NATO STANDARD

AJP-3.8

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

Edition B Version 1
OCTOBER 2018

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

Intentionally blank

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

3 October 2018

1. The enclosed Allied Joint Publication AJP-3.8, Edition B, Version 1, ALLIED JOINT DOCTRINE FOR COMPREHENSIVE CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR DEFENCE, which has been approved by the nations in the Military Committee Joint Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2451.

2. AJP-3.8, Edition B, Version 1, is effective upon receipt and supersedes AJP-3.8, Edition A, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.

4. This publication shall be handled in accordance with C-M(2002)60.

Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

Intentionally blank

RESERVED FOR NATIONAL LETTER OF PROMULGATION

Intentionally blank

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATIONS BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
BGR	1. National COLPRO assets will be applied until acquisition of COLPRO assets which match ATP-70 requirements. Deployed units participating in NATO-led operations will apply procedures for use of COLPRO assets contributed from Leading Nation. 2. Due to the lack of appropriate equipment the Bulgarian Armed Forces will not apply the identification and sampling of biological agents. 3. Bulgarian CBRN units will apply only tactical and operational sampling. The forensic sampling will be applied after acquisition of relevant equipment.
GBR	Within the Enabling Components of CBRN Defence, the UK refers to SENSE, rather than the equivalent NATO Enabling Component 'Detection, Identification and Monitoring (DIM)
USA	1) There are numerous references in the doctrine to 'CBRN agents'. The US will not follow doctrinal guidance concerning 'CBRN agents' Clarity. The US recognizes 'CBRN hazards' (there are biological agents and chemical agents in US doctrine). This reservation will be lifted when the AJP is revised and the reference clarified. 2) There are 2 references (2.14, 3.19) that provide unclear guidance on WMD transfer. The transfer of WMDs are bound by international law; specifically, certain treaties, resolutions, and control regimes. The US will remove this reservation when the AJP clearly states that the transfer of WMD Disablement operations must comply with international law obligations. 3)The US does not recognize "Naval CBRN EOD teams" and "Naval CBRN defence teams" as standard NATO military elements. These descriptions appear to be a nation's unique solution for carrying out their national operations. This reservation will be lifted when the current paragraph is revised to read, "They may require support from CBRN specialists if any associated technical tasks within the mission exceed their internal capabilities" 4) The United States objects to the validity of the following statement: "3.14.3 SOF's main task is to make a safe and secure operation area in order to enable operation to continue in a CBRN

	environment." This statement conflicts with the higher level guidance on SOF operations that the NATO nations have ratified within AJP-3.5, Allied Joint Doctrine for Special Operations. As is stated in AJP 3.5 (A), "SOF conduct three principal tasks: military assistance, special reconnaissance, and direct action." It is NOT their main task "to make a safe and secure operation area in order to enable operation to continue in a CBRN environment". This reservation will be lifted when AJP-3.8 is properly harmonized with AJP-3.5. 5) The United States objects to the use of the term “kinetic.” Joint doctrine does not use the terms ‘kinetic’ and ‘non-kinetic’. Kinetic is defined as “of or relating to the motion of material bodies and the forces and energy associated therewith”, non-kinetic” is not a recognized word. NATOTerm refers to ‘lethal’ and ‘non-lethal’ force or weapons. his reservation will be lifted when the current paragraph is revised 6) The United States objects to the validity of the following statement: "The risk management process consists of five phases: identify hazards and threats, assess hazards to determine risk, develop controls and measures, implement controls and measures, and supervise and evaluate." This statement conflicts with the higher level guidance on risk management within AJP-3, Allied Joint Doctrine for the Conduct of Operations. The risk management process consists of Communication and consultation, Establishing the context, Risk identification, Risk analysis, Risk evaluation, Risk treatment, and Monitoring and review. This reservation will be lifted when AJP-3.8 is properly harmonized with AJP-3. 7) A number of terms introduced in this AJP do not conform to approved NATO terminology, or have been incorrectly introduced. IAW NATO Terminology guidance found in C-M(2007)0023. The US recognizes only NATO approved terms. This reservation will be lifted when the correct NATO terms are cited and proper procedures followed for introducing new terms.

Table of Contents

List of Tables

List of Figures

Related Documents

	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
	Treaty on the Non-proliferation of Nuclear Weapons
	Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction
	Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction
	UN Security Council Resolution 1540
SG(2005)0918	Comprehensive Political Guidance (CPG)
PO(2010)0169	The Alliance's Strategic Concept
	Alliance Maritime Strategy (18 Mar 2011)
MC0603	(11 June 2014), NATO Comprehensive CBRN Defence Concept
MC 400/3 (Final)	MC Guidance for the Military Implementation of Alliance Strategy
MC 0511	MC Guidance for Military Operations in a CBRN Environment
MC 0590	CBRN ReachBack and Fusion Concept
MCM-0230-2014	NATO CBRN Reachback Element Concept of Operations
MC 469/1	NATO Military Principles and Policies for Environmental Protection (EP)
AJP-01	Allied Joint Doctrine
AJP-2	Allied Joint Intelligence Counter Intelligence and Security Doctrine
AJP-2.1	Allied Joint Doctrine for Intelligence Procedures
AJP-3	Allied Joint Doctrine for the Conduct of Operations
AJP-4	Allied Joint Logistics Doctrine
AJP-3.1	Allied Joint Doctrine for Maritime Operations
AJP-3.2	Allied Joint Doctrine for Land Operations
AJP-3.3(A)	Allied Joint Doctrine for Air and Space Operations
AJP-3.5	Allied Joint Doctrine for Special Operations
AJP-3.14	Allied Joint Doctrine for Force Protection
AJP-3.15	Allied Joint Doctrine for C-IED
AJP-4.4	Allied Joint Movement and Transportation Doctrine
AJP-4.5	Allied Joint Host Nation Support Doctrine and Procedures
AJP-4.10	Joint Medical Support Doctrine
AJMedP-7	Allied Joint Medical Doctrine for Support to CBRN Defensive Operation
ATP-3.8.1 Volume I	CBRN Defence on Operations
ATP-3.8.1 Volume II	Specialist CBRN Defence Capabilities
ATP-3.8.1 Volume III	CBRN Defence Doctrine for Education, Training, Exercise and Evaluation
ATP-3.8.1 Vol IV	CBRN Defence Disposition for Education, Training, Exercise 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 CBRN Environment
ATP-71	Allied Maritime Interdiction Operations
ATP-84	CBRN Defence Equipment Operations Guidelines Edition B
ATP-91	Identification of Land Forces on the Battlefield and in an area of Operation
AEP-45(CD)	Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Reference Manual)
AEP-66	NATO HANDBOOK for SIBCRA
C-M(2011)0068	Proposals for Enhanced Civil Military Cooperation in Chemical, Biological, Radiological and Nuclear (CBRN) Defence.
AMedP-6-C	NATO handbook on the medical aspects of NBC defensive operations
AMedP-7.4	Regulations for establishment and employment of MRIIT (Medical radiological incident investigation teams)
AMedP-7.6	Commanders Guide on Medical Support of CBRN Defensive operations
AMedP-8	Planning Guidance for the Estimation of CBRN Casualties
AIntP-10	Allied Joint Doctrine on Technical Exploitation
STANAG 3497 ED3	Aeromedical Training of Aircrew in Aircrew CBRN Equipment and Procedures
STANAG 4586 ED3	Standard Interfaces of UCS for NATO UAV Interoperability
AAP-6 (2013)	NATO Glossary of Terms and Definitions
AAP-15 (2011)	NATO Glossary of Abbreviations Used in NATO Documents and Publications
	NATO Terminology Management System (NTMS)

Preface

CBRN Defence: The plans, procedures and activities intended to contribute to the prevention of chemical, biological, radiological and nuclear incidents, to protect forces, territories and populations against, and to assist in recovering from, such incidents and their effects.

Scope

1. Allied Joint Publication (AJP)-3.8 is the primary Chemical Biological, Radiological and Nuclear (CBRN) Defence doctrine for the North Atlantic Treaty Organization (NATO). This publication is also applicable to Component Commands to plan, execute and support NATO operations where there is the threat or occurrence of a CBRN incident**.**

2. In accordance with MC 400/3, *MC Guidance for the Military Implementation of Alliance Strategy*, one of NATO's permanent tasks remains CBRN defence**.**

3. CBRN defence capabilities may be employed across all NATO operations.

Purpose

4. *NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of WMD and Defending against CBRN Threats* adopts a three-pillar approach to WMD non-proliferation and CBRN defence against CBRN threats**.** The three pillars are as follows:

- **PREVENT :** To prevent or reverse the proliferation of WMD by state and non-state actors;
- **PROTECT** : To protect the Alliance from WMD attack or CBRN incident should prevention fail**;**
- **RECOVER**: To recover should the Alliance suffer a WMD attack or CBRN incident.

5. The implementation of this 'three-pillar' approach not only encompasses the full spectrum of traditional CBRN defensive measures and capabilities existing within NATO, but also includes tasks, such as NATO forces support to reinforcing arms control regimes, promoting disarmament, supporting multilateral non-proliferation agreements and monitoring of the CBRN threat. This encompasses operations across the full range of tactical activities from peacetime military engagement to state-on-state conventional conflict.

6. Preventing proliferation is in principal a diplomatic goal of the Alliance and its member states. In the event of proliferation, the Alliance will seek to counter proliferation and must be capable to conduct WMD Disablement (WMDD) Operations.

