN threats and hazards which may be encountered in the operational environment;

(3) Chapter 3, "Enabling Components of CBRN Defence," identifies the enabling components and characteristics of CBRN defence;

(4) Chapter 4, "Command Considerations for Planning and Conduct of CBRN Defence," provides command considerations for planning and conduct of CBRN defence, including priorities, staff organisation and actions before, during and after a CBRN incident;

(5) The annexes provide several specific focus areas such as: aspects of intelligence preparation of the operational environment (IPOE); risk management; threat levels; and CBRN consequence management (CM). A lexicon of terms is also included.

3. Hierarchy and Related Publications

a. AJP-3.8 is directly subordinate to keystone AJP-3 Allied Joint Doctrine for the Conduct of Operations which describes the fundamental operational aspects of joint operations and provides guidance on conducting joint operations. AJP-3 is directly subordinate to AJP-01 Allied Joint Doctrine.

b. AJP-3.8 is supported by Allied Tactical Publication (ATP)-3.8.1 which expands on the fundamental CBRN defence principles. ATP-3.8.1 is published in three (3) volumes:

(1) ATP-3.8.1 Volume I - CBRN Defence on Operations. This volume provides detailed information guidance on operational CBRN defence planning and implementation of CBRN defence measures to those involved in the preparation, planning and execution of joint operations.

(2) ATP-3.8.1 Volume II – Specialist CBRN Defence Capabilities. This volume provides tactical level commanders and their staff with the principles and fundamentals in the use of specialist CBRN defence capabilities in support of joint operations after a CBRN incident.

(3) ATP-3.8.1 Volume III - CBRN Defence Standards for Education, Training and Evaluation. This volume provides details on CBRN education, training, exercise planning and evaluation protocols.

Table of Contents

List of Tables

List of Figures

Chapter 1

Fundamentals of CBRN Defence

0101. Strategic Context

"NATO faces a whole range of complex challenges and threats to its security, much different from the threat faced by Allies when the Alliance was formed. Present and future security challenges require NATO to be prepared to protect and defend against both State and non-State actor threats. Current threats include the proliferation of CBRN weapons and their means of delivery. In particular, the Comprehensive Political Guidance endorsed at the 2006 Riga Summit noted the spread of CBRN weapons and substances and the possibility that terrorists will acquire them, as the principal threats to the Alliance over the next 10-15 years. Recognising this, the Alliance has been vigilant in developing policies to deal with the significant and growing threat of proliferation of CBRN weapons, which establish the basis for our work today. Despite significant progress, however, major challenges remain. Non-adherence to international arms control, disarmament and non-proliferation commitments, and programmes to develop CBRN weapons and their means of delivery, can undermine global norms and pose a threat to Alliance security. Nuclear weapons and radiological and chemical agents that remain in the world could be vulnerable to exploitation if not properly secured. Rapid advances in biological science and technology continue to increase the bio-terrorism threat and there are indications that terrorists intend to acquire CBRN substances for malicious purposes. Recognising the difficulties associated with defending against these threats - especially those that derive from non-State actors - the Alliance must take a pragmatic and practical approach to address them.

Because of the potentially devastating consequences of CBRN use, robust passive defence and mitigation measures must be in place to enable NATO forces to continue effective military operations in a CBRN environment and to permit NATO and appropriate civilian agencies to assist Allies and partners when CBRN weapons and devices are used against them. Further development of the Alliance's core CBRN defence capabilities remains a top priority, as well as ensuring an appropriate level of CBRN expertise and manning. CBRN defence capabilities are identified in NATO's military guidance for capabilities needed to operate in a CBRN environment and contribute to the prevention of CBRN proliferation; they are also reflective of the ongoing work in support of NATO's Defence Against Terrorism (DAT) Initiative.

In light of the evolving security climate and a greater emphasis on responding to State and non-State employment of CBRN, additional and/or enhanced capabilities will be given higher priority, including: CBRN stand-off detection and identification, collective protection against CBRN, explosive ordnance disposal/improvised explosive device disposal, and

development of render safe capabilities. The Alliance will also continue to enhance capabilities to support consequence management and crisis management."[1]

a. CBRN threats pose unique challenges to NATO operations. The disruptive, destructive and potentially devastating effects of these weapons and substances merit continuous consideration by NATO's joint force commanders (JFCs) and supporting commanders. Robust passive defence and mitigation measures must be in place to enable NATO forces to continue effective military operations in a CBRN environment and effectively deter adversaries from considering the use of CBRN weapons and substances, and to permit NATO and appropriate civilian agencies to assist Allies and partners when CBRN weapons or devices are used.

b. Despite the existence of a broadly (but not universally) accepted regime of international agreements addressing the obligations of states parties in respect of matters such as the development, stockpiling, proliferation and use of certain CBRN weapons, potential adversaries continue to develop and field CBRN weapons or substances. This trend is most pronounced in areas of chronic political instability where NATO may be called upon to mount operations. Additionally, there have been recurring instances of terrorist and other ad-hoc groups seeking CBRN technologies as a powerful means of prosecuting their interests. Unfortunately, scientific advances are unintentionally reinforcing these processes, aided by the free migration of information and scientific expertise around the world. At the same time, expanding urbanization and the process of global industrialization opens up the wider possibilities of accidental release or deliberate misuse of toxic industrial material (TIM).

c. This environment presents numerous opportunities for NATO forces to encounter antagonists possessing CBRN capabilities. These may be CBRN weapons or improvised devices incorporating either CBRN agents or TIM. NATO forces may also be exposed to hazards from these substances as a result of accidental or deliberate release or as consequences of counter-force activity. Survivability and in many cases operability following a CBRN attack or the release of TIM requires a coherent response from, at a minimum, medical, environmental and industrial hazard and CBRN defence staff to mitigate the effects of an incident. Figure 1-1 depicts the origins of CBRN threats and hazards.

[1] 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 Sep 09

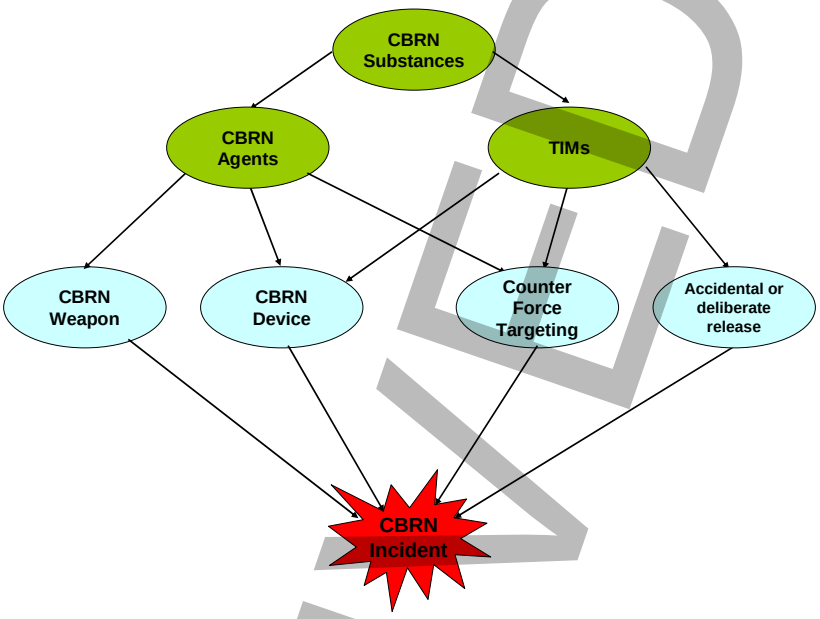


Figure 1-1 CBRN Hazard Origin

d. In the planning and conduct of operations, it is vital that commanders consider the possible emergence of CBRN hazards and develop appropriate CBRN defensive measures against their effects. The characteristics of the threat and associated protective measures should be continually revisited to ensure that both survivability and freedom of action are maintained. The importance of rapid deployment will grow and the need for more agile CBRN defence units with shorter reaction time represents a significant challenge to commanders. With regard to the planning and conduct of operations, the need for closer civil – military coordination has to be reflected in standing operating procedures (SOP), agreements and the concept of operations.

0102. Force Protection and CBRN Defence

a. Force protection (FP) includes all measures and means to minimize the vulnerability of personnel, facilities, materiel, operations and activities to threats and hazards in order to preserve freedom of action and operational effectiveness thereby contributing to mission success. The primary purpose of FP is to conserve the fighting potential of the deployed force by countering the wider threat to all its elements from adversary, natural and human hazards, and fratricide. It minimizes and mitigates both the threat of attack and the effects of any attack by an adversary, including CBRN incidents, and environmental and other hazards. FP also reduces interference of military operations by the civil population, and the threat of attack by irregular forces.

b. FP is not an issue that can be addressed separately or in isolation. It is an integral part of joint operations and is outlined in AJP-3.14 Allied Joint Doctrine for Force Protection. CBRN defence should be an integral part of the any FP plan. To increase survivability and freedom of action, especially when operating in austere environments, CBRN defence measures and capabilities need to be flexible, mobile, rapidly deployable and sustainable.

The UK definition of joint force protection is defined in Joint Doctrine Publication (JDP) 3-64 as:

> The coordinated measures by which threats and hazards to the Joint Force are countered and mitigated in order to maintain an operating environment that enables the Joint Commander the freedom to employ Joint Action.

The UK definition is derived from the requirement for force protection within the context of the UK approach to operations. It recommends a more proactive approach which includes countering threats and hazards, in addition to mitigating actions.

0103. Definition of CBRN Defence

Plans and activities intended to mitigate or neutralize adverse effects on operations and personnel resulting from: the use or threatened use of chemical, biological, radiological or nuclear weapons and devices; the emergence of secondary hazards arising from counter-force targeting; or the release, or risk of release, of TIM into the environment.

The UK considers CBRN defence to comprise of six areas which include:

- arms control;
- preventing supply;
- deterrence;
- disablement[1];
- protection; and
- elimination[2].

It should be noted that only CBRN protection is considered part of force protection. NATO currently has no equivalent term for CBRN protection, but the NATO definition of CBRN defence given at paragraph 0103 closely matches the UK definition of CBRN protection. So, the UK audience should equate the term 'CBRN defence' in AJP-3.8 to the UK's term 'CBRN protection'.

[1] Disablement is the temporary removal of a CBRN capability against the will of the governing authority. It takes place in a semi or non-permissive environment and is a predominantly military activity.

[2] Elimination is the permanent removal of a CBRN capability with the consent of the governing authority. It takes place in a permissive environment and is a predominantly civil activity.

0104. Aim of CBRN Defence

The aim of CBRN defence is to help to prevent the CBRN incidents, protect NATO forces from the effects of CBRN incidents, and to take recovery actions, so that NATO forces are able to accomplish the mission and maintain freedom of action in a CBRN environment.

0105. Principles of CBRN Defence

CBRN defence principles, in conjunction with the FP principles, are established for use as guidance for strategic and operational level commanders and their staffs. These principles need to be taken into consideration during the planning phase of an operation. They provide a foundation for the conduct of CBRN defence on operations before, during and after a CBRN incident. CBRN defence principles compromises the following:

a. Assessment of the Threat. Threat assessments are based on accurate and timely all-source intelligence. Threat assessments must be conducted and continuously reviewed so that the appropriate CBRN defence capabilities and protective measures are selected and adjusted as required. Intelligence sharing among Allies and non-NATO entities is essential for producing actionable intelligence.

b. Risk Management. CBRN risk and vulnerability assessments are required as part of any full assessment of the operational risk to a force entering a joint operations area (JOA). As with wider FP, the principle is risk management, but not risk elimination. Risk and vulnerability assessments linked to CBRN defence provide the opportunity to look at specific CBRN threats, and identify areas for increased measures to limit the operational impact of a CBRN incident. Individual and collective protection (COLPRO), for example, may increase operational capability but at a cost to operations. Casualties and materiel degradation are inevitable in any military operation even without conflict and a desire to avoid them totally is likely to impact adversely on the achievement of the mission. Commanders must manage the balance of human and material costs against operational imperatives. Contamination avoidance, within the dictates of mission requirements, should be a primary consideration. Differences in individual nations' FP philosophies must be resolved to achieve a concerted and common goal. Annexes B and C provide further guidance on risk management and its applicability to CBRN defence.

c. Interoperability. CBRN defence should encompass all components of the joint force, both military and civilian, and address all aspects of threat reduction and mitigation based on a comprehensive threat assessment. Within the JOA, every effort must be made to optimize overall CBRN defence posture through the harmonizing of respective nations' and, where appropriate, host nation's capabilities and information exchange at operational and tactical levels.

d. Prioritization. Notwithstanding that CBRN defence needs to embrace the whole force, it is unlikely that CBRN defence specialist capabilities will be available in sufficient quantities to support all elements of the joint force to the same degree. Priority therefore needs to be given to operationally essential personnel, equipment and infrastructure.

e. Flexibility. CBRN defence must be flexible, modular in application and capable of responding to a rapidly changing threat and operational environment while cognizant of differing national guidelines.

The principles of joint force protection described in JDP 3-64 are: hazard and threat assessment; risk analysis and management; coordination and integration; and flexibility. These are very similar to the principles given above.

Chapter 2

CBRN Threats and Hazards

0201. Introduction

The boundaries between natural and man made threats and their resulting hazards are often difficult to distinguish at the time of the incident. Initially, it may not be possible to differentiate between a deliberate attack and an accidental release, or the outbreak of an endemic/pandemic pathogen. Commanders, therefore, must be able to respond appropriately to the entire threat spectrum based on CBRN defence principles and using resources such as environmental, force health protection and medical assets. ATP-3.8.1 Volume I, CBRN Defence on Operations, elaborates on the operational aspects of CBRN defence planning and implementation. The following subsections summarize the characteristics and effects of the various types of CBRN substances that may be employed by an adversary.

