Ministry of Defence

NATO OTAN

Allied Joint Publication-3.14

Allied Joint Doctrine for Force Protection

Edition B Version 1

NATO STANDARD

AJP-3.14

ALLIED JOINT DOCTRINE FOR FORCE PROTECTION

Edition B, Version 1

OCTOBER 2024

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

21 October 2024

1. The enclosed Allied Joint Publication AJP-3.14, Edition B, Version 1, ALLIED JOINT DOCTRINE FOR FORCE PROTECTION, 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 2528.

2. AJP-3.14, Edition B, Version 1, is effective upon receipt and supersedes AJP-3.14, Edition A, Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

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

Thierry POULETTE
Major General, FRA (A)
Director, NATO Standardization Office

Intentionally blank

Allied Joint Publication-3.14

Allied Joint Doctrine for Force Protection

Allied Joint Publication-3.14 (AJP-3.14), Edition B, Version 1,

dated October 2024,

is promulgated as directed by the Chiefs of Staff

Head Doctrine

Intentionally blank

RECORD OF NATIONAL RESERVATIONS

CHAPTER	RECORD OF RESERVATION 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 Documents Database for the complete list of existing reservations.	

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
CAN	1. CBRN DECON - HN or Coalition support is required for large scale or reoccurring events. Additionally, CDA has no ability to provide DECON to aircraft and associated sensitive components. Aircraft DECON capability is under review. 2. CBRN COLPRO - NH or Coalition support required. CDA his limited quantities of deployable COLPRO units for long term use.
FIN	Most elements of Force Protection exists, but due to the comprehensive nature of STANAG 2528 further studies, planning and reorganizing is needed prior to full implementation of the doctrine. In light of this, exact date for full implementation remains open at the moment.
GRC	GRC land forces cannot execute tasks normally incumbent on civilian agencies and organizations, due to caveat deriving from national legislation.
HRV	– Anti-submarine warfare (Annex A, A.2. Tactical Area of Responsibility Control, (11) Defence of Maritime Forces, (b) Anti-submarine warfare), – Naval Mine Countermeasures (MCM) (Annex A, A.2. Tactical Area of Responsibility Control, (11) Defence of Maritime Forces, (c) Naval Mine Countermeasures), – Ballistic Missile Defence (Annex A, A.3. Integrated Air and Missile Defence, (a) Tactical Ballistic Missile Defence), – Maritime Air Defence (middle and long range) (Annex A, A.3. Integrated Air and Missile Defence, (c) Maritime Air Defence), – CBRN defence of ship Annex A, A.4. Chemical Biological, Radiological and Nuclear Defence, (a) Detection, Identification and Monitoring). All mentioned reservations will be until the construction of a new multi-purpose ship that is planned after 2032. In according with the current national legislation, the collect and process the biometric data in the Croatian Armed Forces can be carried out only by authorized Military Police personnel in according with special regulation. Therefore, regarding to national restriction Croatian Armed Forces do not have the authority and the necessary infrastructure to implement the full

	spectrum of activities and tasks to collect and process the biometric data.
HUN	In case of unilaterally planned and conducted operations, Hungary is going to conduct force protection planning in accordance with its own operation planning procedures. In such cases Hungary will take into consideration and apply chapters of the doctrine to the extent possible.
POL	1. Excluding point 1.13 The original wording is not consistent with the AJP-10 Allied Joint Doctrine for Strategic Communication Reference Document. 2. Excluding section 2.5 point C (1) and (2) 3. Excluding Annex A, point A6 a and b Military Engineering of the Polish Armed Forces does not include the management, protection, strenghtening, maintenance and renewal of the infrastructure. Engineering activities are also not responsible for fire protection and constructing encampments
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 Documents Database for the complete list of existing reservations.	

Summary of changes

REVISION OF ALLIED JOINT PUBLICATION

AJP-3.14 Edition B, Version 1

- Reduces redundancies and improves continuity between Allied Joint Publication (AJP)-3.14, *Allied Joint Doctrine for Force Protection* and related documents.
- Updated to reflect changes in the NATO Command Structure and NATO Force Structure.
- Updated to reflect latest policy, doctrine and acknowledged best practice.
- Updated to better reflect the contemporary operating environment and nature of current identified threats and possible future threats.
- Updated to better reflect the latest policy and doctrine on Cyberspace operations and Strategic Communications.
- Now a more generic, less Afghanistan-centric doctrine publication.
- Risk Management updated to reflect latest policy, doctrine and acknowledged best practice.
- Risk Management now discussed in detail in main publication.
- Gender Perspectives in accordance with United Nations Security Council Resolution (UNSCR) 1325, *Resolution on Women, Peace and Security*, incorporated throughout.
- Risk Management Annex removed.
- Annex on categories of Force Protection measures, actions and tasks added.
- Updates terms and definitions to reflect latest status of NATO Term and ongoing terminology changes.