7. To meet the three-pillar approach, a conceptual framework for a credible, coherent and broad-based NATO CBRN defence capability was developed. This draws upon the collective

competencies of all Allied and NATO bodies into a comprehensive political, military and civilian approach.

8. AJP-3.8 (B) describes NATO's CBRN capabilities in the broader context of NATO's comprehensive approach to both its contribution to WMD non-proliferation and CBRN defence alongside the principal Courses of Action (COA) NATO could take as outlined in Military Committee (MC) 0511, *MC Guidance for Military Operations in a CBRN Environment*. This document:

- adjusts the fundamental guiding principles of CBRN defence;
- outlines the CBRN defence capabilities including how civil-military cooperation in CBRN defence is best achieved;
- describes the activities and measures aimed at preventing a CBRN incident and the actions required to better manage the consequences of a CBRN incident should preventive actions fail.

9. AJP-3.8 guides operational staff to proactively contribute to the prevention of adversaries' CBRN substance possession or release. NATO recognizes that neutralizing an adversary's offensive CBRN capability before it is employed is preferable.

10. CBRN substances include all chemical or biological agents, a Toxic Industrial Material (TIM)[1] or a radioactive material, in any physical state or form. Figure Pre-1 illustrates CBRN incident origin, employment and method of release.

[1] Includes CBRN agents found in industrial, medical and academic facilities.

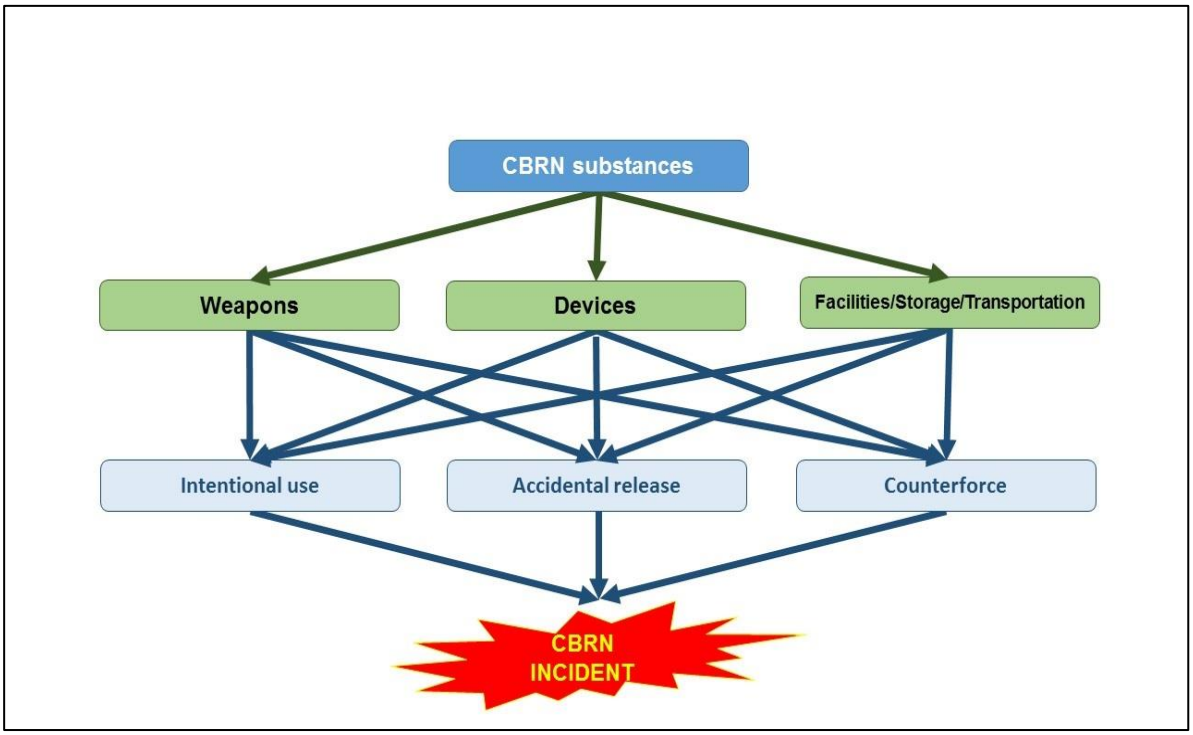


Figure Pre-1. CBRN incident origin

Hierarchy and Related Publications

11. AJP-3.8 is directly subordinate to the keystone document 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.

12. 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 four (4) volumes:

a. ATP-3.8.1 Volume I – CBRN Defence on Operations. This volume provides detailed information and guidance at the tactical level on CBRN defence planning and implementation of CBRN defence measures to those involved in the preparation, planning and execution of joint operations.

b. 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.

c. ATP-3.8.1 Volume III – CBRN Defence Doctrine for Education, Training, Exercise and Evaluation. This volume provides doctrinal details on CBRN education, training, exercise planning and evaluation protocols.

d. ATP-3.8.1 Volume IV – CBRN Defence Disposition for Education, Training, Exercise and Evaluation. This volume provides details on how CBRN training has to be conducted by NATO forces.

CHAPTER 1 − CBRN Threats and Hazards

CBRN Operational Tasks

1.1 CBRN incidents may create effects that disrupt or delay operational and strategic objectives, and even lead to mission failure. NATO forces must be prepared to conduct operations despite the risk of those incidents. The information contained in this chapter will assist the Joint Force Commander (JFC) and subordinate and supporting commanders and their staff understand and appreciate the unique nature of the CBRN threat environment.

1.2 The intelligence cycle, as described in AJP-2, *Intelligence, Counter-Intelligence and Security Doctrine*, is a key function that will generate CBRN related intelligence. In turn, this will help establish the CBRN threat levels that are critical in determining the CBRN defence posture.

1.3 Operations' planning normally takes into account the threat and potential adversarial use of CBRN substances and should include, as appropriate, counter proliferation activities. The JFC's Priority Intelligence Requirements (PIR) and indicators support operations, assist in preventing the surprise use of CBRN weapons and devices by an adversary, and enable planning and preparation to mitigate the effects of a CBRN incident. In addition to mapping potential adversary capabilities and establishing target folders, plans for CBRN Consequence Management (CM) after CBRN incidents arising from TIM and environmental hazards is vital. Planning must include measures for generating adequate and timely force capabilities for countering the threat from potential use or accidental release of CBRN substances. CBRN defence operations can reduce the CBRN threat and create the conditions for sustained operations.

Adversary Types

1.4 As outlined in AJP-01, *Allied Joint Doctrine*, notionally, adversaries are expected to be drawn from 3 broad categories of protagonists: nations, factions within a state, and non-state actors. The preventive activities for countering an adversary possessing a CBRN offensive capability are listed in table 2-1. Allied Forces must be prepared and ready to conduct preventive activities.

1.4.1 **Nation state.** The Alliance remains concerned that WMD proliferation is expanding the list of states that can pose a direct threat to NATO territories. The state actor threat represents the greatest CBRN defence challenge for the Alliance where the CBRN threat is probably the most potent in terms of lethality, scale and doctrinal refinement.

1.4.2 **Factions within a state.** The threats presented are likely to be similar to that of a non-state actor. CBRN forensics will be vital to establishing the link to the supporting network. The ability for Allied Forces to attribute the source of a CBRN substance may act as a powerful deterrent.

1.4.3 **Non-state actors.** Although the CBRN threat from non-state actors might be less potent, it is harder to predict and brings significant challenges in terms of CBRN related intelligence. It is critical

to ensure a robust link between CBRN advisors and the intelligence community. This includes intelligence personnel, education and training to identify CBRN indicators.

Understanding the CBRN Threat Environment

1.5 The Joint Intelligence Preparation of the Operational Environment (JIPOE) provides an understanding of the Operational Environment (OE) and supports the Comprehensive Preparation of the Operational Environment (CPOE). Drawing on the Joint Intelligence Estimate (JIE), it focuses the intelligence effort and delineates the prioritization of intelligence requirements. It is a living product and in addition to contributing to the early stages of the operational estimate, assists in the implementation of the plan by identifying opportunities to promote decisive action. As such, the CPOE should include a detailed analysis of the potential CBRN threats and hazards.

1.6 The nations collaborative information sharing will help the JFC continue to refine and deepen their knowledge and shared understanding of the OE. Estimates require a constant re-examination of the OE that adopts a broader perspective of the situation, problems, and local challenges within the Joint Operations Area (JOA). During mission analysis at the tactical level, commanders and staff can draw most of the relevant information needed for mission analysis from the more comprehensive analysis of their OE, using the variables of mission, adversary, terrain, troops, time, and civil considerations.

1.7 Commanders and staff must continuously analyse their OE, progress of operations, and relevant CBRN factors, comparing them to the commander's initial vision and intent. Understanding the operational variables, their interaction with each other and how relationships among those variables change over time is essential. It helps commanders and staff to realize how the effects of CBRN threats and hazards can affect their OE.

1.8 A CBRN threat can affect forces and require them to conduct WMDD and CBRN CM operations. JIPOE supports JFC's CBRN defence activities by providing analysis on potential threats and hazards within the OE.

CBRN aspects of the Operational Environment

1.9 The analysis of CBRN aspects of the OE utilises the system of system analysis of the Political, Military, Economic, Social, Information and Infrastructure (PMESII) model. This is supported by Annex A.

CHAPTER 2 − Fundamentals of CBRN Defence

General

2.1 The CBRN threat environment has broadened the battlefield to the globe. This includes the Alliance's populations, territory and forces without any restriction concerning temporal, geographical, social or political limits. Forces must be prepared to execute and support prevention, protection, and recovery measures that potentially affect both civilian populations and military forces.