0202. Characteristics and Effects of Chemical Agents

a. Chemical agents are substances which are intended for use in military operations to kill, seriously injure, or incapacitate humans through their physiological impact. The term excludes riot control agents, herbicides and substances generating smoke and flame. Chemical agents can affect different physiological systems by entering the human body through ingestion, skin or eye absorption, and inhalation. They are categorized according to their physiological effects: nerve; blood and choking; and blistering agents. A second useful operational classification of chemical agents is in terms of their persistency.

b. Persistency. In biological or chemical warfare, persistency is the characteristic of an agent which pertains to the duration of its effectiveness in the environment. This varies greatly between agents and is conditioned by agent composition and the influences of weather and terrain.

(1) Non-Persistent Agents. Non-persistent agents are delivered as aerosols or liquids and usually are more lethal agents. Non-persistent agents tend to produce only short-term hazards because they are carried away by even a light wind, although this may cause a downwind hazard. They cause little or no surface contamination.[2]

(2) Persistent Agents. Persistent agents generally take the form of liquid droplets that contaminate surfaces and produce a contact hazard that will penetrate ordinary clothing and then the skin. They also evaporate

[2] Note: Adversarial use of non-persistent agents is likely to be as ‘suppressing fire’ which can be ‘lifted’ rapidly as required.

to form a vapour hazard but this is likely to be less concentrated than the vapour formed by a non-persistent agent. The vapour hazard will exist for as long as the liquid remains or absorbent material continues to off-gas. This can vary from as little as a few days to several days or weeks, depending on the agent and the climatic conditions.[3] Of the two, persistent agents tend to present a greater hazard to deployed forces due to their significant and prolonged contact hazard and the subsequent requirement for effective decontamination. This makes their use particularly attractive to any adversary.

c. Classes of Chemical Agents

(1) Lethal Agents. These comprise the nerve agents, blood and choking agents, and blistering agents:

(a) Nerve Agents. These agents interfere with the nervous system and disrupt bodily functions such as breathing and muscular co-ordination. They may be in persistent or non-persistent form and are cumulative in effect so that repeated doses will produce progressively more serious effects.

(b) Blood / Cyanogen Agents. These agents prevent body tissues from utilizing oxygen in the blood and, in high concentrations, cause rapid respiratory failure. They tend to be highly non-persistent in nature and are generally lighter than air which lessens their overall utility as they persist for only a brief time (seconds/minutes) in the immediate area of employment. Nonetheless they can represent a significant challenge to respirator filters.

(c) Choking / Lung Damaging Agents. These agents attack the breathing passages and cause large quantities of fluid to seep into the lungs, which has a drowning effect. They are non-persistent in form.

(d) Blister Agents / Vesicants. These agents injure the eyes and the lungs, and burn or blister the skin. They can kill but their principal military utility is to damage the body and deny the use of ground. Most blister agents are persistent, however persistency varies depending on the chemical form and environmental factors. They present a contact hazard and both local and downwind vapour hazards. They cause inflammation and, after several hours, blistering of the skin, eyes and

[3] Note: Adversarial use of persistent agents is likely to be to deny ground and/or critical infrastructure as well as to inflict casualties.

breathing passages. Effects are cumulative, as with nerve agents.

(2) Incapacitating Agents. These agents cause temporary disabling conditions which can be either physical or mental and can be viewed normally as non-lethal. However, in extreme concentrations or where unprotected personnel are exposed to them over extended periods, they may also cause death but this is not their primary purpose. Incapacitating agents are not, by their legal definition, considered to be chemical agents when used for law enforcement purposes, such as riot control.

0203. Characteristics and Effects of Biological Agents

a. **Classes of Biological Agents.** The major classes of biological agents are:

(1) Bacteria. Bacterial agents are those that are pathogenic to humans, plants and animals either by causing infectious diseases or by producing toxins. Antibiotic medications have been successful in controlling some bacterial infections; however, bacteria can gain antibiotic resistance, either naturally or through genetic modification.

(a) Rickettsiae. Rickettsiae are organisms similar to bacteria that cause diseases such as spotted fever, typhus and scrub typhus. Rickettsiae agents are normally sensitive to antibiotics.

(b) Chlamydia. Chlamydia are intracellular parasites incapable of generating their own energy source. They are responsive to broad-spectrum antibiotics. Like viruses, they require living cells for multiplication.

(2) Viruses. Viruses, the simplest type of microorganisms, lack a system for their own metabolism and depend on host cells. They cause disease by damaging host cells in target organisms (humans, animals, plants). Viruses are not sensitive to antibiotics, but some may be treated by antiviral compounds. Additionally, vaccines have been developed and are available to prevent infection by some viruses.

(3) Toxins. Toxins are chemicals of natural origin produced by an animal, plant or microorganism, which can cause significant illness at levels much lower than the level required for lethality, and are thus militarily significant incapacitants. Toxins are not sensitive to antibiotics, but antidotes and detoxicants for some toxins exist.

(4) Parasites. Parasites are organisms that benefit by exploiting their hosts (animal, human or plant) for food, habitat and dispersal.

Parasites reproduce more quickly and in greater numbers than their hosts, and can rapidly reduce the health of the host.

(5) Fungi. Fungi are primitive organisms that are capable of causing disease in humans. Spores of mycotoxin-producing fungi are possible anti-personnel biological weapon agents due to their stability, ease of manufacture, and ease of dissemination in aerosol form. Several species of fungi are also effective weapons against domesticated animals. Fungi can also serve as anti-crops agents.

b. Some agents are transmissible whilst others have the capacity to present a sustained, albeit localized, hazard after dissemination. Biological agents which are both environmentally persistent and person-to-person transmittable presents increased complications to NATO forces and local populations.

c. Persistency of biological agents varies greatly and depends on specific agent characteristics and environmental conditions (solar radiation, relative humidity, wind speed, and temperature gradient). Ultraviolet light accelerates decay of most biological agents however, encapsulation or genetic engineering may protect agents from natural decay and increase their persistency.

0204. Characteristics and Effects of Radiological Material

a. Radiological dispersal devices (RDDs) can spread or disperse radioactive materials to produce contamination hazards that could inhibit or degrade military operations. radiological exposure devices (REDs) have the means to contaminate a localized area or have an effect on personnel. Additional hazards may result from radioactive materials released from industrial activities or expended munitions.

b. Radioactive hazards resulting from a RDD will affect a much smaller area than radioactive hazards from a nuclear detonation. Terrorists and other adversaries employing RDDs will likely choose delivery means which maximize the dispersion of radioactive material. These can include explosive dissemination, direct spraying or scattering, or dispersal of solid or liquid aerosols downwind. Fire and smoke can also be used to disperse radioactive material. In addition, a large external gamma source could be employed as a RED and positioned to cause casualties. Detection and management of the hazard will depend on the type of radioactive material present.

c. **Effects.** Radioactive materials have an effect on the human body by direct irradiation, through skin contamination, or via ingestion or inhalation and thus internal contamination. Whereas a radioactive hazard external to the body can be removed or avoided relatively easily, internal contamination is harder

to deal with and decaying radioactive material will continue to cause long term damage until it is removed or excreted from the body. The impact on personnel of any radiation hazard will depend on the equivalent dose received. Equivalent dose is an attempt to allow for the different relative biological effects of different types of ionizing radiation and is calculated by multiplying the absorbed dose by a radiation weighting factor. This weighting factor reflects the type and energy of the radiation incident on the body, or in the case of sources within the body, emitted by the source. Whereas the radiation weighting factor is pre-determined by the radioactive source associated with the hazard, the absorbed dose is dependant upon the proximity of personnel to the source, the degree of shielding afforded to exposed personnel and the duration of exposure.

0205. Characteristics and Effects of Nuclear Weapons

a. **General**. The international security environment encompasses threats from potential adversaries armed with nuclear weapons or devices.

b. **Effects**. The nature and intensity of the effects of a nuclear detonation are functions of the type of weapon, its yield, the physical medium in which the detonation occurs, and the characteristics of the target. At the point of detonation, a typical nuclear weapon will release massive amounts of energy which will be manifested in various ways:

(1) Flash. The immediate flash from a detonation within the atmosphere gives a very short warning to forces in the local area to take cover from the subsequent nuclear effects. Flash can cause permanent or temporary blindness and dazzle, particularly at night. Secondary hazards will result from personnel who are blinded or dazzled whilst operating equipment and platforms, particularly in the air.

(2) Thermal. Thermal radiation can cause severe burns to exposed skin and ignite local flammable material which can also cause burns. Thermal radiation can burn, distort or melt equipment and start fires which may also destroy equipment and resources. Uncontrolled fires in forest or urban areas can also pose a significant hazard.

(3) Blast and Shock. Blast and shock can damage or destroy maritime, land or air platforms as well as equipment, supplies, field-defences, fixed installations and infrastructure. The associated pressure front will be a hazard to personnel both directly and indirectly through flying debris and the razing of structures and trees. This wholesale destruction of urban and rural areas can create significant obstacles to movement.

(4) Initial Nuclear Radiation. In the immediate vicinity of any nuclear detonation, high levels of initial nuclear radiation (INR) are produced which can cause immediate incapacitation and death. This INR, however, decreases rapidly with distance from the fireball and last only as long as nuclear fission occurs. Associated neutron induced activity (NIA) will produce high levels of radioactivity and a consequent hazard in the local area.

(5) Fallout and Rainout. Nuclear fallout consists of fission products resulting from the nuclear explosion itself and debris drawn up into the fireball and subsequently contaminated. It represents a significant radioactive hazard which will be spread by prevailing winds but which will progressively decrease in intensity. Occasionally a nuclear burst will trigger precipitation which removes radioactive particles from the atmosphere and deposits them onto the ground. This will create nuclear fallout by rain, or rainout, which is likely to be highly radioactive and which will pose a significant liquid and ground-contaminating hazard where the precipitation falls and where it collects.

(6) Electromagnetic Pulse (EMP) and Transient Radiation Effects on Electronics (TREE). Normally the EMP produced by a nuclear explosion is attenuated by the atmosphere to such an extent that the damage caused by all other nuclear weapon effects becomes far more significant. However, a burst outside the atmosphere (exo-atmospheric) has the potential to create significant TREE and EMP effects which put all electronics and electrical equipment at risk. The initial component of an EMP is created when high energy gamma radiation from a nuclear detonation liberates electrons from atoms in the upper atmosphere. These electrons travel in a generally downward direction at speeds greater than 90 percent of the speed of light. This short lived but intense pulse of energy can induce dangerously high voltages and current spikes in unshielded electronics. In addition to this initial component of an EMP, the nuclear explosion can also cause a rapid displacement of the Earth's magnetic field and a subsequent returning of that field to its normal position. This can cause geomagnetically induced electrical currents in long conductors which again can damage electrical equipment. The nuclear radiation from the same burst can also put satellites, within line of sight of the detonation, at risk from TREE. TREE is similar to the EMP observed on the Earth's surface in that electronic components can be damaged however, the mechanism for this damage does not rely on interactions within the Earth's atmosphere. Rather it is a result of radiation directly affecting electronic components on a molecular level. It is important to note that the Transient part of the acronym TREE refers to the Radiation and not

the Electronic Effects, which can be long lasting or even permanent. EMP and TREE will inhibit communications and damage or destroy electronic equipment unless specific hardening measures are taken.

(7) Increased Ionosphere Activity. Although the main threat to communications and electronic equipment comes from the EMP itself, increased ionization within the atmosphere following a nuclear explosion can create other long term effects. The propagation of radio waves through the atmosphere can be degraded or even prevented across all frequencies however, it is High Frequency (HF) communications that are especially susceptible with long range, over the horizon communication being particularly vulnerable. Satellite communications systems, including the Global Positioning System, while not as susceptible as HF communications, could also be degraded although these effects would tend to be much more localised and transitory.

c. **Classes of ionising radiation:**

(1) α (Alpha) - emissions (relatively large particles / prevent inhalation)

(2) β (Beta)- emissions (very small particles, penetrates the skin)

(3) γ (Gamma)- emissions (electromagnetic radiation)

(4) neutron

0206. Characteristics and Effects of Toxic Industrial Materials

TIM is a generic term for toxic chemical, biological and radioactive substances in solid, liquid, aerosolized, or gaseous form created for industrial, commercial, medical, or domestic purposes. Normally, such materials are retained within their planned manufacturing, storage, and transport facilities. However, their intentional or accidental release may pose a significant hazard. Forces may be exposed to TIMs as a consequence of friendly action, adversary action, or accidents.

a. Toxic Industrial Chemical (TIC). Industrial chemicals can pose significant toxic hazards and can damage the human body and equipment. Many industrial chemicals are corrosive, flammable, explosive, or react violently with air or water; these hazards may pose greater short-term challenges than the immediate toxic effects. Most but not all TICs will be released as vapour or highly volatile liquid and can have both short-term and long-term health effects. The most important action in case of a massive industrial chemical release is immediate evacuation outside the hazard's path. The greatest risk

from a large-scale toxic chemical release occurs when personnel are unable to escape the immediate area and are overcome by vapours or blast effects. Military respirators and personal protective equipment may provide limited protection against TICs. Shelter in-place is an alternative action if facilities are available and evacuation is impractical. Useful guidance on the hazards resulting from the release of a wide range of TICs and appropriate initial response can be found in the Emergency Response Guide (ERG) and Agreement on Dangerous Goods by Roads (Europe) – ADR. Allied Tactical Publication (ATP)-3.8.1 Volume I, provides a list of TICs of concern to commanders for the conduct of military operations.

b. Toxic Industrial Biological (TIB). TIB has the potential to produce significant environmental damage and result in pollution of water supplies, long-term ecological damage, and present a significant hazard to military operations. Possible sources of TIB include hospitals and other medical installations and research, production, storage or recycling facilities for the pharmaceutical or agricultural industries.

c. Toxic Industrial Radiological (TIR). Possible sources of TIR material capable of producing radioactive hazards are: civil nuclear production, research, recycling and storage facilities; waste containment sites; industrial and medical sources; materials and sources in transit; stolen or smuggled nuclear weapons grade material. The characteristics of radioactive hazards produced will depend on the type of radiation and the nuclide involved. The geographical area of spread of the hazards can vary dramatically according to the source and manner of release.