Intentionally blank

TABLE OF CONTENTS

Record of Reservations iii

Summary of Changes vii

Table of Contents ix

Related Documents xii

Preface xvii

Introduction xix

Chapter 1 – Fundamentals of Force Protection

Introduction 1
Definition of Force Protection 1
Force Protection Applicability 1
Force Protection Coordination 2
Force Protection Principles 3
Force Protection Process 4
Force Protection Coordination Areas and Fundamental Elements 4
Cross-Cutting Topics Considerations 7
NATO Policy for the Protection of Civilians 8
NATO Employed Civilians 9
Captured Persons 9
Gender Perspectives in Military Operations 9
Force Protection and Strategic Communications 9

Chapter 2 – Force Protection Responsibilities and Command and Control

Introduction 11
Responsibilities 11
Force Protection Direction and Guidance 12
Continuous Assessment 14
Functional Areas 14
Communication and Information Systems 21
Interface with Host Nations 21
Information Management 21
Alert States 21

Chapter 3 – Force Protection Process

Introduction 23
Threats and Hazards Overview 23
Alert State Management 25

Force Protection Application of Risk Management 27
Specific Considerations – Cyberspace 34
Specific Considerations – Explosive Safety
and Munitions Risk Management 34

Chapter 4 – Force Protection Planning Considerations

Planning Overview 37
Plans and Procedures 38
Developing Force Protection Procedures 38
Planning Measures, Tasks, and Activities 36
Integration of HN and NATO FP Capability 38
Integrated FP Capability 39
Incident Response Planning 40
Recovery Planning 40
Force Manning Planning 40
Strategic Communication Considerations 40
Media and Force Protection 40
Civil-Military Cooperation and Force Protection 41
International and Non-Governmental Organizations 41
NATO International Civilians, Civilian Contractors and Staffs 42
Battlespace Management and Battlespace Spectrum Management 43
Use of Non-Lethal Force in Force Protection 45
Weapon System Support for Force Protection 45
Insider Threat Considerations 45
Terrorism Espionage Subversion Sabotage and Organized Crime 46
Use of Remotely Controlled Systems in Force Protection 46
Force Protection Training 46

Annexes

Annex A - Force Protection Fundamental Elements

Overview A-1
Tactical Area of Responsibility Control A-1
Integrated Air and Missile Defence A-3
Chemical Biological Radiological and Nuclear Defence A-4
Resilience Overview A-6
Military Engineering Support to Force Protection A-8
Consequence Management A-10
Force Health Protection A-11
Security A-12

Annex B – Categories of Force Protection Measures, Actions and Tasks

Procedural B-1
Personnel B-1

Materiel B-1
Infrastructure B-2
Information B-2

Lexicon

Part 1 – Acronyms and Abbreviations LEX-1
Part 2 – Terms and Definitions LEX-5

Intentionally blank

RELATED DOCUMENTS

C-M(2002)49	Security within NATO
C-M(2002)50	Protection Measures for NATO Civil and Military Bodies, Deployed NATO Forces, and Installations (Assets) Against Terrorist Threats
C-M(2007)0004	NATO Policy for Contractors Support to Operations
AC/237-D(2012)0001	NATO Crisis Response System Manual
MC 0133/4	NATO's Operations Planning
MC 0161	NATO Strategic Intelligence Estimate
MC 0296/3	NATO Geospatial Policy
MC 0324/3	The NATO Military Command Structure
MC 0400/4	NATO's Military Strategy Comprehensive Defence and Shared Response
MC 0411/2	NATO Policy on Civil-Military Cooperation and Civil-Military Interaction
MC 0422/3	Information Operations Policy
MC 0458/3	NATO Education, Training, Exercise, and Evaluation Policy
MC 0472	NATO Military Concept for Defence Against Terrorism
MC 0560/2	NATO Policy for Military Engineering
MC 0603	NATO Comprehensive CBRN Defence Concept
MC 0628	Military Committee Policy for Strategic Communication
MC 0656	Military Committee Policy for Force Protection of Alliance Forces
MCM-0009-2015	Military Guidelines on the Prevention of, and Response to, Conflict-Related Sexual and Gender Based Violence

NATO Policy on Preventing and Responding to Sexual Exploitation and Abuse, dated 18 September 2020

PO(2018)0227-AS1, *NATO Policy for the Protection of Civilians*
PO(2018)0235, *NATO Biometrics Framework Policy*

NATOTerm	NATO Glossary of Terms and Definitions
AJP-01	Allied Joint Doctrine
AJP-2	Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security
AJP-2.1	Allied Joint Intelligence Procedures
AJP-2.2	Counter-Intelligence and Security Procedures
AJP-3	Allied Joint Doctrine for the Conduct of Operations
AJP-3.1	Allied Joint Doctrine for Maritime Operations
AJP-3.3	Allied Joint Doctrine for Air and Space Operations
AJP-3.3.1	Allied Joint Doctrine for Counter-Air Operations