2.2 Potential adversaries continue to develop and field CBRN weapons and/or devices despite the existence of a broadly (but not universally) accepted regime of international agreements prohibiting such actions. This trend is most pronounced in areas of chronic political turmoil and lacking government structure. NATO must be prepared to conduct operations in these regions. Additionally, there have been recurring instances of non-state actors using CBRN substances as a means of prosecuting their interests. Scientific advances in academia, industry, and medicine not designed for weaponisation increase the potential for transfer and use. At the same time, expanding urbanization and global industrialization are opening up wider possibilities for accidental release or intentional misuse of TIM.

2.3 The aim of CBRN defence is the prevention of chemical, biological, radiological and nuclear incidents, the protection of populations, territories and forces against, and the assistance in recovering from, such incidents and their effects. Consequently, the commander will have to plan, coordinate and execute operations with multiple organizations.

The relationship between the policy pillars, aims and tasks is provided in table 2-1:

NATO WMD/CBRN Policy Pillars		
Prevent	**Protect**	**Recover**
Aims		
• Prevent the acquisition of CBRN substances. • Deter the use of CBRN substances. • Prevent intentional use or accidental release of CBRN substances. • Support the reduction of extant CBRN substances.	• Reduce extant CBRN substances • Disrupt CBRN substances • Support the prevention of follow-on incidents • Mitigate the immediate effects of CBRN substances on personnel and Allied capability.	• Prevent follow-on attacks. • Manage the effects of a CBRN incident. • Restore operational effectiveness.
The Cross-cutting functions required for Comprehensive CBRN defence ultimately provide the basis for the CBRN defence Key and Subsequent Tasks. The link between the Functions required for Comprehensive CBRN defence as well as the respective Tasks with the three pillars of prevent, protect and recover.		
Tasks		
• Provide support to CBRN substances non-proliferation initiatives and programmes. • Provide support to prevent the proliferation and use of WMD and their means of delivery.	• Take actions to protect the force and to provide support for the protection of civilians, equipment, facilities, information and infrastructure. • Respond to the evolving threats as early as possible through appropriate CBRN defence measures. • Provide CBRN protection and conduct timely and effective CBRN incident response.	• Support CBRN CM operations, on a case by case basis and within existing means and capabilities.

Table 2-1. Relationship between the Policy Pillars, Aims and Tasks

Comprehensive Approach

2.4 The CBRN defence comprehensive approach is described as coordinated political, military and civilian actions taken to support CBRN defence in accordance with MC 0603/1 NATO Comprehensive CBRN Defence Concept.

2.5 In addition to greater emphasis on prevent activities, the CBRN defence comprehensive approach leverages increased civil-military interaction, improves coordination and cooperation, and brings benefits at the strategic level, ensuring a more holistic approach in meeting the CBRN threat. Moreover, it encompasses the broader role of CM and prevention activities that allows force contribution to reducing the CBRN threat and improved preparation if an incident occurs.

Operational Framework

2.6 In the OE, forces could encounter adversaries possessing offensive CBRN capabilities. In addition to deliberate attack, commanders must take into account the risk of CBRN substances from accidental actions.

2.7 CBRN threats pose additional challenges to operations. They may have disruptive, destructive and devastating effects that merit continuous consideration.

2.8 Commanders will be required to develop and implement measures to minimize the vulnerability of personnel, units, facilities, equipment, material, and infrastructure in order to preserve freedom of action and force effectiveness.

2.9 Commanders must consider CBRN defence aspects during the Operations Planning Process (OPP), because the employment and allocation of CBRN defence assets may determine whether, in addition to survival and self-protection, operations can be continued. Personnel, material, and infrastructure may have to be restored and, when necessary and possible, decontaminated in order to re-establish operational effectiveness.

2.10 Targeting and counter-force efforts leverage all source intelligence and exploitation activities. CBRN defence objectives can only be achieved by thoroughly addressing and prioritizing joint actions through synchronized operations, coordinated intelligence collection, and targeting support.

2.11 CBRN advice has to be an integral component of the planning process. The CBRN defence staff must be fully integrated into the staffing and planning process and support the battle rhythm of every level of command and across all operations. Commanders must consider the possibility of CBRN threat and deploy appropriate CBRN defensive measures. The threat characteristics and associated protective measures should be continually revised to ensure that both survivability and freedom of action are maintained.

2.12 While CBRN defence and Force Protection (FP)[2] have overlapping complementary responsibilities, the comprehensive CBRN defence approach requires activities going beyond the

[2] FP is described in AJP-3.14.

traditional scopes of FP issues, which must be separately addressed, planned, directed and coordinated.

CBRN Defence Principles

2.13 CBRN defence principles are established to provide commanders and their staff guidance. These principles should be taken into consideration during the planning and execution phase, affording a foundation for the conduct of CBRN defence on operations before, during and after a CBRN incident. CBRN defence principles comprise the following:

a. **CBRN related Intelligence requirements.** This is an integrated part of the JIPOE aiming to gather and analyse information in order to address the full spectrum of CBRN threats, hazards and risks across the three pillars. CBRN Detection Identification Monitoring (DIM) supports the CBRN intelligence collection requirements, which should be part of the Joint Intelligence, Surveillance and Reconnaissance (JISR) process. The CBRN related intelligence output will contribute to the CBRN threat assessment.

b. **CBRN Threat Assessment.** Process to determine the most likely and most dangerous case scenario based on the full spectrum of CBRN threats, hazards and subsequent risks. Threat assessments are based on accurate and timely all-source intelligence, and are essential in the identification of hazards. 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, where applicable, is essential for producing actionable intelligence. The JIPOE supporting this activity is further explained in Chapter 3 and Annex A.

c. **CBRN Risk Management**. The principle of CBRN defence in support of FP should be risk management, not risk elimination. Threat and hazard assessment set against own force vulnerabilities allows the identification of risk areas that will need to be managed and increased CBRN defence measures applied in order to limit the operational impact of a CBRN incident. CBRN Risk Management is further discussed in Chapter 3 and Annex B.

d. **Interoperability**. All components of the force should consider CBRN defence interoperability and harmonization of both military and civilian capabilities. The harmonisation of respective nations and, where appropriate, Host Nation's (HN) capabilities and information exchange should be prioritized.

e. **Prioritization**. It is unlikely that CBRN defence specialist capabilities will be available in sufficient quantities to support all elements of the force to the same degree. This should be accounted for in the CBRN Vulnerability Assessment and priorities for support must be determined.

f. **Flexibility.** CBRN defence must be flexible, modular and scalable in application and capable of responding to a rapidly changing OE while cognizant of differing national policies and capabilities.

g. **Force preparation.** NATO forces must be prepared for CBRN defence to include the appropriate doctrine, equipment, procedures, organisation, and training. These preliminary CBRN defence measures need to be in place before NATO is committed to operations so that the necessary operational capability is present in theatre. Such preparations also serve to deter potential adversaries from considering the use of CBRN substances.

h. **Sustainability.** CBRN incidents place additional burdens on the sustainability of the elements deployed. Effective CBRN defence will require additional logistic resources, and CBRN incidents may degrade the supply chain. The logistic plan will need to address the inherent vulnerability of fixed assets and facilities to CBRN hazards at entry points into theatre and on Lines of Communication (LOC) through protection and redundancy.

Application of the Three-Pillar Approach

2.14 Prevent

2.14.1 The prevention consists of actions to stop adversaries from successfully acquiring, delivering and using CBRN offensive capabilities. Preventive actions could include early and sustained operations to secure CBRN substances including the disruption or destruction of CBRN offensive capabilities if required, and the establishment of multi-layered defences against CBRN threats. The employment of the Intelligence Surveillance Target Acquisition and Reconnaissance (ISTAR) process from the strategic to tactical level will contribute to the reduction of force vulnerability and could assist in threat reduction and/or the will of an adversary to employ CBRN offensive capabilities. Prevention requires an understanding of threat and partner network capabilities.

2.14.2 Of the additional actions, WMDD operations may be the most prominent and effective. They are actions to systematically locate, characterise, secure, disable, or destroy WMD programmes and related capabilities. The objective of WMDD operations is to prevent the looting or capture of CBRN weapons, devices and related materials; render harmless or destroy weapons, materials, agents, and delivery systems that pose an immediate or direct threat to NATO populations, territory and forces; and exploit, for intelligence purposes, programme experts, documents, and other media, as well as previously secured weapons and material to counter further WMD proliferation and prevent regeneration of an offensive WMD capability. Once these activities have been accomplished, WMDD operations may be transferred, if directed, to Other Government Agencies (OGA), Intergovernmental Organizations (IGO), or HN to continue destruction, redirection, and monitoring activities. If transfer is not directed, the commander could be required to accomplish the remaining activities, and should request coordination and technical assistance from applicable agencies, as necessary. When determining whether to disable or destroy WMD capabilities, especially by using kinetic weapons, commander must consider the possible adverse effects on local populations and friendly forces by inadvertent contamination.

2.15 Protection

2.15.1 The commander must undertake CBRN protection measures to keep CBRN threats and hazards from having adverse effects on personnel, equipment, critical assets, and facilities. CBRN protection involves identifying CBRN threats and hazards as well as avoiding and preventing or mitigating the effects of those hazards. CBRN protection may also extend beyond protection of the

force to encompass civilians, systems, and civil infrastructure. Throughout an operation, a commander must constantly consider and evaluate the effectiveness of current CBRN protection measures, and utilize both active and passive defence capabilities to reduce vulnerability to CBRN threats and hazards. These actions reduce the CBRN risk, and influence or deny a potential adversary the benefit of proliferation and employment of CBRN offensive capabilities.