Chapter 3

Enabling Components of CBRN Defence

Section 1 – Introduction

0301. General

a. CBRN defence is divided into five enabling components. The foundations for these enabling components are established based on CBRN defence policy, doctrine, capabilities, procedures, organisations and training. The five enabling components are briefly summarized below and discussed in detail in the following sections of this chapter.

(1) Detection, Identification and Monitoring. This component detects and characterizes CBRN incidents, identifies the agents and hazards, delineates areas of contamination, and monitors the changes.

> The UK title for the Detection, Identification and Monitoring component of CBRN protection is Sense; this largely covers the same area, but it is both more inclusive and more closely aligned with wider intelligence, surveillance and reconnaissance (ISR) capabilities.

(2) Information Management. This component concerns the management of all forms of CBRN defence related information. The operational Communication and Information Systems (CIS) network is used to collect, process, store and disseminate CBRN defence data in order to: collate information about and assess threats and risks; plan the deployment of and manage detection, identification and monitoring systems; report incidents; predict hazards, identify and warn forces at risk; compile the CBRN contribution to the common operational picture; command and control CBRN units and assets; manage hazards; and, plan and manage physical protection, medical countermeasures and medical support.

> The UK title for the CBRN Information Management component of CBRN protection is CBRN knowledge management. This better reflects the content of the component and avoids confusion with the routine information management function carried out in all organisations for information exploitation. CBRN knowledge management includes a decision support function for Commanders and staff.

(3) Physical Protection. Individual protection and collective protection (COLPRO) are required so personnel can survive CBRN incidents and continue to operate in a CBRN hazard environment. Measures to protect facilities, aircraft, ships, vehicles and equipment are also included.

(4) Hazard Management. This component limits the impact of CBRN hazards. Hazard management is based on the principles of pre-hazard precautions, hazard control through avoidance, control of hazard spread, control and management of individual exposures, and decontamination.

(5) Medical Countermeasures and Support. This component serves to diminish the susceptibility of personnel to CBRN hazards and to determine if personnel have been exposed. The treatment and evacuation of casualties in a CBRN environment, whether contaminated or not, must be considered. The medical staffs are responsible for advising the commander on medical countermeasures and support.

b. Interoperability and compatibility through advancing technology will assist the five enabling components in ensuring a holistic approach to CBRN defence.

Section 2 – Detection, Identification and Monitoring

0302. Detection

a. Detection is the discovery by any means of the presence of CBRN substances. The equipment and techniques, tactics, and procedures needed to detect incidents and protect against them must be made ready and rehearsed at appropriate threat levels so that hazards can be detected at the earliest possible opportunity and timely alerts and/or alarms given.

(1) Detectors. A CBRN detector is a device or system, including the observation of living organisms, employed to recognize the emergence, presence or absence of CBRN hazards. Detectors are divided into:

(a) Point Detector. Detectors that react to hazards at the point of interception.

(b) Stand-Off Detector. Detectors that react to distant incidents or hazards.

(2) Detection Capability. Point and stand-off detectors may range from fully capable platform-mounted systems to man portable devices intended only for immediate indication of hazards. Whatever the design, they are only able to test the atmosphere, surface or suspect material at the point of sampling or at the limit of stand-off capability. Advance warning is thus achieved by placing the equipment upwind of the bulk of personnel at risk but downwind of the anticipated point of release. Inevitably, these criteria impose costs in terms of physical vulnerability, routine maintenance, periodic relocation and the numbers required. Use of these detectors may in fact not be possible in all operational scenarios. Point detectors and stand-off detectors can significantly improve the timeliness of hazard detection if used remotely. Commanders and staffs will need to make careful choices in the employment of detection equipment, balancing the full utilization of their inherent capabilities against limited numbers and restrictions on geographical dispersion.

(3) Biological Agent Detection by Disease Surveillance. In addition to the detection capability given above, biological agents can be detected through the systematic, large scale and regular health monitoring of joint force personnel and, where possible and applicable, the local civilian population. Changes in health patterns can be targeted and analyzed for the early signs and symptoms of disease or illness induced by biological agents.

b. Assessment of Detector Data. While some detection data will be clear and unambiguous, other indications of a CBRN release may be inconsistent or even contradictory. In the case of biological agents, there will be a need to assess the available information before translating an alarm into a command-endorsed warning. Within this process, detector outputs may be awarded a confidence level which is a measure of the credibility of the output from a detector or combination of detectors. Confidence levels are ordinarily expressed as one of three levels; indicative, presumptive and definitive.

c. In the case of biological detection and identification, it may be difficult to confirm that an incident has taken place. Since some biological agents occur naturally, a comparison of the quantity of agent found versus its natural abundance and the way of infection will be of vital importance in the assessment of a possible biological incident.

d. The CBRN detection component also includes the tasks of surveillance, reconnaissance and survey:

(1) Surveillance. Surveillance is the systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means for determining the presence or absence of CBRN hazards. The integration of detection reports via the Warning & Reporting (W&R) process, described below, facilitates early warning.

(2) Reconnaissance. Reconnaissance is a deliberate mission undertaken to obtain information by visual observation or other methods and/or confirm the presence or absence of CBRN hazards. It may include gathering information on adversary use of CBRN weapons or devices, associated hazards, or meteorological data for CBRN hazard prediction.

(3) Survey. Survey is a directed effort to determine the nature and degree of CBRN hazards in an area of confirmed or suspected contamination, and to delineate the boundaries of the hazard area. This may include monitoring the degree of radiation or the presence of a biological or chemical hazard, and the sampling of items suspected of CBRN contamination. It is likely to be carried out by specialist personnel using sensors and equipment designed for the task.

0303. Sampling and Identification

a. On the presumption of hostile (first) use of CBRN agents, or by discovery of suspected CBRN materials and/or a positive alarm of detectors, the JFC may order sampling teams to gather information and determinate the identity of the CBRN hazard in conjunction with specialized CBRN laboratories.

b. Sampling and identification are required:

(1) To allow strategic commands to support timely Alliance decisions in response to such CBRN incidents and to identify possible arms control treaty violations;

(2) To allow the JFC to make timely and informed decisions on the positioning, operating posture, hazard management, tempo and manoeuvre ability of the joint force;

(3) To enable the medical services to provide the most appropriate health care for casualties and determine the most appropriate protective actions to implement health protection for the joint force;

(4) To support further consequence management (CM), site decontamination and eventual recovery.

c. **Sampling**. Sampling is the retrieval for analysis of material known or suspected to have been employed in a CBRN incident, or of material suspected to have been contaminated in such an incident. Sampling needs to be conducted by trained personnel with specific equipment to warrant a considered choice of samples, uniformity, viability, safety, and accountability in the sampling procedures.

(1) **Field Sampling.** There may be a need for field sampling of potential contaminants for local and operational use. Depending on the situation, such an operation may require medical support for invasive medical specimen collection and/or explosive ordnance disposal (EOD) support and could also involve the use of deployable analytical laboratories (for confirmed identification) or home-based laboratories (for unambiguous identification). When possible, the application of the drills and procedures outlined in AEP-10 and AEP-49 is recommended.

(2) **Forensic Sampling.** For strategic purposes, there may also be a need for forensic sampling in order to identify CBRN hazards and to confirm, by forensically acceptable techniques, the unequivocal use of CBRN agents by an adversary. As the proof of use of CBRN agents must be such that it cannot be refuted, this degree of certainty cannot be achieved by information obtained solely from field sampling or

unusual numbers of casualties. In such a case, additional forensic support for securing crime scene evidence may be required. The application of the procedures as outlined in AEP-10 and AEP-49 is mandatory and the analysis can only be conducted in an accredited laboratory in order to meet international standards.

d. **Identification.** Identification is the determination of the identity of an agent or material. There are three types of identification with varying degrees of reliability; provisional, confirmed and unambiguous identification.

e. **Sampling and identification of biological, chemical and radiological agents (SIBCRA).** The term SIBCRA is used when referring to the process of collection, transportation and identification of suspected Chemical, Biological, Radiological materials within a chain of custody.

0304. Monitoring

Monitoring is the continuous or periodic process of determining whether a CBRN hazard is present or not. CBRN hazards can be significantly affected by a number of factors including weather, terrain, and time of day and agent decay. Monitoring is conducted on personnel, equipment, or terrain to establish the presence or not of contaminants and to validate decontamination. Monitoring assists the commander in determining the protective posture of the force.

Section 3 – CBRN Information Management

0305. General

a. CBRN defence is an integral component of the headquarters staff operational planning process. CBRN information management includes systematic information collection, the issuing of critical warning messages, exchange of CBRN information, reach back capacity, analysis, storage, exploitation and the provision of CBRN assessments and advice for the planning operations prior, during and after CBRN incidents. CBRN information management includes W&R.

b. The detailed organization of the CBRN defence, including subject matter experts at the different staff levels and CBRN information management procedures, should be included in the command SOPs and adjusted to fit the operational environment and specific mission/task assigned.

c. Effective command and control (C2) of the CBRN situation can only be maintained when CBRN information is an integrated part of the common operational picture (COP). It is essential that CBRN defence information, particularly critical issues such as safety matters and warning messages, is communicated rapidly both up and down the chain of command and horizontally with other units, agencies and civilian authorities in adjacent locations. Figure 3-1 depicts an example of the CBRN information flow between elements (including collection centres (CCs)) and bodies throughout the operation.

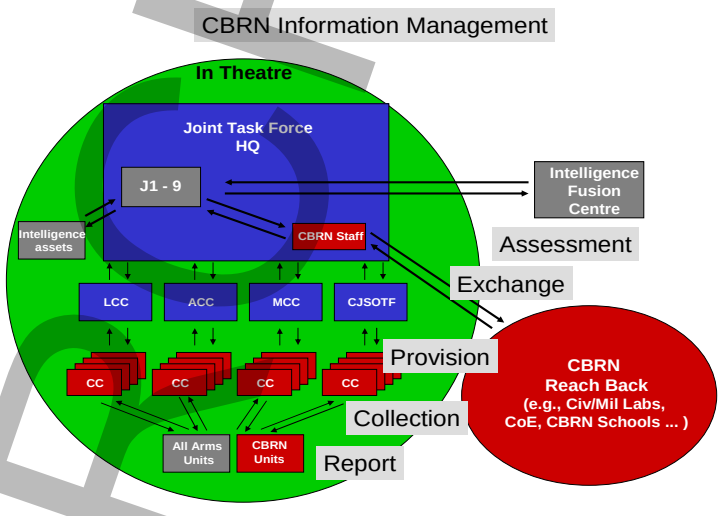


Figure 3-1 CBRN Information Flow

0306. CBRN Defence Staff and Collection Centres

a. CBRN defence staff should be fully integrated into the normal staff planning process at every level of command and across all operations. Their function is to provide CBRN specific advice to the commander to aid the decision making process and to lead in the production of CBRN IPOE which informs the joint operational picture. Each staff branch should have a member that has received appropriate CBRN defence training and education who can contribute to the production of contingency plans for CBRN incidents, participate in planning and assessments and address functional tasks.

b. CBRN W&R centres must be established at all levels of command. The CBRN W&R functions and responsibilities should not be confused with the normal chain of command or staff planning process.

0307. Communication and Information Systems

The operational Communication and Information Systems (CIS) network is used to collect, process, store and disseminate CBRN defence data in order to: collate information about and assess threats and risks; plan the deployment of and manage detection, identification and monitoring systems; report incidents; predict hazards, identify and warn forces at risk; compile the CBRN contribution to the common operational picture; command and control CBRN units and assets; manage hazards; and, plan and manage physical protection, medical countermeasures and medical support.

0308. Warning and Reporting

a. Commanders and staff at all levels need to assess the impact of CBRN incidents on their plans and decisions using timely, accurate and evaluated CBRN information. W&R is the process by which reports of CBRN incidents are forwarded through the chain of command, and units are warned of the resulting hazards and predicted hazard areas. The process is coordinated by a hierarchical structure of CBRN centres. This regime is described in ATP-3.8.1 Vol I and ATP-45, and detailed procedures are provided in ATP-45.

b. The purposes of CBRN W&R are:

(1) Reporting and exchanging of information on all CBRN incidents.

(2) Predicting and warning of hazard areas from CBRN incidents.

(3) Evaluation of CBRN information so that an assessment can be made of the influence of CBRN incidents on operations.

(4) Exchange of CBRN information between the components of the joint force and national military and civil authorities and agencies.

c. A CBRN alarm is an indication from any source that a CBRN incident may have occurred. The alarm should be passed across the joint force in a timely and accurate manner so that appropriate protective measures can be taken. Alarms passed using CIS should use the procedures in ATP-45. Alarm functions must be capable of being set and reset to take account of subsequent changes in the level of CBRN risk.