AJP-3.3.5	Allied Joint Doctrine for Airspace Control
AJP-3.6	Allied Joint Doctrine for Electronic Warfare
AJP-3.7	Allied Joint Doctrine for Recovery of Personnel in a Hostile Environment
AJP-3.8	Allied Joint Doctrine for Comprehensive Chemical, Biological, Radiological, and Nuclear Defence
AJP-3.10.1	Allied Joint Doctrine for Psychological Operations
AJP-3.10.2	Allied Joint Doctrine for Operations Security and Deception
AJP-3.12	Allied Joint Doctrine for Military Engineering
AJP-3.13	Allied Joint Doctrine for the Deployment and Redeployment of Forces
AJP-3.15	Allied Joint Doctrine for Countering-Improvised Explosive Devices
AJP-3.16	Allied Joint Doctrine for Security Force Assistance (SFA)
AJP-3.18	Allied Joint Doctrine for Explosive Ordnance Disposal Support to Operations
AJP-3.19	Allied Joint Doctrine for Civil Military Cooperation
AJP-3.20	Allied Joint Doctrine for Cyberspace Operations
AJP-3.21	Allied Joint Doctrine for Military Police
AJP-3.22	Allied Joint Doctrine for Stability Policing
AJP-4	Allied Joint Doctrine for Logistics
AJP-4.4	Allied Joint Doctrine for Movement
AJP-4.3	Allied Joint Doctrine for Host-Nation Support
AJP-4.6	Allied Joint Doctrine for the Joint Logistic Support Group
AJP-4.10	Allied Joint Doctrine for Medical Support
AJP-5	Allied Joint Doctrine for the Planning of Operations
AJP-10	Allied Joint Doctrine for Strategic Communications
AJP-10.1	Allied Joint Doctrine for Information Operations
ATP-1, Vol. I	Allied Maritime Tactical Instructions and Procedures
ATP-3.3.6	NATO Force Protection Doctrine for Air Operations
ATP-3.7.2	NATO Military Police Guidance and Procedures
ATP-3.8.1, Vol. I	CBRN Defence on Operations
ATP-3.8.1 Vol. II	Specialist CBRN Defence Capabilities
ATP-3.12.1	Tactical Doctrine for Engineering
ATP-3.12.1.3	Allied Tactical Doctrine for Route and Area Clearance
ATP-3.12.2	Allied Tactical Doctrine for Military Search
ATP-3.16.1	Countering Insider Threats (CIT)
ATP-3.18.1	Allied Tactical Publication for Explosive Ordnance Disposal
ATP-18	Allied Manual of Submarine Operations
ATP-45	Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Operators Manual)
ATP-74	Allied Maritime Force Protection
ATP-94	Harbour Protection

AIntP-10	Technical Exploitation
AIntP-15	Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence
AIntP-17	Joint Intelligence Preparation of the Operating Environment (JIPOE)
AJMedP-3	Allied Joint Medical Doctrine for Medical Intelligence
AJMedP-4	Allied Joint Medical Force Health Protection Doctrine
AJMedP-7	Allied Joint Chemical, Biological, Radiological, and Nuclear (CBRN) Medical Support Doctrine
AMedP-1.10	Medical Aspects in the Management of Major Incident/Mass Casualty Situation
APRP-3.3.7.7	NATO Personnel Recovery Tactics, Techniques and Procedures (TTPs)
APP-34	Testing and Interoperability of Area Access Control Obstacle System

ACO Comprehensive Operations Planning Directive

AC/237-D	NATO Crisis Response System Manual (NCRSM)
AD 65-11	ACO Standing Policy and Procedures for Intelligence Production Management
AD 70-1	ACO Security Directive
AD 80-25	ACO Force Protection Directive

Commercial Publications

International Organization for Standardization (ISO) 31000. Risk Management – Principles and Guidelines

Intentionally blank

PREFACE

1. **Scope**. Allied Joint Publication (AJP)-3.14, Allied Joint Doctrine for Force Protection, is the doctrine for the planning, execution and assessment of Force Protection in the context of the full spectrum of Alliance activity in accordance with Military Committee (MC) 0656 *Policy for the Force Protection of Alliance Forces*. It is subordinate to and refers to Allied Joint Publication (AJP)-3, *Allied Joint Doctrine for the Conduct of Operations* and is part of the Allied Joint Doctrine Architecture.

2. **Purpose**. Although all activity is unique, the planning and conduct of any activity can be approached in a similar manner. The purpose of this publication is to describe the fundamental aspects of Force Protection and provides guidance to commanders and their Staff on the planning and implementation of Force Protection, primarily at the Joint Operational level but, it can be used at any level.