2.15.2 Appropriate in-place CBRN defence measures prior to incident allow the force to be suitably protected immediately on warning of and during an incident, reducing the impact and lowering casualty numbers. Such measures include contamination avoidance, unit relocation, Collective Protection (COLPRO) systems, Individual Protective Equipment (IPE), medical MedCM and casualty care, and immediate decontamination procedures.

2.15.3 Commanders must continuously consider measures to reduce the force's vulnerability to CBRN threats and hazards. Preparatory activities are fundamental to increasing the survivability of the force during a CBRN incident but some measures can degrade operational efficiency and the commander's freedom of movement. Effective risk management will allow the commander to achieve an appropriate balance. This means that pre-incident actions are not pre-defined but are a result of appropriate CBRN related assessments balanced against other threats to the force. During this phase, measures and equipment are planned, prepared, tested, and, if necessary for some measures, implemented.

2.16 Recovery

2.16.1 Planning for CBRN incident recovery is a multi-dimensional effort, requiring continuous coordination with the HN, including its civilian emergency planning authorities, as well as with participating partner nations and other International Organisations (IO), as appropriate. Recovery aims to restore freedom of action as quickly as possible.

2.16.2 Incident response. Properly prepared forces will respond effectively to ensure appropriate action against hazards by initially mitigating the effects of a CBRN incident and performing only those tasks required to allow continuation of the mission and, within mission constraints, save lives.

2.16.3 Incident recovery. The response must enable the quick restoration of essential capabilities or combat power required to accomplish the current mission and achieve operational objectives. In addition, implementation of CM plans allows restoration of acceptable environment conditions, enabling continued freedom of movement.

Enabling Components of CBRN Defence

2.17 General

2.17.1 NATO must ensure an appropriate level of CBRN expertise and manning throughout the command structure

2.17.2 The capability levels of CBRN defence are listed in table 2-2:

Capability levels	Description of capability
Basic capability	To ensure the survivability of the individual.
Enhanced capability	To ensure the continuation of operations under CBRN threat or in a CBRN environment.
Specialised capability[3]	To ensure the qualified accomplishment of CBRN defence missions and tasks by Allied Force Specialist CBRN defence force.

Table 2-2. CBRN defence capability levels

2.17.3 NATO developed five enabling components underpinning all CBRN defence activities and they are the foundation for CBRN defence on operations. The five enabling components are listed and summarized below:

- Detection, Identification and Monitoring (DIM).
- CBRN Knowledge Management (KM)[4].
- Physical Protection (PP).
- Hazard Management (HM).
- Medical Countermeasures (MEDCM) and Casualty Care.

2.18 Detection, Identification and Monitoring (DIM)

2.18.1 DIM capabilities, to include area reconnaissance and surveillance, allow CBRN hazards to be characterised, analysed and identified. This includes delineation of areas of contamination, and allows monitoring of changes over time. It contributes to the CBRN layer of the Common Operation Picture (COP) and CBRN forensics and technical exploitation.

2.18.2 Detection indicates, by any means, the presence of a CBRN substance. The equipment must be made ready and tactics, techniques, and procedures executed to detect hazardous materials at appropriate threat levels at the earliest possible opportunity and timely alerts and/or alarms given. In addition, medical detection, direct observation, diagnosis and/or pattern recognition supports effective response.

2.18.3 Identification is the recognition of a specific CBRN substance arising from a CBRN incident. There are three levels of identification[5] with varying degrees of reliability: provisional, confirmed and unambiguous.

2.18.4 Sampling supplements identification and is the retrieval for analysis of CBRN substances and related devices, materials, artefacts and traces. Based on the aim of sampling and available

[3] The term specialized refers to qualified level of CBRN defence capabilities as described in MC 0603/1.
[4] The term knowledge management is described as efficient handling of information and resources, and thus a more appropriate term than information management as described in MC 0603/1.
[5] More details in ATP 3.8.1 Vol I.

sampling assets/teams, sampling is divided in three types: tactical, operational and forensic. Sampling should be conducted by CBRN specialists or specially trained personnel equipped with specific equipment.

2.18.5 Monitoring is the continuous or periodic process of determining the presence or absence of a CBRN hazard and can be conducted on personnel, equipment, terrain or facilities.

2.19 CBRN Knowledge Management (KM)

2.19.1 CBRN KM aims to collect and manage CBRN-related information from one or several sources, along with the dissemination of raw and/or analysed information. It provides situation awareness to decision-makers, thus contributing to information superiority and timely decision making.

2.19.2 To assess vulnerability and provide input in support of planning processes, KM must be an integrated part of the JIPOE. As part of a comprehensive CBRN defence approach, the KM processes must provide the critical intelligence cycle link and handle initial forensic information whilst facilitating both reachback and the fusion of CBRN information. This holistic approach supports decision-making across the three pillars.

2.19.3 CBRN KM is composed of the following functional areas and enablers:

- CBRN advice.
- CBRN Warning and Reporting (W&R).
- Information management, fusion and dissemination.
- Sensor Integration and network management.
- CBRN Reachback.
- Advanced modelling, simulation, and hazard prediction.

2.20 Physical Protection (PP)

2.20.1 Physical protection combines measures and equipment intended to enhance the survivability of personnel and materiel in a CBRN environment.

2.20.2 Although PP enhances survivability, it can reduce operational capability. The commander must reconcile the joint force vulnerability to CBRN hazards with the protective measures restrictions and mission accomplishment.

2.20.3 Personnel should be provided with IPE. The commander needs to be aware that there are limitations on the effectiveness of the different types of IPE issued and used by each nation may provide different levels of burden and protection. The commander needs to continuously monitor the risk of personnel exposure to CBRN hazards and adapt the protective measures accordingly.

2.20.4 IPE use will result in performance degradation; however, COLPRO systems can provide necessary protection against the broad range of CBRN hazards. To mitigate performance degradation COLPRO systems may allow the continued performance of operational functions while lessening the psychological and physiological effects that result from the extended use of IPE.

2.21 Hazard Management (HM)

2.21.1 Hazard Management is an enabling component where forces seek to avoid contamination, recover personnel, regenerate equipment and restore infrastructure to maintain or re-establish operational tempo and effectiveness. HM combines preparatory and responsive measures and should be an integral part of operational planning and, as much as possible, be prepared well in advance.

2.21.2 HM comprises a wide range of measures, including those for CM, ensuring:

- Survivability.
- Pre-hazard precautions.
- Hazard avoidance.
- Hazard control.
- Decontamination.

2.22 Medical Countermeasures (MEDCM) and Casualty Care

2.22.1. Medical Countermeasures include, among others, pharmaceuticals, biologics, vaccines designed to diminish the susceptibility of personnel to the lethal and damaging effects of CBRN substances, and to treat any effects arising from exposure to such hazards. MEDCM must be issued to personnel under national guidelines but declared to allied nations to ensure effective medical interoperability and reduced risk of adverse drug interactions .

2.22.2. MEDCM are divided into pre-exposure and post-exposure. Pre-exposure medical countermeasures rely on a trigger based on threat assessment. Post-exposure medical countermeasures rely on a detection or intelligence trigger. There are four concepts of use for MEDCM:

- Pre-exposure prophylaxis (prevention).
- Pre-treatment (or treatment enhancers).
- Post-exposure prophylaxis (prevention)
- Immediate therapy (treatment).

2.22.3. Medical Support to CBRN Defence Operations. The medical contribution to CBRN defence covers all five of the enabling components. AJMedP-7 provides the link between CBRN medical support and other areas of joint medical support described in AJP-4.10, Joint Medical Support

Doctrine.

a. Detection and Medical Operations. Medical forces may to help clarify the meaning and implications of information provided by DIM, or from other indicators of CBRN incidents. In addition, medical forces have a primary role in the DIM component of CBRN defence through health and disease surveillance, especially for biological agents. When a CBRN incident is suspected, specialized medical capabilities, such as the RDOIT or MRIIT, may be directed to support targeted surveillance, reconnaissance, and survey actions.

b. Knowledge Management and Medical Operations. Medical forces are responsible for management of CBRN medical information and for supporting the integration of medical information with CBRN defence KM and across the force. Medical staff will also support commanders in fulfilling obligations for information as reporting of public health emergencies of international concern as required by International Health Regulations.

c. Physical Protection and Medical Operations. Medical staff, in coordination with CBRN, meteorology, and operations staffs, will be responsible for providing advice on managing the adverse physiological effects of wearing IPE, such as heat stress and dehydration.

d. Hazard Management and Medical Operations. Medical forces are responsible for CBRN casualty HM, including procedures for decontamination of casualties. Planning of medical evacuation in a contaminated environment requires information from CBRN defence control centres for the anticipated type, duration, size, and location of hazard areas. In the event of contagious disease casualties, medical staff is responsible for advising the commander on the implementation of Restriction of Movement (ROM) intended to prevent the spread of disease.

e. Medical Countermeasures and Casualty Care in a CBRN Environment. Medical staff is prepared to support Command decisions on the implementation of medical countermeasures. Medical advice should include criteria for the implementation of medical countermeasures, timing and procedures for implementation, and information on potential adverse reactions and/or operational degradation. Sustainment of medical operations and continuity of care during operations in a CBRN environment will be challenging. The tempo of medical operations is likely to be very high, with an associated strain on the availability of scarce resources.