INTENTIONALLY BLANK

Section 4 – Physical Protection

0309. General

Physical protection enhances survivability, but can reduce operational capability. Commanders must reconcile the vulnerability of the joint force to CBRN hazards with the restrictions imposed by the use of protective measures and the need to pursue the mission. Physical protection consists of:

a. Individual Protection. Individual protection is protection provided to an individual in a CBRN environment by protective clothing and/or personal equipment.

b. Collective Protection. COLPRO is afforded by facilities or systems equipped with air filtration devices and air locks which provide personnel with a CBRN hazard-free environment for performing critical work and obtaining rest and relief in order to sustain combat operations.

c. Equipment and Materiel Protection. Equipment and materiel protection is protection of mission-essential equipment and materiel from contamination, thus reducing equipment damage, spread of contamination and the need for subsequent decontamination. All mission-essential land, maritime and air platforms and equipment, that risk becoming contaminated, need to be covered and concealed, dispersed, or otherwise protected.

0310. Physical Protection - Risk Assessment

The purpose of risk assessment for the physical protection enabling component is to determine the defensive posture, to reduce degradation and to improve operational efficiency. The risks involved will change with time and will need to be reviewed regularly. The factors that must be considered are discussed below.

a. CBRN Threat. Responsibility for establishing CBRN threat levels rests with the commander based on advice provided by the intelligence staff and CBRN defence specialists. Local commanders typically have the authority to determine the appropriate degree of CBRN physical protection, based on their assessment of local conditions, the associated protective measures necessary, and the operational imperatives of the local situation. The assessment of the threat should not be limited to conventional methods of disseminating classical agents. Asymmetric dissemination methods and the release of TIM should be assessed as well.

b. Operational Task. The priority and urgency afforded to the operational task and an assessment of the risk both need to be considered to ensure that over-protection does not hinder effective and timely completion of the

mission. In particular, greater risks are typically accepted in combat operations than in peace support operations.

c. Location of Personnel. While the disposition of personnel will affect their chances of being targeted with CBRN weapons or devices, the physical protection afforded by their location will influence their vulnerability. Personnel under cover and unlikely to be exposed to surface contamination may not need to wear CBRN foot protection or gloves, while those in COLPRO will not necessarily need to wear individual protective equipment (IPE).

d. Weather Conditions. Temperature and weather are crucial factors that influence the degree of thermal stress imposed by wearing IPE. Weather conditions can also affect the likelihood and duration of any CBRN incident.

e. Nature of Work Undertaken. The physical effort involved in conducting any task has a direct effect on the level of degradation caused by IPE. If a heavy workload is combined with high temperatures there will be a risk of heat stress casualties, particularly if there is insufficient water intake.

f. Protection of Vital CIS. Information and decision superiority are so fundamental to the success of any operation that the users of vital CIS services, the system operators, maintainers and the equipment are afforded, as a pre-hazard precaution, the degree of physical protection appropriate to their functions.

0311. Individual Protection

a. All individuals in a hazard area should be provided with an individual respiratory protection system (respirator or mask), prophylaxis/pre-treatment medications, antidotes, an individual decontamination kit, a first aid kit and protective clothing. Commanders need to be aware that there may be limitations on the effectiveness of existing IPE and respirators against certain threats, including many TIMs. The risk of exposure of personnel to CBRN hazards needs to be continuously monitored and the necessary medical records updated, so support and aftercare can be arranged. IPE is not usually designed to protect against TIMs, but may improve the users' ability to escape from a TIM release. Impermeable clothing and self-contained breathing apparatus may be available and provide better protection for CBRN defence specialists against the majority of hazards.

b. Commanders should consider the effects of wearing IPE on the performance of individuals such as dehydration, restricted vision and less effective communications. The physiological and psychological effects of wearing IPE can affect the maximum continuous time that an individual can be reasonably

expected to work in any type of operational environment. In most instances, work/rest cycles must be set up to maximize combat effectiveness.

c. IPE has a limited protective lifetime particularly if worn frequently in operations. Commanders must ensure their personnel have adequate protection. Re-supply of IPE should be based on usage. The scaling of IPE stock levels is one of the major issues to be addressed in the CBRN defence risk analysis. In areas of reduced threat, lower levels of stocking may be acceptable. Damaged or torn IPE should be routinely replaced, and commanders must ensure that the IPE in use by personnel retains its protective capabilities.

d. Ideally personnel will get sufficient warning of attack to adopt an appropriate dress state before arrival of the agent. This will ensure that IPE always provides appropriate protection and any wear is compensated for as soon as possible after an incident.

e. It is important to consider the IPE as a total ensemble, and not as individual elements. Mask filters and coveralls are usually the items that need replacing most often, but hand protection, to include liners, also get considerable wear. Sizing of replacement equipment is also vital, as ill-fitting IPE will not provide optimum protection. Requests for CBRN defence re-supply should specify the sizes necessary, and specifically any non-standard sizes.

f. Commanders shall ensure that NATO forces only operate in a TIM contaminated area when essential for the operation. In this instance, professional assessment by industrial hygienists, toxicologists, and occupational and/or environmental specialists of the actual and potential exposure can ensure reasonable exposure guidelines and appropriate use of protective equipment. Such assessments normally will only be available via reach back.

0312. Collective Protection

a. Protection against CBRN hazards via the use of IPE alone may result in unacceptable performance degradation and may allow an adversary to shape the battlespace to his advantage. COLPRO systems offer a means of balancing the need for protection against the requirement to maintain tempo. The purpose of COLPRO is to allow the continued performance of operational functions without the psychological and physiological effects that result from the extended use of IPE. COLPRO provides adequate protection against airborne CBRN hazards and may also, depending on design and placing, resist some forms of surface contamination. However, commanders need to be aware that:

(1) Limited biological detection capability may prevent the accurate assessment of biological agent contamination of individuals and thus impose limitations on entry into COLPRO after the arrival of a hazard. This risk will be particularly pronounced in cases where transmissible agents are employed as COLPRO may act as a focus for secondary infection;

(2) In the presence of immediate or deposited radiation hazards, the protection afforded by the COLPRO will be conditioned by the density of the surrounding platform or structure; and

(3) COLPRO filters may not be effective against high concentrations of agents which displace oxygen and may provide only limited protection against some TIM compounds.

b. In general, the use of COLPRO is based on the principles below.

(1) Hazard avoidance. The underlying principle remains hazard avoidance. If it is possible to avoid the hazard by moving then moving is the best option. COLPRO is always the second choice.

(2) Priorities. There will be many competing demands for COLPRO. The operational plan must establish priorities for the allocation of COLPRO resources.

(3) Security. COLPRO facilities should be provided in locations that are protected from direct and indirect hostile fire, and from civil intrusion. It will be impossible for personnel in the facility to defend themselves, so security must be provided. In particular, air or artillery attacks could rupture the protective membrane or damage the facility and put all occupants at risk. Local protection, including air defence is a key consideration.

(4) Entrance/Exit. Personnel entering any COLPRO facility must go through a ‘decontamination line’ or contamination control area (CCA), and leave their outer clothing and personal equipment in a secure storage area. The COLPRO of medical/surgical facilities presents a special case, as casualties must go through the CCA.

(5) Operating Personnel. The operation of any COLPRO facility will present a significant personnel bill. ‘Commanders should consider that, as the number of personnel required to enter or leave a COLPRO facility is reduced, then so is both the number of personnel required to operate it and the chance of inadvertent contamination. Dedicated operating staff will be required for high traffic COLPRO

shelters. These individuals operate the air handling facilities, change filters and provide dressing, showering and monitoring assistance.

(6) Contamination. Continual use of a COLPRO facility could eventually lead to it becoming contaminated. Continuous monitoring will be necessary throughout the facility, and rapid and effective plans needs to be available to avoid contamination or breaches of the toxic free area.

(7) Decontamination and COLPRO. Decontamination and COLPRO are complementary functions. In many cases, the tactical choice is either decontaminate, or provide COLPRO to allow the personnel to continue to operate in a contaminated area. The COLPRO plan must support the decontamination plan, and vice versa.

c. Collective Protection Categories. The fundamental purpose of all CBRN COLPRO systems is to enable occupants to maintain maximum operational efficiency in a CBRN environment. This objective may be satisfied by the selective employment of the following categories of CBRN COLPRO.

(1) Fixed. These are COLPRO systems integral to static facilities and may be hardened, semi-hardened or unhardened in specially built or adapted facilities.

(2) Mobile. These are COLPRO systems integral to land, maritime or air platforms. They may or may not be capable of operation on the move or of allowing entry and exit in the face of chemical, biological or radioactive hazards. The ‘citadel’ on board a ship is a type of mobile COLPRO and comprises a group of interconnecting compartments which can be protected inside a vapour tight boundary within which clean air can be circulated.

(3) Transportable. These are stand-alone COLPRO systems capable of being deployed into an area of operations. They will usually be unhardened but may be capable of erection within buildings or other enclosures. Transportable COLPRO can also be used within ships which do not have citadels.

(4) Hybrid. Hybrid COLPRO systems are internally mounted systems designed to provide augmented filtration and/or airflow to individuals operating or occupying aircraft or vehicles. These systems are designed to provide either enhanced respiratory protection to individuals by increasing the protection factor or to provide increased airflow to individuals who have been, or are required to sustain moderate to high levels of physical activity.

0313. Equipment and Materiel Protection

a. In addition to those protective general measures detailed earlier, platforms and equipment need to be designed so that once contaminated they can be operated by crews dressed in full IPE with only minimal (operational) surfaces requiring decontamination to continue the mission.

b. The survivability of equipment against the effects of CBRN weapons and devices should be enhanced through the effective use of mitigation techniques or 'good practices' identified in the following paragraphs.

(1) CBRN Contamination. The contamination and penetration of equipment surfaces can be avoided or reduced by the protection provided by buildings, use of chemically resistant materials or any appropriate cover, and closure of all doors, windows and hatches.

(2) Nuclear Electromagnetic Pulse and Transient Radiation Effects on Electronics. Penetration by EMP into equipment and TREE can be minimized if all enclosures are kept shut, cable runs are as short as possible and not elevated, unused equipment is switched off and disconnected, and any unauthorized electrical modifications removed.

Section 5 – Hazard Management

0314. General

a. Hazard management includes measures to limit the operational impact of CBRN incidents. Hazard management is based on the principles of pre-hazard precautions and hazard control through avoidance, control of spread, exposure control and decontamination. Once personnel or their equipment, vehicles or stores come into contact with hazards, IPE may need to be worn for a prolonged period. Wearing IPE degrades operational performance so its wear should be kept to a minimum, both in terms of the amount of equipment worn and duration. The principal means of countering these difficulties is to avoid hazards and the risk of becoming contaminated. If decontamination does become necessary, it needs to be undertaken as soon as other operational priorities allow. Hazard management needs to be an integral part of all operational planning and, as much as possible, be prepared for well in advance.

b. Types of Contamination. Contamination is the deposit, or adsorption or absorption of radioactive material, or of biological or chemical agents on or by structures, areas, personnel or objects. Any activity within a contaminated area which causes particles or liquid to be disturbed will cause a secondary hazard as they are carried away by the wind or in running water. Most decontamination waste products will form a secondary toxic hazard. Consequently, the following types of contamination resulting from a CBRN incident may be encountered .

(1) Surface. Surfaces contaminated by liquid or solid hazards.

(2) Air. Air contaminated by vapour, or liquid or solid aerosols.

(3) Water. Water contaminated by liquid or solid hazard.

0315. Pre-Hazard Precautions

Pre-hazard precautions can greatly reduce the possibility of forces being targeted by CBRN weapons and devices and, should CBRN incidents occur, can minimize the effects of CBRN agents. These measures need to be considered and prepared for during the operational planning process and, if the threat warrants, implemented before the incident occurs. Pre-hazard precautions are discussed in the following paragraphs.

a. Use of Cover. Hardened shelters, buildings and ships' citadels provide the best cover against all forms of hazard but any type of overhead cover provided by an impermeable material is worthwhile. Failing this, tarpaulins, ground sheets and even camouflage nets may reduce contamination.

b. Camouflage, Concealment, Dispersion, Deception. The strict application of camouflage, concealment, dispersion, and deception techniques will do much to avoid discovery and potential targeting of the joint force.

c. Pre-Wetting for Ships. Pre-wet is the fitted water spray system which enables a ship to wet and wash down all upper deck surfaces as a means of protection from CBRN contaminants. This reduces residual contamination.

d. Overpressure. Navy units and military vehicles may have a system which allows creation of a hyperbaric pressure within the unit thereby preventing ingress of particles, liquids or gases.

e. Redundancy. The impact of CBRN hazards on a force can be minimized if a degree of redundancy can be planned. This principle can operate at all levels.

f. Avoidance. Whenever possible, position critical assets outside the threat ring of CBRN-capable delivery systems.

0316. Hazard Control

a. The most effective hazard control measure is to avoid hazards and the risk of becoming contaminated; this will obviate or forestall the need for any other measures. However, this may not be easy to achieve because operational demands may result in the unavoidable exposure of forces.

b. **Hazard Avoidance**. Hazard avoidance measures are discussed in the following paragraphs.

(1) Marking. Stores, equipment and areas of ground that are known to be contaminated need to be marked so they can be avoided.

(2) Movement Control. Movement control measures are needed to prevent forces from moving into contaminated areas.

(3) Route Planning. Informed route planning can reduce the danger of picking up contamination in transit.

(4) Relocation. Forces in a CBRN hazard area need, where possible, to move away from the hazard.

c. **Control of Spread**. Methods to control the spread of contamination are discussed in the following paragraphs.