2.22.4. General guidance on the implementation of medical countermeasures can be found in AMedP-7.6 Commanders' Guidance on Medical Aspect of CBRN Defence

Cross-cutting Functions

2.23. **Appropriate level of CBRN expertise and manning in all command structures**. Command structure, CBRN expertise, and staff are essential for an immediate and successful CBRN incident response. CBRN defence staff must be able to perform and/or assist with:

- a CBRN threat assessment;

- a vulnerability assessment of own force and HN capabilities, population, territory and CBRN assets; and

- a risk assessment based on the CBRN threat assessment, vulnerability assessment and likelihood of occurrence in order to develop risk management plans.

2.24. **Comprehensive fusion of information**. JIPOE requires a comprehensive fusion of information about potential adversaries linked with potential hazards. These potential hazards include research facilities, medical installations, industrial plants such as chemical industry, bulk storage of toxic materials, nuclear power plants and other potential sources of toxic releases such as waste disposal sites.

2.25. **Effective Communication Information System (CIS).** Effective CIS that incorporates specialist CBRN information requirements and services and provides risk management, planning and execution support is essential. It needs to follow network enabled principles and process information from the sensors through an automated W&R system to the CBRN defence specialist network. All data needs to be processed and displayed in the form of a COP. Relying on effective communication and information exchange, reachback provides additional expertise and a better understanding supporting the decision making process**.**

2.26. **Joint Intelligence Surveillance and Reconnaissance[6] (JISR).** JISR is an integrated intelligence and operations set of capabilities, which synchronises and integrates the planning and operations of all collection capabilities with processing, exploitation, and dissemination of the resulting information in direct support of planning, preparation, and execution of operations. CBRN staff will need to engage early in order to ensure the requirements and contributions to and from KM and DIM functional areas are incorporated into the JISR architecture.

2.27. **Strategic Communication (STRATCOM)**. Media attention will be intense, and the identified or perceived CBRN threats will generate considerable disquiet, both in the operational area and at home. A CBRN incident requires a proactive information flow addressing the current and future concerns. Based on the threats and emergent hazards, a comprehensive strategic communication plan needs to be implemented and lines to take considered in advance. STRATCOM will enable the provision of accurate, timely and credible information to the media and the public, in case of a CBRN incident and facilitate CM and recovery efforts by keeping the general population informed.

2.28. **Education, Training, Exercise and Evaluation.** Allied operations' multinational and joint character demands coherence and interoperability between national force contributions. The adoption of common CBRN doctrine, Training, Tactics and Procedures (TTP) and the exercising of these standards is imperative. This is brought together in the Individual Training and Education Programme (ITEP) and the Multinational Training and Exercise Programme (MTEP). Evaluation is conducted in accordance with ATP-3.8.1 Vol IV and ACO Forces' Standards (AFS).

[6] AJP-2 – Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security (Para. 3.9).

Intentionally blank

CHAPTER 3 −Command Considerations for Planning and Conduct of CBRN Defence

Section 1 – Introduction

General

3.1 Plans must include options for countering CBRN threats within the OE. The CBRN staff plans and coordinates the activities to prevent, protect, and recover from adverse effects on operations and personnel. Planning staff are required to take into account the comprehensive approach for CBRN defence and the strategic enabling activities that are available.

3.2 The commander should anticipate and incorporate planning factors such as HN, national and international laws to ensure compliance. CBRN staff in collaboration with J2 needs to recommend PIR in order to be able to fully appreciate the CBRN threat picture. Commanders should take pre-crisis actions to identify all CBRN threats, detect and prevent adversary employment of CBRN substances, and plan active and passive defence operations to prevent or minimize CBRN attacks. A fully supported JIPOE will inform a commander, enabling him to counter, mitigate and manage the effects of CBRN incidents, whatever the cause.

3.3 With HN, coalition partners, and other governmental and civilian authorities and organizations in the OE, particular emphasis should be placed on early warning, detection, and awareness of differing operating procedures as well as actions to protect friendly military forces, threatened civilian populations and essential infrastructure.

3.4 Integration is a fundamental principal for countering the CBRN threat. Planning staff must understand and consider the CBRN threat within the operational estimate and not view it as a separate planning topic. To enable this, CBRN staff, must be integrated into the OPP from the start so they can provide advice and guidance on:

- CBRN threat;
- Relevant HN capabilities;
- Allied CBRN defence capabilities requirements; and
- CBRN risk management and COA development.

Section 2 – Key CBRN Defence Planning Considerations

3.5 The commander utilizes the CBRN risk assessment to provide guidance on the balance between operational and CBRN defence priorities.

3.6 It is the commander’s responsibility that plans take into account appropriate CBRN defence

measures. The commander must be provided with timely, accurate and evaluated CBRN threat, vulnerability and risk assessments.

3.7 It is essential that CBRN defence staff engage early in the planning process and incorporate CBRN-related intelligence requirements into the Intelligence Collection Plan (ICP). The staff must contribute to a CBRN JIPOE in order to ascertain the threat. The full JIPOE, of which CBRN is a minor but essential part, supports the estimate process and helps to both identify and satisfy the commander's PIR.

Section 3 – Conduct of CBRN defence operations

Introduction

3.8 Effective C2 is the key to successful CBRN defence operations supported by an integrated Command, Control, Communications, Computers and Information (C4I) architecture. CBRN defence Standing Operating Procedures (SOP) must be prepared enabling the compilation, processing, and dissemination of information before deployment and this section offers some activities that may be included in the SOP. The joint force must exercise, train, validate and adjust these SOP prior to and during deployment to meet the likely conditions in the OE. Checks must be made to confirm which general operating procedures may be used or modified for employment within a CBRN environment.

3.9 If prevention fails or a possible broader threat is identified, there are three distinct phases of a CBRN incident as it relates to CBRN defence activities. These phases are as follows:

a. Pre-incident. Knowledge and preparatory activities are fundamental to increasing the survivability of the force during a CBRN incident but some measures can degrade operational efficiency and therefore the commander's freedom of action. During this phase, measures and equipment are planned, prepared, tested, and, if necessary for some measures, implemented.

Specific activities that may need to be addressed and included in SOP are the following:

- Establishment of a CBRN defence organisation;
- Engagement with organisations/ authorities to identify and mitigate TIM threats and hazards;
- CBRN defence equipment preparation;
- Electronic/sensitive equipment protection;
- DIM and HM planning;
- CBRN risk levels assessed and protective measures installed;
- MEDCM and casualty care implementation;

- COLPRO availability confirmed;
- STRATCOM requirements confirmed;
- Contribution to public information on risks.

b. During-incident. Application of the appropriate pre-incident CBRN measures allows the force to be suitably protected immediately on warning of and during an incident. This includes contamination control, unit relocation, COLPRO system use, IPE, and immediate decontamination procedures.

Specific subjects that may need to be addressed and included in SOP are the following:

- Emergency alarms and W&R system available;
- DIM availability to confirm and identify hazards;
- IPE availability confirmed;
- Effective and timely CBRN KM;
- STRATCOM requirements confirmed;
- MEDCM and casualty care established;
- HM procedures established;
- Contribution to public information and collaboration with HN on hazards.

c. 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 protection level 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.

Specific subjects that may need to be included in SOP are the following:

- CBRN KM processes and requirements;
- DIM to confirm contamination status of personnel, equipment and affected area;
- MEDCM and casualty care is conducted;
- STRATCOM requirements confirmed;
- HM is conducted;

- Recovery is conducted;
- Contribution to public information and collaboration with HN;
- Additional support requirements considered.

CBRN Defence Considerations at Component Level

3.10 General

3.10.1 A strong and effective CBRN defence posture can only be achieved through active participation of and cooperation between all elements of the Task Force (TF). Joint operations must be planned, conducted and supported, against the full spectrum of CBRN threats and hazards.

3.10.2 When deciding the force lay down, the commander should consider CBRN threats and hazards within the vicinity of force elements that could directly affect and may significantly reduce readiness and operational effectiveness.

3.11 Land Component

3.11.1 AJP-3.2, *Allied Joint Doctrine for Land Operations*, describes the fundamental principles of land operations.

3.11.2 The varied nature of land operations causes the various characteristics and effects of CBRN hazards to have different operational impacts to those arising in the air and maritime operating environments.

3.11.3 The varied vulnerabilities of Land Forces may be mitigated to a considerable degree by the application of preventive principles that build upon wider operational doctrine. There may be significant opportunities for vulnerability reduction by means of dispersion, concealment, deception, maintenance of tempo, targeting and the application of the principle of surprise. These will deny or diminish an adversary's ability to find targets, assemble appropriate delivery systems and deliver effective CBRN attack.

3.12 Air Component

3.12.1 AJP-3.3(A), *Allied Joint Doctrine for Air and Space Operations*, describes the fundamental principles of air and space operations.

3.12.2 Persistent air operations require the availability of secure airbases sufficiently close to or within the JOA to enable freedom of movement in support of surface operations. Following a CBRN incident, air operations may need to be conducted within the hazard area because it may not be practical to transfer operations to another base outside the affected area in response to a short-term hazard.

3.12.3 When operating under CBRN conditions, the launch rate for air missions will be significantly reduced. Aircrew CBRN equipment and procedures require high standards of user training and crews are subject to physiological degradation in these conditions[7].

3.13 Maritime Component

3.13.1 AJP-3.1, *Allied Joint Doctrine for Maritime Operations*, describes the fundamental principles of maritime operations.

3.13.2 Maritime platforms may be able to transit CBRN hazards by the use of the COLPRO provided by the citadel and the use of the pre-wet system. However, maritime platforms may be more vulnerable to CBRN incidents when in harbour or operating in the littoral waters. Considerable planning effort is required to re-embark air or amphibious assets that may have been operating within or near a contaminated area.

3.13.3 Maritime forces play an important role in counter proliferation activities. The maritime security operation tasks that support counter proliferation (Uphold Freedom of Navigation, Maritime Interdiction, Fight weapons of mass destruction (WMD) proliferation, Protect Critical Infrastructure, Support Maritime Counterterrorism, Contribute to Maritime Security Capacity Building, Support Maritime Situational Awareness) are described within AJP-3.1. CBRN Defence specialists may be called upon to support maritime assets and provide capabilities that exceed maritime regular capabilities. Maritime assets/ units should be equipped and trained sufficiently in accordance with NATO standards to respond to CBRN threats and incidents.

3.14 Special Operations Force Component

3.14.1 AJP-3.5, *Allied Joint Doctrine for Special Operations*, describes the fundamental principles of special operations.

3.14.2 Special Operations Forces (SOF) are a significant part of allied capabilities to support NATO's counter proliferation and trafficking objectives related to WMD and CBRN substances. They may require support from CBRN Specialists such as CBRN EOD team and CBRN defence team if the associated tasks within the mission exceed their internal capabilities.

3.14.3 SOF's main task is to make a safe and secure operation area in order to enable operation to continue in a CBRN environment. Interoperability and seamless integration of CBRN assets is vital.

3.15 Joint Logistics Support Group (JLSG)

3.15.1 AJP-4, *Allied Joint Doctrine for Logistics*, describes the fundamental principles of logistic support operations; AJP-4.5, *Allied Joint Doctrine for Host Nation Support*, and AJP-4.4, *Allied Joint Doctrine for Movement & Transport*, provide additional related information.

3.15.2 Logistic bases, installations and LoC may provide an attractive target for an adversary with a CBRN offensive capability. This is because they are likely to be fixed, cover a wide area and be well defined.

[7] See more information in STANAG 3497

3.15.3 By their nature, logistic bases and installations are highly likely to contain large quantities of TIM that could present a hazard through either intentional or accidental release. In addition, such sites are likely to contain a significant proportion of joint force resources in transit and storage which may become contaminated and spread and transmit CBRN hazards.

CBRN Threat Levels and Responsibilities

3.16 The CBRN threat levels may be different across the JOA. Authority can be specifically delegated to assess the level of risk 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. The assessment of these factors requires experienced and suitably qualified CBRN personnel who are able to recommend appropriate CBRN defence measures to the commander.

3.17 The implementation of protective measures should be subject to the commander's appreciation of the operational impact of the effect of wearing CBRN IPE on individual and unit performance during military operations (ATP-65).

3.18 There is a clear distinction between a CBRN weapon threat and that posed by a TIM release. While both pose a hazard, the level and flexibility of employment may vary resulting in different planning and operational considerations.

CBRN WEAPONS OR DEVICES – THREAT LEVELS		
Threat Level	**Code**	**Description**
LOW	■ Green	A state or non-state or faction within a 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 or faction within a state has been identified as possessing both the capability and intention of targeting NATO forces or individuals.
SIGNIFICANT	■ Orange	A state or non-state actor or faction within a state 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 or faction within a state 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 3-1. CBRN Weapons or Devices – Threat Levels

CBRN TIM - THREAT LEVELS		
Threat Level	**Code**	**Description**
LOW	■ Green	Although TIM release is possible, infrastructure[8] and security levels are robust.
MEDIUM	■ Yellow	There is an increasing risk of TIM release due to a decay of infrastructure and/or a degradation of the security for the infrastructure.
SIGNIFICANT	■ Orange	Release of TIM may occur with little additional warning due to weakness of infrastructure and/or insufficient security for infrastructure.
HIGH	■ Red	There is an immediate risk of TIM release, without warning, due to damage to infrastructure and/or a lack of security for infrastructure.

Table 3-2. CBRN TIM Threat Levels

3.19 Joint Staff Responsibilities for CBRN Defence

3.19.1 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 the JFC's operational objectives in a CBRN threat environment. The CBRN defence staff must then collate the combined JFC staff output to produce a coherent full spectrum CBRN defence annex for the OPLAN.

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

a. Personnel. J1 priority is to maintain all personnel records and availability of combat effective forces. Procedures for dealing with mass fatalities and contaminated remains are particularly sensitive and will require guidance from the strategic level. An approved plan for the management of contaminated human remains and mass fatalities in a CBRN environment needs to be in place. 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. Medical staff will ensure that procedures are in place to record individuals' exposure to CBRN substances but such information must remain part of individuals' personnel records both during and after their period of service.

b. Intelligence. Intelligence staff must provide accurate, timely and relevant intelligence on the possible CBRN threat, to meet the JFC's operational and FP needs. Within the JFC headquarters, 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. Intelligence staff will draw on expertise from within the CBRN defence staff to

[8]To include: Industrial Installations, storage sites, transportation networks, pipelines, medical, research, and educational facilities.

ensure that the significance of scientific or technical information derived from intelligence sources is fully appreciated.

c. Operations and Planning. CBRN defence expertise in JFC's headquarters will be responsible for providing CBRN defence advice to on-going operations. However, as the main source of CBRN expertise, the staff in this area should ensure that the full spectrum of CBRN aspects are considered and incorporated into operational planning and contingency planning. When included as part of a deployed Joint Task Force (JTF), CBRN defence specialist assets are coordinated and assigned within the JOA by the CBRN defence staff. These assets may be a mix of military and civilian organisations/agencies from different nations that have various specialized capabilities and will require careful coordination to achieve optimum effect.

d. Knowledge Management . To ensure that the commander can quickly carry out measures to mitigate the CBRN threat, hazard, and risk, the CBRN defence staff will:

- collect and collate information;
- assess threats and risks;
- plan the deployment of and manage DIM assets;
- report incidents;
- predict hazards, identify and warn forces at risk;
- compile the CBRN contribution to the COP;
- advise and direct CBRN units and assets;
- track samples;
- manage hazards;
- plan and manage liaise on matters such as PP, MEDCM and casualty care.

e. Communication and Information Systems (CIS). It is essential that CBRN defence is provided with the ability to be fully integrated within the JFC CIS in order to maintain a comprehensive CBRN COP layer. This will enable the commander to receive timely warnings, exercise effective C2 over assets, and balance the CBRN risk to assets within the JOA.

f. 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.

g. Training. The commander has responsibility for ensuring that all members of the joint force (which may include civilians) are trained to survive in a CBRN environment. The CBRN training staff, IAW ATP-3.8.1 Vol III and IV, must ensure that the correct training package is undertaken by all members of the joint force operating in the JOA.

h. Legal. Legal staff will advise commanders and staff regarding applicable HN, Troop-Contributing Nation (TCN) and international law.

i. Medical. The medical staff's role is particularly important, as initial indication of a CBRN incident, especially of biological incidents, may come from the medical chain. If a CBRN threat is identified, medical staff will be responsible for developing, coordinating and executing timely and appropriate Counter measures and care to counter effects of possible CBRN hazards; in compliance with the given operational priorities and established international and national guidelines. It is important to note these may vary between the different joint force components. Full responsibilities of medical staff are covered in AJMedP-7, Allied Joint Medical Doctrine for Support to CBRN Defensive Operations and AMedP-7.6, Commanders Guidance on Medical Support to CBRN Defensive Operations,, but it is key to highlight that individuals' exposure or potential exposure to CBRN substances is communicated to the commander and subsequently recorded on personal medical records.

j. Civil Military Cooperation (CIMIC). The CIMIC staff is responsible for advising the JFC Commander on the implications of all CBRN defence activities which directly concern relations between the joint force and local government, civil population, IO, Non-Governal Organizations (NGO), and other organisations/ 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.

k. Public Affairs Office (PAO). The PAO staff is responsible for advising the JFC Commander on what 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, PAO staff need to be provided with accurate and timely information about CBRN incidents from commanders and staff. In addition, the PAO staff must be prepared to respond to information and/or misinformation that may be promulgated through the Internet or social media sites.

3.19.3 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 OE. 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 OE requires continual liaison and sharing of information between the joint force, coalition nations, IGO, NGO, regional security, and HN entities.

3.20 Cooperation between NATO and non-NATO authorities

CBRN Defence Comprehensive Approach is used to describe the competencies required to manage CBRN threats and incidents. The policy recognises NATO's approach to conflicts as "the coherent and comprehensive application of various instruments of the Alliance to create the overall effects that will achieve the desired outcome". Specifically it calls for coordinated political, military and civilian measures to prevent proliferation and to protect NATO populations, territory and forces from the effect of a CBRN incident, including recovery measures, should an incident occur.[9]

3.20.1 Though the implementation of the comprehensive approach may vary between the levels of warfare and from one crisis to another, a number of guiding principles apply:

a. The need for proactive engagement between all stake holders, before, during and after a CBRN incident.

b. A cooperative working relationship, liaison, education and the use of a common language are important in a shared understanding.

c. The value of collaborative working based upon mutual trust and a willingness to cooperate - familiarity and information sharing are key.

d. Thinking focused on outcomes and agreed objectives, underpinned where possible by unity of purpose.

3.20.2 As a CBRN hazard could cross international borders, and the consequences of CBRN incident may exceed the capacity of the HN, Allied Forces may be able to provide co-ordination and additional capacity to deal with the incident. This could include establishing a robust HM plan including potential liaison with the affected nation.