(1) Limitation of Spread. Limitation of spread involves the close control of movement around, into, within and from a hazard area after a CBRN

incident. Movement plans need to balance operational priorities and CBRN penalties using advice from operational and CBRN defence staffs. When biological hazards are identified, troop movement measures need to be considered to prevent possible cross-infection.

(2) Hazard Containment. Every effort is needed to physically contain CBRN hazards so that they do not spread to uncontaminated areas and pose a risk to unprepared forces. Physical containment may also be necessary to control the spread of CBRN hazards from leaking munitions, improvised devices or industrial facilities. Measures may be permanent, temporary or expedient.

(3) Waste Management. Contaminated or infectious materials, including runoff from decontamination, need to be contained and marked to await subsequent disposal.

d. **Exposure Management.** The management of exposure to hazards is exercised by:

(1) Exposure Control. The exposure of personnel to CBRN hazards needs to be kept as low as reasonably achievable subject to risk assessment including operational imperatives.

(2) Management of CBRN Hazard Data. An accurate record of CBRN information needs to be maintained for CBRN incidents. This is to assist operational planning, to avoid friendly forces inadvertently encountering a hazard area and for post-conflict remediation. Full details of exposure must be documented in personnel medical records to ensure post-event medical evaluation, treatment, and long-term monitoring. Similarly, equipment and vehicle maintenance records must be annotated.

(3) Rotation of Assets. The rotation of force assets through a CBRN hazard area needs to be considered and planned. This is so that the degradation of personnel performance caused by high levels of CBRN physical protection is minimized and exposure to CBRN hazards is kept as low as possible throughout the force. There is a particular need to rotate personnel through hazard areas because exposure may accumulate with time.

0317. Decontamination

If pre-hazard precautions and control measures are not effective, or exposure is unavoidable, decontamination may be necessary. Decontamination is the process of making personnel, objects or areas safe by absorbing, destroying, neutralizing, making harmless, or removing chemical or biological agents and radioactive material.

The UK disagrees with the NATO definition of decontamination detailed at paragraph 0317 because decontamination does not make any area, person or object safe, it merely reduces the risk posed by a hazard. The UK defines decontamination as:

> The process of absorbing, destroying, neutralizing, removing or otherwise making harmless chemical or biological agents, or removing radioactive material.

a. **Principles of decontamination**. The following principles of decontamination must be recognized:

(1) As soon as possible;

(2) Only what is necessary or based on operational requirements;

(3) As close to the contamination as possible; and

(4) Prioritization.

b. Decontamination may be passive or active, reflecting the urgency of the operational and/or tactical situation. The types of decontamination are discussed in the following paragraphs.

(1) Passive Decontamination. Also called 'Natural Decontamination' or 'Weathering'. Passive decontamination is decontamination effected by natural processes of decay, without benefit of human or mechanical intervention. Although weathering is a time consuming process, it carries minimal manpower and logistic costs. Its efficiency depends on weather conditions which have to be taken into account. Assets left for passive decontamination must be isolated and marked as a hazard.

(2) Active Decontamination. Active decontamination is the employment of chemical, biological or mechanical processes to remove or neutralize chemical, biological or radioactive materials. Active decontamination is conducted when contamination will adversely affect the operational capabilities of the joint force. There are three levels of active decontamination employed by operational forces: immediate, operational and thorough decontamination.

c. **Clearance Decontamination**. Decontamination of equipment and/or personnel on temporary or permanent removal from an operation to a standard sufficient to allow unrestricted transportation, maintenance, employment and disposal. Clearance decontamination will generally occur at the completion of a mission or when transfer of authority has occurred and will be conducted according to national arrangements.

The UK disagrees with the definition of Clearance Decontamination given at paragraph 0317c and recognises that a form of clearance decontamination is likely to be required throughout any operation. The UK definition of clearance decontamination is:

> Decontamination performed on personnel, equipment, materiel and terrain (including infrastructure) with the primary aim of enabling unrestricted use, handling, operation, and release from military control of contaminated items, subject to the approval of national civilian authorities. Where there is a requirement for repatriation or for the temporary or permanent removal of equipment and/or personnel from an operation, clearance decontamination must be conducted to a standard sufficient to allow, with additional safety measures where required, transportation or disposal.

AJP 3.8 does not include the definitions for immediate, operational or thorough decontamination as these are contained in AAP 6 and AAP 21(B). However, the UK disagrees with these definitions and it is, therefore, worthwhile including them in this high level doctrine. The UK definitions are as follows:

> **Immediate decontamination**. Decontamination performed on individuals, irrespective of dress state, with the primary aim of saving life. This may include decontamination of personal clothing and/or personal equipment.
>
> **Operational decontamination**. Decontamination performed on specific parts of operationally essential equipment, operationally essential materiel, limited terrain (including infrastructure) and individuals wearing individual protective equipment (IPE) with the primary aim of sustaining operations in a CBRN contaminated environment. The minimizing of contact and transfer hazards is a priority so as to reduce the challenge to IPE and limit the spread of contamination.
>
> **Thorough decontamination.** Decontamination performed on personnel, equipment, materiel and terrain (including infrastructure) with the primary aim of restoring normal operational tempo by removing the need for personnel to wear CBRN individual protective equipment (IPE).

Section 6 – Medical Countermeasures and Support

0318. Medical Countermeasures and Pre-Treatments

a. Medical countermeasures and pre-treatments are designed to diminish the susceptibility of personnel to CBRN hazards.

b. Commanders and staffs need to make decisions, on advice from the medical staff, about the timely and appropriate administration of prophylactic or preventive compounds (immunization, medication) as well as other pre-treatment measures (skin barrier sprays or repellents). These countermeasures and pre-treatments must to be issued to personnel under national guidelines.

c. The use of countermeasures to mitigate the effects of CBRN hazards include:

(1) The scrupulous application of field hygiene measures during operations;

(2) Specific prophylaxis/ pre-treatment against assessed threat agents in advance of a possible attack;

(3) Post-event exposure screening to determine if medical intervention is warranted;

(4) Post-exposure vaccination, with or without the simultaneous use of antibiotics;

(5) Restriction of movement and surveillance of possible direct and indirect victims of transmissible agents, to include disinfecting of exposed body surfaces.

0319. Medical Support in CBRN Environments

a. One of the most difficult challenges faced by a medical planning staff is defining requirements for adequate force protection and the medical management of casualties in a CBRN environment. Coordinating an effective response requires access to the full spectrum of military and emergency management resources, the marshalling of most of NATO's military medical resources, and support from the medical systems of host nations (HNs).

b. **Situational Awareness (SA) and C2**. The medical planning staff has the following specific responsibilities that support effective SA and C2:

(1) Evaluate the medical intelligence available and advise the commander and his staff on the potential CBRN health implications of the operating environment;

(2) Prepare the medical risk assessment to support the overall operational risk assessment; and

(3) Support the W&R of potential and actual CBRN incidents and hazards into command and control systems to minimize the health effects of toxic or incapacitating exposure to deployed forces.

c. **Force Health Protection Planning**. When considering force health protection medical planners must consult with J2 medical intelligence services to determine likely CBRN hazards and ensure appropriate pre-treatments and countermeasures are made available.

d. **Casualty Management**. Casualty management refers to a group of post-incident medical capabilities that are applied to preserve the health of the force, to deliver optimal care to casualties, and to maximize the rate at which casualties return to duty. In the aftermath of a CBRN incident, the number of casualties may far exceed the capacity of the medical treatment system. The medical planning staff must develop a plan for managing a substantial increase in casualty flow and the demand for treatment. The plan must address handling and movement of CBRN casualties, avoiding contamination spread, and treating infectious diseases. CBRN casualty care requires extensive coordination and negotiation with the hospitals of contributing nations and HN.

e. **Casualty Evacuation**. The medical evacuation of casualties is the controlled process of moving any person who is wounded, injured, or ill to and/or between medical treatment facilities. Patients or personnel known or suspected to be contaminated with CBRN agents will not normally be moved within the aeromedical evacuation system prior to being decontaminated. In rare cases, movement may be essential to preserve life, limb or eyesight or to maintain operational capabilities and on these occasions every effort must be made to prevent the spread of contamination during movement.

Note: To prevent the spread of transmissible disease, aeromedical evacuation of contagious and contaminated casualties may require the approval of the JFC and national authorities.

f. **Sustainment of Medical Operations**. The medical system has a responsibility to provide patients with appropriate, effective, and timely care. The proper planning and management of medical supplies, waste, contamination, and facility operations will facilitate the sustainment of medical operations to provide continuity of care.

Chapter 4

Command Considerations for Planning and Conduct of CBRN Defence

Section 1 – Introduction

0401. General

a. The joint force's operational planning must consider a potential adversary's employment of CBRN weapons / devices or the occurrence of other CBRN hazards. In particular, campaign and supporting plans must include options for producing acceptable and timely force capabilities (including force protection) to counter the possibility of early adversary CBRN employment in the JOA or other supporting areas. There is no single doctrine for multinational action, and each alliance or coalition develops its own protocols and operation plans (OPLANs).

b. The JFC should anticipate and incorporate planning factors such as HN, national and international laws to ensure compliance. They also establish priority intelligence requirements, take pre-crisis actions to prevent adversary employment of CBRN weapons and devices, plan counterforce and active defence operations to prevent or minimize CBRN attacks, plan actions to help deter adversary CBRN employment, and counter, mitigate and manage the effects of CBRN incidents.

c. With host countries, coalition partners, and other governmental and nongovernmental agencies in the JOA, particular emphasis should be placed on early warning and detection and exchange of SOPs as well as actions to protect friendly military forces, threatened civilian populations and essential infrastructure.

Section 2 – Key CBRN Defence Planning Considerations

0402. Operational and CBRN Defence Priorities

The JFC provides guidance to subordinate commanders on the balance between operational priorities and avoidance of CBRN hazards both within his 'Statement of Intent' or “Commander’s Intent” and as guidance in the campaign plan. Application of policy to minimize the exposure of personnel to CBRN hazards must be coordinated between the different national components, the HN and other in-theatre agencies including, but not limited to, non-governmental organizations (NGOs).

0403. Extension of CBRN Defence and CBRN Consequence Management (CM)

NATO forces may also be tasked to support civil authorities in situations where a deliberate or unintentional release of a CBRN substance has occurred. The joint force may be required to render technical support to identify, assess, transfer, and dispose of a contaminant or conduct decontamination operations. The requirement to carry out CBRN CM is likely to be as the result of specific tasking from the strategic level, and will therefore be a mission in its own right. Annex D, “Consequence Management,” provides a number of additional considerations for planning and executing CBRN CM to supplement those given in this chapter.

0404. Joint Staff Responsibilities for CBRN Defence

CBRN defence planning requires extensive coordination across the entire staff to provide the JFC with relevant options to respond to potential CBRN incidents in a timely and effective manner. The entire staff has a responsibility for ensuring their area of expertise is properly organized and prepared to meet JFC’s objectives in operations in a CBRN contaminated environment. The CBRN defence staff must then collate the combined JFC staff output to produce a coherent CBRN defence annex for the OPLAN.

a. The following is a list of potential joint staff functions when a risk of operating in a CBRN environment exists:

(1) Personnel. Procedures for dealing with mass fatalities and contaminated remains are particularly sensitive and will require guidance from the strategic level. Establishing acceptable levels of decontamination will be critical and may complicate the disposition of contaminated human remains. An approved plan covering procedures for initial disposition and burial of contaminated human remains and mass fatalities in a CBRN environment needs to be in place and should be applicable to all levels of command and staff, HN and joint force national participants. Once strategic guidance and constraints are given, these need to be codified in all planning and execution documents and refined as the situation dictates. Coordination with medical, logistics and operations planners is vital. Personnel must also

ensure that procedures are in place to record individuals' exposure to CBRN substances once this has been highlighted to the commander by the medical staff. Such information must remain part of individuals' personnel records both during and after their period of service.

(2) Intelligence. Intelligence staff must provide accurate, timely and relevant intelligence on the possible CBRN threat, to meet the JFC's operational and force protection (FP) needs. Within the CBRN defence staff, this will need to be combined with medical information, including the location of environmental and industrial hazards, to establish a comprehensive view of the CBRN situation as a subset of the wider force protection picture. Intelligence staff may need to draw on expertise from within the CBRN defence staff to ensure that the significance of scientific or technical information derived from intelligence sources is fully appreciated.

(3) Operations and Planning. CBRN defence expertise will typically be located within the FP staff of a headquarters, and will be responsible for providing CBRN defence to ongoing operations. However, as the main source of CBRN expertise, the staff in this area will have a key role to play to ensure that due account is taken of CBRN aspects in planned operations and contingency planning. When included as part of a deployed joint task force (JTF), CBRN defence specialist assets such as CBRN reconnaissance and decontamination units and biological surveillance and sampling units, are coordinated by the CBRN defence staff and are assigned for employment across the JOA. These assets may be a mix of military and civilian agencies from different nations that have various specialized capabilities and will require careful coordination by the CBRN defence staff to achieve optimum effect. In addition to the wider role of providing CBRN expertise to the commander and staff, the CBRN defence staff will typically have the following responsibilities within current operations:

(a) Coordinate with all staff to ensure an accurate COP of the JOA, including possible or actual CBRN hazards that may or will be encountered.

(b) Carry out hazard prediction and W&R of CBRN incidents accurately and in a timely and consistent manner in accordance with the procedures in ATP-45, to ensure that commanders at all levels can quickly carry out measures to mitigate the effects of CBRN incidents.

(4) Logistics. Operations in a CBRN environment place significant demands on the logistics chain both in terms of CBRN equipment and consumables such as water. Logistics staff must work closely with

CBRN defence staff to establish and maintain sustainability plans both supplies and equipment in the event of a CBRN incident. These will need to reflect the likely threat or hazard and the commander's intent for maintaining operations in a CBRN environment. Logistics staff must also consider the following:

(a) Provide logistic assessment to operations of impact on ability to support the force and mission, if major logistic centres or lines of communication are contaminated.

(b) Monitor and advise staff and commander on changes in status, availability and capacity of airport of debarkation and seaport of debarkation in the JOA, if part or all of them are attacked and subsequently sustain CBRN contamination.

(5) Engineering. The task force engineers can provide resources such as EOD capabilities, the construction and maintenance of expedient facilities for decontamination sites and COLPRO.

(6) CIS. The CIS staff via the CIS network will collate information about and assess threats and risks; plan the deployment of and manage detection, identification and monitoring systems; report incidents; predict hazards, identify and warn forces at risk; compile the CBRN contribution to the common operational picture; command and control CBRN units and assets; manage hazards; and, plan and manage physical protection, medical countermeasures and medical support.

(7) Training. The commander has responsibility for ensuring that all members of the joint force (which may include certain civilians) are trained to survive in a CBRN environment. Training staff must therefore ensure that the correct training package, as determined by CBRN defence staff, is undertaken by all members of the joint force operating in the JOA.

(8) Legal. Legal staff will advise commanders and staff regarding applicable HN, TCN and international law.

(9) Medical. The role of medical staff is particularly important, as initial indication of a CBRN incident, especially of biological incidents, may come from the medical chain. The medical staff has key responsibilities in CBRN defence as follows:

(a) Develop, coordinate and execute timely and appropriate administration of prophylactic or preventive medical pre-treatment measures to counter effects of possible CBRN hazards; in compliance with the given operational priorities and established

international and national guidelines because these will vary between the different joint force components;

(b) Provide medical surveillance activities for the JTF;

(c) Provide consultation, selection and treatment for casualties and responders;

(d) Augment existing medical treatment facilities in accordance with status-of-forces agreements;

(e) Assist medical administration and management during an incident;

(f) Collect medical specimens as required for laboratory analysis and identification;

(g) Transport and track patients;

(h) Distribute medical supplies;

(i) Manage stress;

(j) Ensure casualties are decontaminated before entering medical treatment facilities where possible;

(k) Ensure that individuals' exposure or potential exposure to CBRN substances is highlighted to the Commander and subsequently recorded by medical staff on personnel records.

(10) Civil Military Cooperation (CIMIC). The CIMIC staff is responsible for advising the JFC on the implications of all CBRN defence activities which directly concern relations between the joint force and local government, civil population, international organisations, NGOs, and other agencies in the JOA. Local civilian authorities have prime responsibility for dealing with CBRN incidents within their areas of responsibility but, if their resources are inadequate, they may request assistance. Similarly, the joint force may request support from civilian authorities before, during and after a CBRN incident. Annex D, "Consequence Management", provides guidance to commanders and staff on factors for consideration if they are tasked with a CM mission.

(11) Public Information. The public information staff is responsible for advising the JFC on what public information is required regarding CBRN defence in the JOA. This needs to be co-ordinated with the relevant strategic-level staff and with representatives from joint force

components. Forces responding to a CBRN incident need to be prepared to handle requests for information from the international and local media, the public and joint force personnel. Therefore, public information and media operations staff need to be provided with accurate and timely information about CBRN incidents from commanders and staff at all levels. In addition, the public information staff must be prepared to respond to information and/or misinformation that may be promulgated through the Internet or social media sites.

In UK headquarters organisations, some of the distinct functions identified in Section 2 (such as civil-military cooperation (CIMIC)) are carried out by groups within the Operations *and* Planning staff. However, the planning considerations given for these functions are still valid.

b. These summarized joint staff responsibilities provide general guidelines for the commander to consider if an operation in a CBRN environment or CBRN defence is needed in the JOA. These CBRN defence operations require a high-level of international, intergovernmental, and interagency coordination and activity. The complex nature of the operations and coordination needed during and after a CBRN incident in the JOA requires continual liaison and sharing of information between the joint force, coalition nations, intergovernmental organizations, NGOs, regional security, and HN entities.

Section 3 – Conduct of CBRN Defence

0405. Introduction

a. This section provides a guide to the subjects that may need to be included in CBRN SOPs. The joint force CBRN defence SOPs must be prepared during pre-deployment. Once deployed, the joint force must exercise, train, validate and adjust, if necessary, these SOPs to meet the conditions encountered in-theatre. A check must also be made to ensure that general operating procedures are workable in a CBRN environment.

b. There are three distinct phases of a CBRN incident as it relates to CBRN defence. These phases are discussed in the following paragraphs.

(1) Pre-incident. These activities are critical because they will increase the unit's survivability and maintain the commander's freedom of action to the greatest possible extent. Pre-incident actions are essentially contingent measures and are the result of the CBRN risk and threat assessment as well as the CBRN IPOE. During this phase, measures and equipment are planned, prepared, tested, and, if necessary for some measures, implemented.

(2) During-incident. These activities are the implementation of contingent measures in response to a CBRN incident. These measures are directed mainly at ensuring that assets are suitably protected immediately on warning of and during an incident and minimizing the decontamination burden. These include the avoidance of contamination, the relocation of units, the use of COLPRO systems, the wearing of IPE, and immediate decontamination procedures.

(3) Post-incident. These activities follow a CBRN incident and are essential to protect assets, restore operational capabilities and regain operating tempo. These measures will be performed to reduce the required level of protection and minimize the spread of contamination. These will include the operations necessary to determine the location, type and extent of the contamination, movement control to limit the spread of contamination, and decontamination operations.

0406. Pre-Incident Activities

a. Specific pre-incident preparations and activities are covered below. Pre-incident actions include the use of cover, camouflage, concealment and dispersion of the joint force to avoid CBRN hazards.

b. Specific subjects that may need to be included in SOPs are the following:

(1) CBRN defence equipment;

(2) Electronic/sensitive equipment protection;

(3) Pre-hazard precautions;

(4) CBRN risk levels and protective measures;

(5) Detection;

(6) Information Management, and establishment of a supporting CBRN CIS network;

(7) Medical protection;

(8) COLPRO.

0407. During-Incident Actions

The equipment and procedures necessary for the protection of the joint force during a CBRN incident need to be made ready and exercised in the pre-incident phase. This paragraph is concerned with the immediate response to a CBRN incident, including initial detection, warning and the implementing of individual protection and COLPRO. Specific subjects that may need to be included in SOPs are the following:

a. Emergency alarms of hazard or attack;

b. Individual physical protection;

c. Downwind hazard warning;

d. Medical evacuation;

e. Immediate flash reporting;

f. Information Management.

0408. Post-Incident Actions

This paragraph is concerned with the post-incident measures necessary to limit the impact of CBRN incidents on operations. The procedures, equipment and training necessary for effective CBRN W&R, recovery and control measures, hazard management and medical countermeasures and support need to be prepared and practised in the pre-incident phase. Specific subjects that may need to be included in SOPs are the following:

a. CBRN W&R;

b. Detection and identification;

c. CBRN reconnaissance, survey and monitoring;

d. Health surveillance;

e. Medical support;

f. Casualty management;

g. Hazard management;

h. Decontamination;

i. Post-incident recovery;

j. Public information.

INTENTIONALLY BLANK

Annex A - Factors for CBRN Intelligence Preparation of the Operational Environment

Section 1 – Intelligence Preparation of the Operational Environment

A01. This annex provides a guide to actions the CBRN defence staff must take, in conjunction with the intelligence staff, to carry out the CBRN IPOE. The CBRN defence staff participates in planning to prevent CBRN threats from affecting friendly troops or local populations or creating environmental catastrophes including planning of targeting. The IPOE process is the staff tool that helps identify and answer the commander's priority intelligence requirements and is the first step in the JFC's operational planning process. IPOE is a continuous process that identifies confirmed and potential adversary capabilities, plans, and actions. IPOE should include an analysis of the capabilities and limitations of adversary CBRN weapons and delivery systems; their command, control, and release procedures; and the indicators of intent to employ CBRN weapons. IPOE includes:

a. Threat and hazard evaluation;

b. Area of operations evaluation;

c. Terrain analysis;

d. Meteorological evaluation.

A02. Threat and Hazard Evaluation. The CBRN defence staff must assess the vulnerability of the joint force to CBRN hazards by conducting the following:

a. Threat Evaluation. Evaluate the composition, disposition, capability and intent of an adversary.

b. Vulnerability Assessment. Vulnerability needs to be assessed against CBRN weapons or devices:

(1) Determine if the adversary has a capability by examining industrial and military infrastructure, access to precursor agents, potential storage and dual use facilities;

(2) Determine the types and effects of biological and chemical agents and radiological weapons or devices that are the most likely to be used and those constituting the 'worst case';

(3) Determine/estimate adversary's probable nuclear yields;

(4) Determine the adversary's tactics for employment;

(5) Identify the adversary's policy on use;

(6) Identify the capability for delivery.

c. TIM Determination:

(1) Chemical. Identify and record known chemical industrial plants and storage facilities (agriculture, pesticide, and research).

(2) Biological. Identify and record any industrial and medical facilities (agriculture and research) that could possess, produce and process biological agents.

(3) Radiological. Identify and record facilities that have radioactive sources in the area of operations (for example hospitals, nuclear, metallurgy and pipeline construction facilities).

A03. Area of Operation Evaluation. Identify the areas of operations and interest and conduct an in-depth evaluation to describe the operational environment:

a. Topography / weather;

b. Population;

c. Political/socio-economic and cultural analysis;

d. Infrastructure;

e. Rules of engagement, legal restrictions, and religious considerations;

f. Civil emergency planning;

g. Economy;

h. Standards.

A04. Terrain Analysis. The terrain is analyzed to determine its military significance and how it will affect operations in a CBRN environment. For example, large forests magnify the obstacle producing effects of nuclear and chemical weapons and valleys are possible targets for chemical weapons.

A05. Meteorological Analysis. Detailed weather information such as temperature, humidity, wind-speed, wind direction, precipitation and stability needs to be obtained to determine the effects on the employment of CBRN weapons and devices.

Annex B - Vulnerability, Risk Assessment and Risk Management

B01. General. CBRN defence is a subset of the overall vulnerability, risk assessment and risk management process carried out for FP in general. If the CBRN assessment is done in isolation it may not take proper account of other 'most likely' threats, the mitigation of which could be adversely affected by CBRN defence actions.

B02. Vulnerability Assessment

a. Vulnerability is an inherent exploitable weakness in an asset. Vulnerabilities include deficiencies in planning, preparedness, training, awareness, warning, physical security, hardening, redundancy/back up and response capability. A vulnerability assessment is a process used to determine the susceptibility of assets to attack from threats identified in the threat and hazard assessment. A vulnerability assessment compiles and examines information on the vulnerability of assets, including personnel, materiel, establishments, information, and activities. Vulnerability assessments may be conducted by multi-disciplinary assessment teams that conduct operational analyses and assess the vulnerability of employed personnel and materiel assets or by engineering and technical specialists who assess the structural vulnerability of facilities.

b. The result of a vulnerability assessment is the identification of deficiencies or weaknesses that render critical assets, areas or special events vulnerable to a range of known or likely threats.

B03. Risk Assessment. The risk assessment considers three points:

a. Probability or likelihood that a CBRN incident caused by threat or hazard will occur.

b. Probability or likelihood that a specific vulnerability will be exploited.

c. The impact on mission success in terms of numbers killed or numbers and degree of injury to personnel, damage to materiel or facilities, loss or corruption of information or other mission-impinging factors, such as morale or public opinion, that are caused by the degree of impact or severity of the threat.

B04. Risk Management. CBRN defence staffs will contribute to the operational planning process by highlighting force vulnerabilities and recommending mitigation. CBRN defence staff will also contribute to the risk management process described in AJP-3.14 which goes through four consecutive stages: avoidance, transference, mitigation and ultimately acceptance. This aims to minimize risk wherever possible, not eliminate it. Risk management integrates the processes of assessing the value of assets, threats and vulnerabilities, and weighs the risk of compromise or loss against the cost of implementing controls and measures and the impact on mission success.

Annex C – CBRN Threat and Risk Levels: General Guidance for CBRN Defence Components

C01. CBRN Threat Levels and Responsibilities. Threat levels may be different across the JOA. Authority will be specifically delegated to commanders to raise and/or lower threat levels within their area of responsibility. The risk to the joint force depends on the CBRN threat and the vulnerability of the force given its situation and CBRN defence capabilities. Assessment of these factors requires experienced CBRN defence personnel who can provide the commander with recommendations. Combined with inputs from other staff elements, the commander will then be able to decide on the appropriate CBRN defence measures and/or other actions to manage the risk.

C02. The implementation of protective measures should be subject to the commanders own risk and vulnerability assessment (based on the threat level) and risk management. ATP-65, The Effect of Wearing CBRN Individual Protection Equipment on Individual and Unit Performance During Military Operations, provides guidance on the effects of wearing CBRN IPE on individual and unit performance.

C03. A clear distinction is to be made between the threat posed by CBRN weapons and devices and those originating from a TIM release. Both are to be considered when planning and conducting operations as it is possible that NATO forces will encounter CBRN weapons and devices and TIM threats but not necessarily at the same time and to the same level.