3.20.3 The comprehensive approach requires not only a shared situational understanding of the problem but also recognition that sometimes non-NATO authorities may support NATO and conversely on other occasions, NATO will play a supporting role. To add more complexity, this relationship is dynamic and considerable flexibility will be required by all parties, along with robust management of the transition of lead responsibility. Unambiguous LOC are critical in such a context.

[9] MC 0603, NATO Comprehensive CBRN Defence Concept, Annex A. Page A-1.

ANNEX A −CBRN-related Intelligence Support to Planning and Execution of Operations

A01. This annex provides a guide to actions the CBRN defence staff must take, in conjunction with J2 staff, in contribution to the operational level PMESII analysis. CBRN threat assessment is a subset of the overall vulnerability, risk assessment and risk management process carried out for operations 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 adversely affect CBRN defence activities.

a. JIPOE is a continuous process that can identify and confirm potential adversary's capabilities and limitations for weapons and delivery systems; their C2, and release procedures; any indicators of intent to employ CBRN weapons or improvised devices; the governance of CBRN substances; and the maintenance/security of storage sites. CBRN defence contribution to JIPOE includes:

(1) CBRN threat assessment;

(2) Area of operations[10] vulnerability analysis**.**

b. An extremely high percentage of the information required for a CBRN contribution to JIPOE is already held with the joint command areas supporting planning activity for J2, J3, J4, J5, J9 and full spectrum targeting; it just needs to be considered using a CBRN perspective. NATO's CBRN Reachback Element (RBE) can provide support to a deploying or deployed force via the NATO process detailed in ATP-45 and NATO Reachback SOP. The JIPOE process is a staff's (or staffing) tool that helps identify and answer the commander's PIR and is the first step in the JFC OPP.

A02. **Threat Assessment.** The CBRN defence staff needs to be able to contribute to the intelligence cycle by assisting in the evaluation of the composition, disposition, capability and intent of an adversary and/or the possibility of a release of CBRN substances by :

a. Determining if the adversary has a capability by examining industrial and military infrastructure, access to precursor agents, potential storage and dual use facilities;

b. Determining 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 most dangerous scenario;

c. Determining/estimating the adversary's probable nuclear yields in close cooperation with the Nuclear Operations (NUCOPS) Cell;

d. Determining the adversary's tactics for employment;

e. Reviewing ROE and any other legal restrictions;

f. Identifying the capability for delivery.

[10] IAW AJP-2.1 para. 0204.

g. Identifying TIM sites and assessing possible risk to mission:

(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 substances.

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

A03. **Area of Operation.** The CBRN defence staff need to assist the J2 in assessing the areas of operations and interest. An assessment needs to be conducted for the way in which particular characteristics of the environment will affect the impact of a CBRN incident. The CBRN defence staff will need to examine the following from a CBRN perspective (not exhaustive):

a. Terrain;

b. Climate and weather;

c. Population and health;

d. Political/socio-economic;

e. Infrastructure;

f. Security;

g. Industry and standards;

h. Religious and cultural considerations;

i. Civil emergency capabilities.

A04. **CBRN OE Analysis.** The CBRN OE analysis should encompass the following:

a. All adversaries and supporting networks known or suspected of possessing a CBRN capability and their intent or commitment to using it.

b. All current and potential locations of potential adversary CBRN delivery systems.

c. All known and suspected adversarial CBRN capabilities and their storage and production facilities and distribution networks.

d. Evaluate own force vulnerability to CBRN incidents

e. Advanced dual-use technologies and capabilities.

f. Proliferation of CBRN substances, capabilities, expertise, and sensitive technologies.

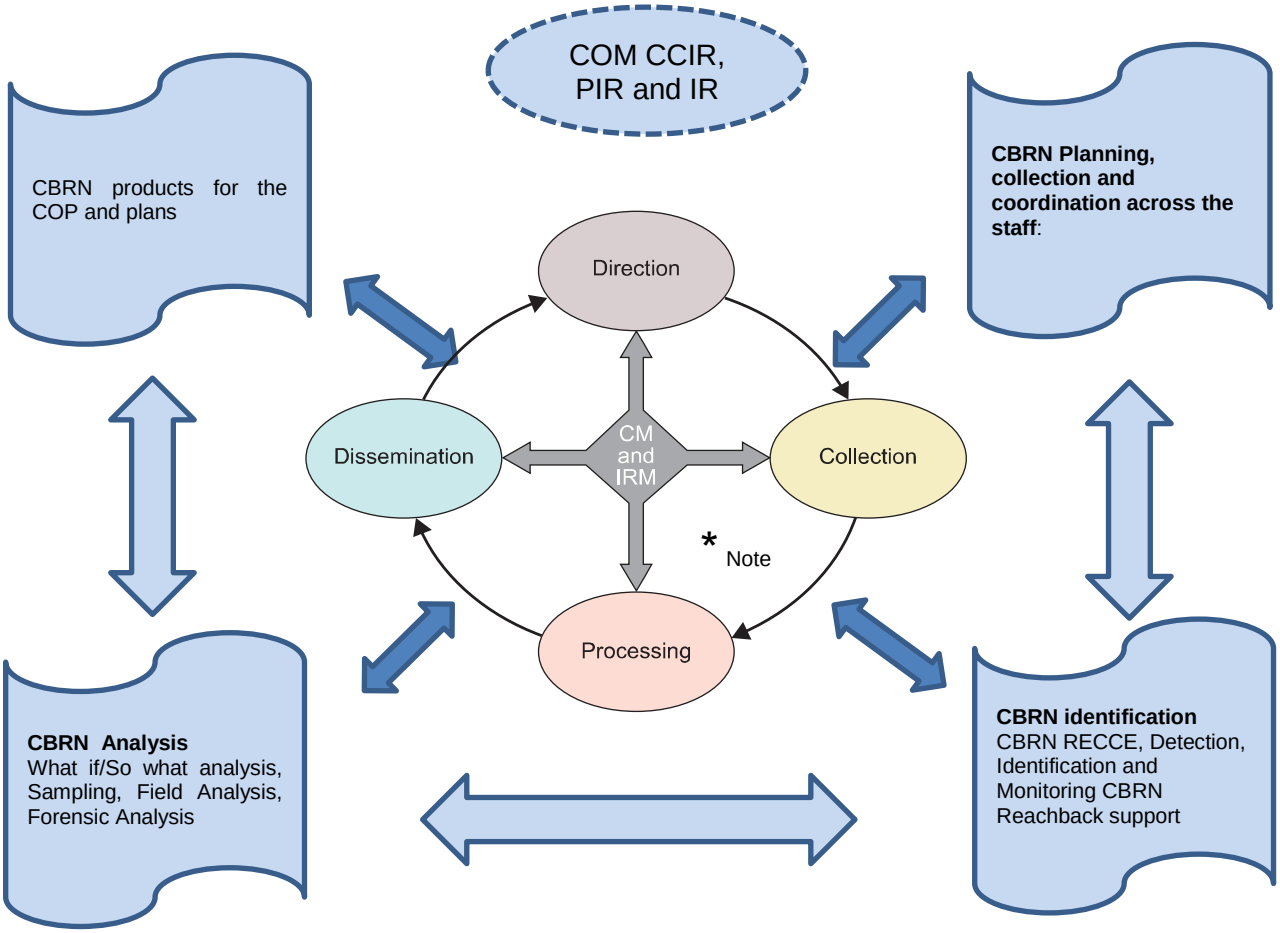
g. Friendly and neutral nations CBRN threats and hazards, to include military and TIM, their storage, management and checks and controls within the OE.

h. Assess HN CM capabilities and establish appropriate leadership engagement.

i. Assessment of the natural biological environment such as the endemic biological agents and the specific factors of epidemic spreading that could hamper the combat effectiveness of the force.

A05. The CBRN contribution to the Intelligence Cycle is illustrated in figure A-1.

CBRN Joint Intelligence Preparation of the Operational Environment



***Note**: Ref.: AJP 2.1 (Chap 3, sect 1. fig 3.1): While the intelligence cycle outwardly appears to be a simple process, in reality it is a complex set of activities comprised of many cycles operating at different levels and speeds. Some tasks overlap and coincide so that they are often conducted concurrently rather than sequentially. In essence, direction can be applied at any stage, not just after dissemination has taken place; equally, collected material can, if the requirement is urgent, be disseminated without being processed with the appropriate caveats. Legend: CM Collection management. IRM Intelligence requirement management*

Figure A-1. CBRN JIPOE

ANNEX B −CBRN Defence Related Risk Management

B01. **General.** CBRN defence related assessments are a part of the operational planning and risk management processes, and should not be done in isolation.

B01.1 **Risk Management.** Risk management integrates the continuous 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 potential impact on mission success. This aims to minimize risk wherever possible, not eliminate it. Risk management consists of choosing the appropriate response to a risk, by selecting one or a combination of the following possibilities: avoidance, transference, mitigation, or acceptance. The risk management process consists of five phases: identify hazards and threats, assess hazards to determine risk, develop controls and measures, implement controls and measures, and supervise and evaluate.

B01.2 **Identify Hazards and Threats**. Using the JIPOE understand the full spectrum threat and assess the probability or likelihood that a CBRN incident caused by that threat will occur. This phase includes an analysis of the mission, listing of hazards and threats, and identification of underlying causes. It is the first step in completing a risk assessment. The aim is to identify CBRN related hazards, including toxic industrial hazards as well as, in close coordination with medical staff, potential environmental and endemic hazards to the force and civilian population. Hazard assessments use the tools of CBRN Modelling and Simulation. Examples of hazards are listed in the AEP-72.