CBRN WEAPONS OR DEVICES – THREAT LEVELS		
Threat Level	**Code**	**Description**
LOW	Green	A State or non-State actor has been identified who may possess either the capability or intention of targeting NATO forces or individuals. Although it is possible, there are no other indications of use.
MEDIUM	Yellow	A State or non-State actor has been identified as possessing both the capability and intention of targeting NATO forces or individuals.
SIGNIFICANT	Orange	A State or non-State actor has been identified as possessing both the capability and intention of targeting NATO forces or individuals, and will likely attempt to do so in the near term.
HIGH	Red	A State or non-State actor has been identified as possessing both the capability and intention of targeting NATO forces or individuals within a specific time frame and/or against a specific target.

Table C1. CBRN Weapons or Devices – Threat Levels

CBRN TIM - THREAT LEVELS[4]		
Threat Level	**Code**	**Description**
LOW	Green	Although TIM release is possible, industrial infrastructure[5] and security levels are robust.
MEDIUM	Yellow	There is an increasing risk of TIM release due to a decay of industrial infrastructure and/or a degradation of the security of industrial infrastructure.
SIGNIFICANT	Orange	Release of TIM may occur with little additional warning due to weakness of industrial infrastructure and/or insufficient security of industrial infrastructure.
HIGH	Red	There is an immediate risk of TIM release, without warning, due to damage to industrial infrastructure and/or a lack of security of industrial infrastructure.

Table C2. CBRN TIM – Threat Levels

C04. Risk Level. The impact of a risk is a function of the value of the asset and is compared with the likelihood (probability) of the exploitation of vulnerabilities by threats and hazards. Risk is displayed as a probability-impact risk-rating matrix. The risk assessment considers two points.

a. Probability. This is the likelihood that an incident caused by threat or hazard will occur and that a specific vulnerability will be exploited.

(1) Frequent. Expected to occur in most circumstances.

(2) Likely. May occur in most circumstances.

(3) Occasional. Could occur at some time.

(4) Seldom. Not expected to occur.

(5) Unlikely. Occurs in exceptional circumstances only.

b. Impact. The impact on mission success in terms of levels of death or injury to personnel, damage to materiel or facilities, loss or corruption of information or other mission-impinging factors that are caused by the level of impact or severity of the threat.

(1) Catastrophic. Would stop achievement of functional goals/ objectives.

(2) Critical. Would threaten functional objectives.

[4] The likelihood of release is based on an assessment of accidental, collateral or intentional release.
[5] e.g. Installations, storage sites, transportation networks, pipelines.

(3) Marginal. Necessitates significant adjustment to overall function.

(4) Negligible. Would threaten an element of the function.

c. The combination of impact and probability produces the overall risk level as shown in table C3. Commanders must decide whether this level of risk is acceptable for the mission or may take further action to mitigate the risk by reducing the impact or the likelihood.

Annexes B and C describe a simplified version of the UK force protection risk management process described in JDP 3-64 Chapter 3. The UK process should be followed, with a similar table to Table C3 being produced as an output to address the levels of mitigated risk.

Impact	**Probability of Exposure**				
	Frequent	**Likely**	**Occasional**	**Seldom**	**Unlikely**
Catastrophic	Extremely High	Extremely High	High	High	Moderate
Critical	Extremely High	High	High	Moderate	Low
Marginal	High	Moderate	Moderate	Low	Low
Negligible	Moderate	Low	Low	Low	Low
	Risk Levels				

Table C3. CBRN Defence Risk Analysis 1

C05. Table C4 offers general guidance on CBRN defence measures. Based on the risk assessment, commanders should consider mitigation options such as counter-force activity, securing TIM sites, and the CBRN defence posture. Once CBRN suits have been issued in addition to respirators, the standard dress states given in table C5 may then be used to control the dress of personnel according to their immediate situation.

Risk Level	Code	Component of CBRN Defence Recommended Posture[6]				
		Detection, Identification & Monitoring (DIM)	Information Management	Physical Protection	Hazard Management	Medical Countermeasures
Low	GREEN	Plan in place	CBRN information management system in place but dormant	Conduct recurring training to use physical protection (Unless high-readiness)	Plan in place	Long-term vaccinations in place
Moderate	YELLOW	Specialist equipment in theatre but not operating	CBRN information management System in place but dormant	Respirator Issued Suit Ready COLPRO Deployed	Specialist equipment in theatre but not issued	Countermeasures deployed but not issued
High	ORANGE	Specialist equipment ready & operating	CBRN information management System active and proved	Respirator issued Suit ready COLPRO set up	Specialist equipment ready	Countermeasures issued
Extremely High	RED	Specialist equipment ready & operating	CBRN information management System active and proved	Respirator issued Suit issued COLPRO activated	Specialist equipment issued	Pre-treatments taken
NOTE: Implement national guidance when appropriate in lieu of the guidance on this table.						

Table C4. CBRN Defence Measures – General Guidance

[6] For definitions of postures used in this table see notes at the end of the section.

Dress States	ITEMS OF DRESS			
	RESPIRATOR	SUIT	FOOT PROTECTION	HAND PROTECTION
ZERO	Issued and Carried	1st set ready		
		2nd set deployed		
ONE	Carried	Issued and Carried	Issued and Carried	Issued and Carried
TWO	Carried	Worn	Carried	Carried
THREE	Carried	Worn	Worn	Carried
FOUR	Carried	Worn	Worn	Worn

Table C5. CBRN Defence Dress States

Notes and Remarks with Regards to the Tables C4 and C5

1. The CBRN defence measures and the graduated individual protection equipment regimes, as set out in the tables, are advisory and are to be viewed as an illustration. Depending on the equipment in use national instructions may be issued.

2. As a general rule, the protection measures to be adhered to are the ones giving the adequate degree of protection associated to risk level. Designated subordinate local commanders are authorised to either reduce or increase the level of protection in a particular area, taking into account special local conditions or situations demanding a different degree of protection. For example, a designated commander may order the level of protection to be:

   a. Reduced if warranted by special conditions (e.g. personnel inside CBRN COLPRO and/or commanders assess the risk of CBRN casualties is outweighed by benefits of reduced individual protective equipment).

   b. Increased (e.g. if local conditions demand a higher degree of protection).

3. Definitions:

   a. Deployed = available in theatre

   b. Ready = available in unit stores / rear areas

   c. Issued = available to individuals

   d. Carried / worn = by / on the individuals

   e. Setup = install

   f. Activated = operating

4. To the maximum possible extent, respiratory and body protection must be appropriate to the specific risk. Specific canisters/suits might be required depending on

the possible concentration of the specific threat substances.

5. The term “Mask” or “Respirator” may be added to any of the dress state in order to encompass any nationally-recognised form of respiratory protection.

The UK has introduced an additional CBRN Dress State (0C, or ‘Zero-Charlie’) in recognition that Commanders should be able to direct personnel who do not routinely carry their respirators (as on current operations) to do so. The UK CBRN dress states are thus as follows:

Dress states	**Items of dress**			
	Respirator	**Suit**	**Foot protection**	**Hand protection**
Zero	Issued	1st set ready		
		2nd set deployed		
Zero-Charlie	Issued and carried	1st set ready		
		2nd set deployed		
One	Carried	Issued and carried	Issued and carried	Issued and carried
Two	Carried	Worn	Carried	Carried
Three	Carried	Worn	Worn	Carried
Four	Carried	Worn	Worn	Worn

UK Table 6. UK CBRN protection dress states

Annex D – CBRN Consequence Management

D01. Introduction

a. Consequence management comprises those measures taken to mitigate the damage, loss, hardship and suffering caused by catastrophes, disasters or hostile actions. It also includes measures to restore essential services, protect public health and safety and provide emergency relief to affected populations. Essential services and activities may include transportation, communications, public works and engineering, fire fighting, information planning, mass care, resources support, health and health services support, urban search and rescue, hazardous materials, food and energy, banking and finance. CM operations may include support to the protection of public health and safety; restoration of essential government services; and provision of emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. However, this annex will focus on CM in response to CBRN incidents.

b. NATO forces may be required to support civil authorities in the event of a CBRN incident. NATO could be required to render support to identify, assess, transfer, and dispose of a contaminant or conduct decontamination operations. The task force commander would conduct planning to meet the various mission-specific CBRN threats.

D02. Approach to CM Operations. Effective C2 is essential to fully use available assets in accomplishing CM missions. C2 relationships in CM may be tailored to a particular situation. Unity of effort focuses on the commander's intent and in maintaining coordination with the HN.

D03. Planning for CBRN CM Operations

a. A challenge for commanders conducting CM operations is to adequately protect personnel, materiel, equipment and mission critical facilities from further CBRN effects caused by the CBRN incident. There is a need for a response capability to save lives, contain an incident, and recover to a point that permits operations to resume. Confronting this challenge requires a comprehensive and integrated approach from threat identification to incident response and recovery. This comprehensive planning ensures that measures of effectiveness are considered. These measures serve to provide a tool to help assess when the mission's established end state is met.

b. No single agency possesses the capability and expertise to act unilaterally on many complex issues that may arise in response to CBRN incidents. For example, an act of terrorism, particularly CBRN attack directed against a large population centre, may produce major consequences that could overwhelm the capabilities of the HN.

c. For a CBRN incident, essential elements of information (EEI) may include the following:

(1) Damage and injury profile. Assess the damage and casualty estimates. CBRN devices or vectors each present unique considerations that impact CM contingency planning. Planners use available decision support tools to conduct the assessments.

(2) Information management. Timely collection, analysis, reporting and dissemination of information is paramount. Establish measures to coordinate information management activities. Other requirements include information management measures that ensure the following:

(a) Interoperability for reports being submitted to and received from the civilian incident control system; and

(b) Measures that provide SA to support the commander and staff (e.g. number of casualties, boundaries of contamination).

(3) Containment. Planners receive information where perimeters have been established from the civilian incident commander. The contaminated site should be clearly marked to prevent personnel from mistakenly entering. Personnel who have been in contaminated areas must be identified and requisite actions taken (medical treatment, decontamination, etc.). Site containment also provides for actions to consolidate and confine any contaminated material (water runoff). Personnel exposed during the incident, subsequent cloud passage, or post-incident entry into the contaminated area, are given a high priority in response actions. This includes responders and other contaminated individuals. Early definition of the perimeter is important so that potentially contaminated people may be identified and measures taken to prevent the contamination of additional people. The potential contamination of critical infrastructure and transportation assets presents a health problem for both responders and bystanders. Procedures to be considered include the following:

(a) Initial monitoring upon arrival to determine preliminary site characterization and personnel contamination;

(b) Procedures to minimize the spread of contamination.

(4) Decontamination. Planners identify and understand the casualty, personnel, and equipment decontamination requirements and standards. Coordination is required with HN authorities. Resources must be provided that can monitor, detect, and identify the degree and source of contamination. Subject matter experts conduct risk assessments to determine options for the conduct of decontamination and recommend the allocation of necessary resources to support the

decontamination process. Safety is a paramount concern in the decontamination planning process to ensure that first responders' exposure is minimized. Control measures are also taken to minimize the exposure to and the spread of any contamination.

(a) Contamination control. Contamination-control measures ensure contamination is not transferred from an area that is already contaminated to an uncontaminated area through the orderly processing of personnel, equipment, and vehicles entering and leaving the contaminated area. The actual amounts of material used for contamination control depends on conditions at the incident site.

(b) Equipment decontamination. Military-specification equipment should be decontaminated according to pertinent military technical publications; however, similar guidelines may not exist for other equipment. Some equipment used by the response force in the contaminated area may remain there for future use and will not require immediate monitoring or decontamination. Some equipment may not be salvageable and will require proper disposal. If civilians in the contaminated area are sent or go to processing points using their own vehicles, the vehicles should be monitored before moving away from the area. All outer surfaces and the air filters may have been contaminated by airborne contamination. Wheel wells, tires, and the underside may be contaminated from driving across contaminated areas. Unless the windows were down or ventilators open, detectable contamination of the interior is most likely on those surfaces contacted by vehicle occupants (e.g. floorboards, seats).

(5) Evacuation. Planners determine if personnel in downwind hazard areas were directed to seek shelter in place or evacuate. This planning is coordinated with HN authorities. Specific planning factors include resourcing protective-equipment requirements for large numbers of people and medical support. Personnel or equipment evacuated from a hazard area are checked for the possibility of residual contamination. Contaminated casualties are decontaminated before evacuation to avoid health-care-facility contamination. For example, the presence of a contaminated casualty in a hospital and the passage of chemical vapours throughout a building's ventilation system could close the entire hospital.

(6) Medical requirements. Health services support planners need any available epidemiological and diagnostic patterns resulting from the incident. Health services support capabilities can provide either specialized CBRN advisory response capabilities or augmentation that can expand existing medical capabilities. This process includes

receiving input from first responders reporting information on signs and symptoms from casualties or agent characteristics (i.e., smell/odour). Health services support planning addresses preventive medicine, laboratory services, casualty evacuation, and decontamination and treatment of casualties.

(7) CBRN RECCE. Military units usually have basic sampling and detection capabilities. CBRN defence units have more specialized capabilities and may be required to conduct reconnaissance, sampling, survey and monitoring in order to determine the extent of any hazard.

(8) Weapon disposition. Determine what type of weapon is involved. If the military is tasked, units are prepared to determine the nature of the weapon or provide assistance as required to the agency with the task.

(9) Transition and disengagement. The termination of military support to civil authorities during a CM operation is a politically sensitive phase requiring detailed planning. The "end state" defining the point at which military forces disengage from the CM operation is based on the policy that NATO will withdraw from the operation after eliminating the immediate danger of weapon/agent effects, saving lives, and restoring critical services. NATO forces will generally not remain to conduct site-recovery operations. When it is agreed that local authorities are capable of assuming responsibilities for the remainder of the operation, NATO forces will disengage. This could be phased either by function or area. Development of an exit strategy should begin as soon as possible during the response.

(10) Force protection. FP is a top priority during CM operations; it begins from the time units are alerted to move, involves impacted personnel and evacuees, and does not end until redeployment is complete. The following FP considerations are provided as a guide:

(a) Protection from potential threats. Ensure that proper protective equipment is available to response personnel.

(b) Safety. Safety in training, planning, and operations is crucial to successful operations. On-scene command authorities and response personnel must implement requirements established by the appropriate site safety and health plans.

(c) Security. Security elements protect against all acts designed to, or which may, impair the effectiveness of the military forces. This includes guarding equipment and supplies from loss or damage.

(d) Individual awareness. Commanders and supervisors stress the significance of hazards and the importance of being aware of what is going on around them.

(e) Health. Take measures to protect personnel from contaminants. This will require avoiding contaminated areas and observing their boundaries. Protection of the response personnel includes proper preventive medicine and mental health considerations.

D04. Conducting CBRN CM

a. **Civilian and political considerations**. Operations associated with CM are very sensitive to civilian and political considerations. Planners modify and tailor information activities to meet the unique challenges presented in each operation. Information resources at every echelon are structured to provide support that is proactive, predictive, and flexible. The commander ensures all sources of information are considered and fully involved.

b. **Legal considerations**. Any plans for military operations associated with CBRN CM must receive a thorough legal review. The operations themselves must also receive legal support.

c. **Information gathering**. Support to CM requires a multidiscipline approach. A single-source approach cannot support all requirements.

(1) EEIs that drive the collection-management process require an understanding of all aspects of the area and its cultures, politics, religion, economics, environment, technology, and other related factors.

(2) CM will likely involve in-depth coordination or interaction with civil authorities and NGOs. The term "information gathering" should be used rather than the term "intelligence." Non-military organizations may resent being considered a source of intelligence. By using the term "information gathering," military forces may be able to foster better communications with other agencies and thereby benefit from their valuable knowledge.

(3) The importance of mapping, charting, and geodesy should not be overlooked. It is essential that maps, charts, and support data (to include datum and coordinate systems) are coordinated.

(4) Imagery, if approved, can provide information concerning the extent of damage and could be useful for operations planning.

d. **Information support**. Successful support during CM relies on continuous information collection and analysis. This includes anticipating and initiating collection against long lead-time requirements, synthesizing available information on the JOA, and orchestrating the collection efforts of existing organizations.

(1) Technical information support. The provision of technical information about possible agents and weaponized materials, the methods of dissemination and the impact on targets are essential to planning. This information is required during the conduct of an operation. A responder at an incident site should be able to provide information to technical and scientific agencies and receive further information about the type of device or material found on site.

(2) Remote information support. A remote ("reach-back") information-collection capability is needed. The Task Force Consequence Management must be able to access assets such as scientific support, which could be at a fixed or mobile analytical facility.

e. **Response Activities**

(1) During the initial response phase (that includes pre-deployment and deployment), activities will be tracked and briefed to the commander. This information provides input to support the commander's SA and to support the decision-making process. This information also focuses the staff's efforts, assists in resource allocation and assists staff when making recommendations. Liaison and effective coordination with HN agencies assists the commander in gaining required information. The intent is for the commander to have the best available information on activities within the JOA.

(2) Information that is significant to emergency-response operations during a CBRN incident include, but is not limited to the following:

(a) Threat conditions/situations/capabilities;

(b) Determination of FP status and shortfalls;

(c) Detailed knowledge of the area;

(d) Detailed information on the type of material used. Consider worst and best case scenarios for options. The types of protection possible against such weapon(s), materials, or vectors; their size, weight, description, and capability; and the methods that could neutralize them;

(e) Medical facilities or equipment available and shortages of such equipment that could impact on any attempt to neutralize the threat or lessen the consequences. The number of people they can handle and the emergency transportation methods available;

(f) Number and location of victims and/or other damage;

(g) Description and status of lines of communications including major roads, railroads, waterways, ports, and airports;

(h) Meteorological conditions including precipitation, fog, cloud conditions, temperature, relative humidity, prevailing winds, and sunrise/sunset data;

(i) Characteristics of physical damage in the specific disaster area;

(j) Population of areas such as trailer parks, apartments, and subdivisions. School buildings and warehouses in these areas are excellent candidates for shelter, feeding, and life-support sites;

(k) Status of sanitation systems;

(l) Relief and drainage systems;

(m) Surface materials. Identify the type and the distribution of soils and sub soils in the area and soil trafficability;

(n) Sources of all classes of supply needed for critical restoration of normal activities;

(o) Availability of civilian engineer equipment and personnel.

D05. Recovery, Transition, and Redeployment – General Outlines

a. **General**. Recovery, transition, and redeployment operations start when civil authorities or other designated agencies are prepared to take over operations from the task force commander. The operational duration of the response mission is determined by the requirements established by the appropriate task force commander. A transition plan is developed and implemented such that CM tasks are transferred from the task force commander to the appropriate civil authorities commensurate with their ability to continue to conduct operations. NGOs and/or contracted services may augment these civil authorities. Upon completion of the required recovery support, the task force commander executes transition and redeploys.

b. **Recovery Operations**

(1) Start the recovery phase. The recovery phase begins when the immediate hazards are contained or controlled to the point that military assets are replaced or are no longer needed. During the recovery phase, emergency-response elements initiate the action to restore conditions at and in the vicinity of the incident site to a technically feasible and acceptable state. During the recovery phase, the response commander will facilitate the orderly transition of C2 and conduct the withdrawal of military forces from the incident site when the capabilities and services of the response elements are no longer required.

(2) Develop and implement a mission-specific recovery plan. This plan must be coordinated with civil authorities to determine the requirements. Clearly defined goals and objectives ensure that tasks between civil authorities and the task force commander are understood and completed. Top priorities are re-establishing mission capability, developing a plan to cover short and long term recovery requirements, and returning to normal operations. Special consideration is given to minimizing and mitigating environmental damage. The mission-recovery plan can address the following areas:

(a) Logistic support and re-supply;

(b) FP;

(c) Documentation and reporting requirements, to include resource expenditures, losses, and environmental-exposure data that are necessary to estimate exposure (to determine long term and short term health effects);

(d) Decontamination;

(e) Environmental considerations to prevent pollution and restore the area;

(f) Medical issues to include:

(i) Personal protection;

(ii) Casualty-handling operations;

(iii) Medical screening and documentation and critical-incident stress management.

(g) Liaison with local, regional and HN officials as required;

(h) Public affairs activities.

c. **Transition**

(1) Transition in CM operations involves the transfer of responsibilities and functions to other organizations. Transition generally occurs between units and the HN. Transition and/or termination are initiated once objectives are met and authority is given from the task force commander.

(2) A transition plan helps the staff identify transition issues in relation to the desired or projected end state. It is especially important to identify those parties or agencies that will receive functional responsibilities from the task force commander. Considerations include which staff sections will write annexes, based on what the transitioning

organization will do. The transition plan should identify organization, operating procedures, and transition recommendations and considerations. When implementing the transition plan, the transitioning parties should discuss criteria for transferring operations. The plan should be unclassified, clear and concise using terminology appropriate to all parties.

(a) Transitioning may be by function or by specific areas of the incident site. The transition process should be incident driven and not tied to calendar dates. Functions or areas transfer only when a similar capability becomes available or is no longer needed. Procedures for the transfer of equipment or supplies, either between task force CM units and the civil authorities, or to local or HN agencies, must be established according to regulation and command guidance.

(b) Planners identify other key transition factors within functional areas that may include logistics, communications, security, and technical services. Planners should develop a series of transition criteria to monitor progress; the important part of choosing indicators is to have a consistent method by which to measure progress during the transition.

d. **Redeployment**

(1) Simultaneous with deployment, the task force commander begins planning redeployment. Redeployment decisions are based on civil and military considerations. Redeployment begins as soon as objectives are accomplished or the need for military forces diminishes. Redeployment planning should follow normal guidelines and protocols. Careful consideration should be given to what physical assets can be safely removed from the incident and which should be contained or controlled; and whether or not those should be left at the incident site. High-value assets which cannot be removed may have to be secured or destroyed in place to prevent unauthorized handling or movement out of the incident site.

(2) Redeployment includes the use of the after action report (AAR) process to help evaluate mission and task performance. The AAR addresses the following:

(a) What was the original mission? How was it stated and how was it interpreted at the various levels of command?

(b) What should have happened (e.g. the mission or plan)? What actually happened (e.g. a description of the incident)?

(c) How it happened (e.g. key facts that led up to the incident)?

(d) Why it happened (e.g. inferences about probable causes)?

(e) How to improve performance next time (e.g. alternative courses of action)?

Lexicon

Part I – Acronyms and Abbreviations

AAR	after-action report
AJP	Allied joint publication
ALARA	as low as reasonably achievable
ATP	Allied tactical publication
C2	command and control
C4ISR	command, control, communication, computer, intelligence, surveillance and reconnaissance
CBRN	chemical, biological, radiological and nuclear
CCA	contamination control area
CIMIC	civil-military cooperation
CIS	communication and information systems
CM	consequence management
COLPRO	collective chemical, biological, radiological and nuclear protection
COP	common operational picture
EEI	essential elements of information
EMP	electromagnetic pulse
FP	force protection
HN	host nation
IPE	individual protective equipment
IPOE	intelligence preparation of the operational environment
JFC	joint force commander
JOA	joint operations area
JTF	joint task force
NSA	NATO Standardisation Agency
RDD	radiological dispersal device
RED	radiological exposure device
TFA	toxic-free area
OPLAN	operation plan
SA	situational awareness
SIBCRA	sampling and identification of biological, chemical and radiological agents
SOP	standing operating procedures
TIB	toxic industrial biological
TIC	toxic industrial chemical
TIM	toxic industrial material
TIR	toxic industrial radiological
TREE	transient radiation effects on electronics
W&R	warning and reporting

Part II - Terms and Definitions

Notes:

1. The majority of the terms and definitions used within AJP-3.8 are drawn from AAP-6 'NATO Glossary of Terms and Definitions' and AAP-21 'NATO Glossary of CBRN Terms and Definitions'.

2. Bracket indicates the short title of the source when applicable.

CBRN agent
A generic term used for substances in solid, liquid, aerosolized or gaseous forms that are designed to incapacitate or kill a person.

chemical, biological, radiological and nuclear defence (CBRN defence)
Plans and activities intended to mitigate or neutralize adverse effects on operations and personnel resulting from: the use or threatened use of chemical, biological, radiological or nuclear weapons and devices; the emergence of secondary hazards arising from counter-force targeting; or the release, or risk of release, of toxic industrial materials into the environment. (AAP-21)

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. Note: CBRN incidents are either `suspected´ or `confirmed´ as appropriate to the situation.

Consequence Management
Measures taken to mitigate the damage, loss, hardship and suffering caused by catastrophes, disasters or hostile actions. Note: It also includes measures to restore essential services, protect public health and safety and provide emergency relief to affected populations. (NSA(JOINT)0478(2009)1/CBRN dated 27 April 2009)

environmental and industrial hazard (EIH)
A natural or artificial risk or challenge to the well-being of personnel or the employment of forces that derives from any source other than the presence or use of CBRN weapons or analogous devices. Note: An EIH may be of a chemical, biological or radiological nature but may also result from the physical form or behaviour of a material or process.

Reference Publications

PO(2010)0169	The Alliance's Strategic Concept
SG(2005)0918	Comprehensive Political Guidance (CPG)
EAPC(C)D(2009)00119	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
MCM-077-00	Military Committee Guidance on the Relationship between NATO Policy and Military Doctrine
MC 327/2	NATO Military Policy for Non-Article 5 Crisis Response Operations
MC 400/2	MC Guidance for the Military Implementation of Alliance Strategy
MC 411/1	NATO Military Policy on Civil-Military Cooperation (CIMIC)
MC 422/3	NATO Policy on Information Operations
MC 457/2	NATO Military Policy on Public Affairs
MC 472	NATO Military Concept for Defence Against Terrorism
MC 511	MC Guidance for Military Operations in a CBRN Environment
MC 586	Military Concept for the NATO Response Force
AAP-6 (2010)	NATO Glossary of Terms and Definitions
AAP-15 (2011)	NATO Glossary of Abbreviations Used in NATO Documents and Publications
AAP-21	NATO Glossary of Chemical, Biological, Radiological and Nuclear (CBRN) Terms and Definitions
AJP-01	Allied Joint Doctrine
AJP-2	Allied Joint Intelligence Counter Intelligence and Security Doctrine
AJP-3	Allied Joint Doctrine for the Conduct of Operations
AJP-3.10	Allied Joint Doctrine for Information Operations
AJP-3.14	Allied Joint Doctrine for Force Protection
AJP-5	Allied Joint Doctrine for Operational Level Planning
AJP-9	Doctrine for NATO Civil-Military Co-Operation (CIMIC)
ATP-3.8.1 Volume I	CBRN Defence on Operations
ATP-3.8.1 Volume II	Specialist NBC Defence Capabilities
ATP-3.8.1 Volume III	CBRN Defence Standards for Education, Training and Evaluation

ATP-45	Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Operators Manual)
ATP-65	The Effect of Wearing CBRN Individual Protection Equipment on Individual and Unit Performance during Military Operations
ATP-70	Collective Protection in a Chemical, Biological, Radiological and Nuclear Environment (CBRN - COLPRO)
AEP-10 Volume I	NATO Handbook for Sampling and Identification of Biological and Chemical Agents (Procedures and Techniques)
AEP-49 Volume I	NATO Handbook for Sampling and identification of Radiological Agents (SIRA) (Operational)