B01.3 **Hazard Assessment (Risk Assessment).** Risk is a function of the value of the asset and is compared to the potential impact of the exploitation of vulnerabilities by threats and hazards. This phase answers the question “What are the odds (probability) of something going wrong and what is the effect or impact (severity)?” The CBRN hazard assessment is integral part of risk management. The effect could be mission failure, injury, or loss due to a threat exploiting vulnerabilities or a hazard.

a. Vulnerability needs to be assessed against CBRN threats. CBRN defence staff in consultation with other FP staff should identify vulnerabilities that could be exploited by threats or hazards and the impact of incidents on the force’s effectiveness and Allied political will, thereby affecting mission success. Vulnerabilities include deficiencies in planning, preparedness, training, awareness, warning, physical security, hardening, redundancy/back up and response capability, but can also include operational constraints imposed through legal and/or national policy.

b. The risk assessment considers four points and should include a prioritisation of the risks to support the decision-making process:

(1) Likelihood that an incident caused by threat or hazard will occur.

(2) Likelihood that a specific vulnerability will be exploited.

(3) 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, that are caused by the degree of impact or severity of the threat.

(4) The proximity of the risk.

B01.4 **Develop Controls and Measures.** What are the potential ways to treat the CBRN risk, and of these, which strikes the best balance between being affordable and effective? Is the remaining risk acceptable? In this phase, controls and measures are developed and analysed as hazards are re-assessed to determine any residual risk.

a. The impact of a risk is a function of the value of the asset and is compared with the likelihood 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.

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

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

(b) Likely. May occur in most circumstances.

(c) Occasional. Could occur at some time.

(d) Seldom. Not expected to occur.

(e) Unlikely. Occurs in exceptional circumstances only.

(2) 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:

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

(b) Critical. Would threaten functional and operational objectives.

(c) Significant. Necessitates adjustment to overall function.

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

b. The combination of impact and probability produces the overall risk level as shown in table B1. The commander 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.

B01.5 **Implement Controls and Measures.** Leaders and staffs need to integrate controls and measures into SOP, written and verbal orders, mission briefings, and staff estimates. This is usually achieved by converting controls into clear and simple execution orders, establishing proper authorities and accountabilities, and providing the necessary support to implement.

B01.6 **Supervise and Evaluate.** Is your plan working? Are changes or updates required? The purpose of phase five of the risk management process is to ensure that risk controls are implemented and enforced to standard and that a feedback mechanism is in place. As with the rest of the risk

management process, supervision and evaluation must occur throughout all phases of an operation or activity.

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

Table B-1 CBRN Defence Risk Analysis

B02. Further Risk Management guidance is given in AJP-3.14.

Intentionally blank

Lexicon

Part I – Acronyms and Abbreviations

AFS	ACO Force's Standards
AJP	Allied Joint Publication
ATP	Allied Tactical Publication
C2	Command and Control
C4I	Command, Control, Communications, Computers and Information
CBRN	Chemical, Biological, Radiological & Nuclear
CIMIC	Civil-Military Cooperation
CIS	Communication and Information Systems
CJTF	Combined Joint Task Force
CM	Consequence Management
COA	Course of Action
COLPRO	Collective Protection
COP	Common Operational Picture
CPOE	Comprehensive Preparation of the Operational Environment
DIM	Detection, Identification & Monitoring
FP	Force Protection
HM	Hazard Management
HN	Host Nation
ICP	Intelligence Collection Plan
IED	Improvised Explosive Device
IGO	Intergovernmental Organization
IO	International Organisation
IPE	Individual Protective Equipment
IRC	Information Related Capabilities
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
ITEP	Individual Training and Education Programme
JCBRND COE	Joint CBRN Defence Centre of Excellence
JFC	Joint Force Commander
JIE	Joint Intelligence Estimate
JIPOE	Joint Intelligence Preparation of the Operational Environment
JISR	Joint Intelligence, Surveillance and Reconnaissance
JLSG	Joint Logistics Support Group
JOA	Joint Operations Area
JTF	Joint Task Force
KM	Knowledge Management
LOC	Lines of Communications
MC	Military Committee

MEDCM	Medical Countermeasures
MIO	Maritime Interdiction Operation
MSA	Maritime Situation Awareness
MSO	Maritime Security Operation
MTEP	Multinational Training and Educational Programme
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organization
NSO	NATO Standardization Office
NTMS	NATO Terminology Management System
NTO	NATO Terminology Office
NUCOPS	Nuclear Operations
OE	Operational Environment
OGA	Other Government Agency
OPP	Operations Planning Process
PAO	Public Affairs Office
PIR	Priority Intelligence Requirements
PMESII	Political, Military, Economic, Social, Information and Infrastructure
PP	Physical Protection
RBE	Reachback Element
ROE	Rules of Engagement
SIBCRA	Sampling & Identification of Biological, Chemical &Radiological Agents
SOF	Special Operations Forces
SOP	Standing Operating Procedures
STRATCOM	Strategic Communications
TCN	Troop-Contributing Nation
TF	Task Force
TIB	Toxic Industrial Biological
TIC	Toxic Industrial Chemical
TIM	Toxic Industrial Material
TIR	Toxic Industrial Radiological
TTP	Tactics, Technics and Procedures
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Disablement
W&R	Warning and Reporting

Part II − Terms and Definitions

attribution
In CBRN defence, an analytical process that uses all information sources for positive identification of the originator of an incident or a threat. (NATO Agreed 2015-04-01)

CBRN defence staff
The group of suitably qualified and experienced personnel capable of collating, fusing and analysing CBRN information and intelligence in order to provide threat assessment and hazard prediction to advise the command on CBRN defence decisions (Not NATO Agreed)

CBRN defence
The plans, procedures and activities intended to contribute to the prevention chemical, biological, radiological and nuclear incidents, to protect forces, territories and populations against, and to assist in recovering from, such incidents and their effects (NATO Agreed 2013-10-31).

CBRN defence comprehensive approach
The coordinated political, military and civilian actions taken to support chemical, biological, radiological and nuclear defence. (NATO Agreed 2013-10-31)

CBRN device
An improvised assembly or system intended to cause the release of CBRN substances. (NATO Agreed 2014-11-20)

CBRN environment
An environment, where there are CBRN threats or hazards. (NATO Agreed 2015-04-01)

CBRN forensics
The scientific methods and techniques used to analyse materials and data in support of a CBRN incident or threat investigation.(NATO Agreed 2014-04-10)

CBRN incident
An occurrence due to the suspected or confirmed presence of CBRN substances, either arising from the intention to use them by an aggressor, or following their intentional or accidental release. (NATO Agreed 2015-04-01)

CBRN reachback
A process by which commanders, their staffs and deployed forces may be provided with timely, coordinated and authoritative advice on chemical, biological, radiological and nuclear issues, drawing upon remote expert sources of information. (NATO Agreed 2015-04-01)

CBRN reconnaissance
A mission undertaken to obtain information by visual observation or other methods, to confirm or deny the presence of CBRN hazards or attacks. It may include gathering information on enemy use of CBRN weapons or devices or on associated hazards, or meteorological data for CBRN hazard prediction. (Not NATO Agreed)

CBRN sampling

The retrieval for analysis of materials that have arisen from a CBRN incident.
Note: When sampling is based on scientific methods and techniques, and is compliant with the chain of custody, it is called forensic sampling. (NATO Agreed 2015-04-01)

CBRN substance
A chemical or biological agent, a toxic industrial material or a radioactive material, in any physical state or form. (NATO Agreed 2014-11-20)

CBRN weapon
A weapon designed and manufactured to cause the release of a chemical or biological agent, or to generate a nuclear burst. (NATO Agreed 2015-04-01)

consequence management
Actions taken to maintain or restore essential services and to lessen the effects of natural or man-made disasters. (NATO Agreed 2012-08-31)

contamination
The deposit, absorption or adsorption of radioactive material or of biological or chemical agents on or by structures, areas, personnel or objects. (NATO Agreed 2006-01-07, currently in review)

hazard management
In CBRN defence, all preparatory and responsive measures taken to mitigate CBRN hazards through avoidance, control of hazard spread, control and management of exposures, decontamination and waste management.(NATO Agreed 2015-04-01)

Multinational Training and Exercise Programme
It is an annual publication aims to develop, schedule, synchronize and publish the approved NATO Military Training and Exercise Programme. Also covers on a period of five years all collective training and exercises, including with non-NATO members.(Not NATO Agreed)

physical protection
The measures and equipment intended to provide protection to personnel and materiel in a CBRN environment. (NATO Agreed 2015-04-01)

sampling and identification of biological, chemical and radiological agents (SIBCRA)
The collection and transportation of materials suspected to contain chemical, biological and radioactive substances and the identification of such substances within the chain of custody in support of the investigation of a CBRN incident. (NATO Agreed 2014-11-20)

toxic industrial material
Any toxic industrial material manufactured, stored, transported, or used in industrial or commercial processes, to include toxic industrial chemicals, toxic industrial radiologicals, and toxic industrial biologicals.(Not NATO Agreed)

weapon of mass destruction
A weapon that is able to cause widespread devastation and loss of life. (NATO Agreed 2014-11-20)

weapon of mass destruction disablement

The operations who aim to systematically locate, secure, characterize, eliminate or dispose WMD, CBRN weapons, CBRN devices and CBRN materials and / or a potential adversary's capability to research, develop, test, produce, stockpile, deploy, or employ such weapons, devices and materials.(Not NATO Agreed)

AJP-3.8(B)(1)