3. **Application**. AJP-3.14 is intended primarily as guidance for North Atlantic Treaty Organization (NATO) commanders and staffs. However, the doctrine is instructive to the planning for activities by a coalition of NATO members, partners and non-NATO nations. It also provides reference for non-military actors[1].

4. **Linkages**. AJP-3.14 is based on the policy set in MC-0656, *Military Committee (MC) Policy for the Force Protection of Alliance Forces*. As a 'Joint Coordinating Function' Force Protection seeks to bring multiple capabilities and disciplines together in a coherent, effective and resource efficient manner in order to Protect against any and all Threats and Hazards. As a coordinating function, Force Protection has linkages across all activity as demonstrated by the plethora of Related Documents listed above.

---

[1] Non-military actors include international organizations, non-governmental organizations (NGOs), the International Red Cross and Red Crescent Movement (ICRC), governments and governmental organizations, local actors/population and private sector actors. For more information about non-military actors see AJP 3.19, *Allied Joint Doctrine for Civil Military Cooperation (CIMIC)*.

Intentionally blank

INTRODUCTION

1. This edition of AJP-3.14 has been updated in accordance with the feedback received from the Nations, the NATO Command Structure, the NATO Force Structure and Centre's of Excellence to reflect the 360-degree nature of contemporary threats[2] and the different scales of effort likely required to provide effective risk-based Force Protection (FP) across the spectrum of conflict.

2. Military capabilities need to be increasingly interconnected to achieve operational objectives and ultimately mission success. Therefore, this document is designed to provide guidance on what consideration *may* be necessary to best protect systems (or systems of systems) that are likely to span different locations (e.g. in order to provide reach-back), jurisdictions and chains of command. Alliance vulnerabilities need to be understood and these vulnerabilities, or weakest links, protected. In the contemporary operating environment, FP needs to encompass the entire system and the networked environment it exists in, not just individual assets or activities.

3. NATO forces need to retain the ability to operate as expeditionary forces that can be engaged in Allied joint operations either within NATO borders or, at range, external to NATO borders.

4. The spectrum of threats and hazards in all domains and environments, including cyberspace and space, is increasing and migrating more quickly. The operating environment may have no discernible front-lines or rear areas and adversaries can be expected to target Allied vulnerabilities anywhere they can be found with an increasingly wide range of peer or near peer capabilities. Security, one of the principles of operations, and protection, delivered through FP (a Joint Function and a fundamental element of which is security) assumes an even higher importance in such an environment. Most if not all counter threats and hazard methodologies captured in earlier versions of this publication are as effective now as they were in the cold war era (when FP was referred to as Survive to Operate), through campaigns in the Balkans and more lately, when adapted for operations within Afghanistan. The key to effective risk-managed FP is Alliance forces and partners, who have institutionalized the core FP principles, methodologies and competencies whilst also having the intellectual agility, at all levels of command, to adapt these principles and methodologies to emerging challenges.

5. This doctrine provides the framework for the comprehensive protection of capabilities. AJP-3.14 *Allied Joint Doctrine for Force Protection* is primarily intended for use by commanders and staffs at the operational level during joint operations, however, it can be used as a reference at any level to include during peacetime, on national territory, and for

---

[2] NATO's key purpose is to ensure the collective defence of Allies, based on a 360-degree approach, against all threats from all directions. To do this, the Alliance fulfils three core tasks: deterrence and defence; crisis prevention and management; and cooperative security.

NATO infrastructure within host nations (HNs), in accordance with Military Committee (MC) 0656 *Policy for the Force Protection of Alliance Forces*.

6. This publication describes the fundamental elements of FP and provides guidance on the planning and implementation of FP, at the joint operational level. FP is complex and starts with situational awareness leading to understanding. The need for FP is ever-present (e.g. the need for Force Health and Safety Protection) although threats and hazards as well as the scale of FP response will vary, dependent on the situation. Specific to deployed activity, FP for Allied joint forces starts with preparation to deploy and continues during deployment, employment, and redeployment. FP covers not only military personnel; it may also include non-military actors (e.g. contractors, civilians, or non-governmental organizations etc.) and their facilities.

7. The importance of FP for NATO-led forces is reflected in the fact that the ability to 'Protect' has been identified as a Main Capability Area (see Lexicon Part 2).

8. FP covers a wide range of protective measures, actions and tasks and uses a spectrum of military capabilities. This publication outlines, for commanders and staffs, the FP principles, methodologies and key considerations as well as describing the main capabilities required. FP must balance the need to preserve combat power and unit capabilities while maximizing freedom of action. A proactive approach to FP will often involve joint action implemented through the co-ordination and synchronization of manoeuvre, joint fires, information and outreach activities. This means the boundaries between FP and joint action will often overlap since deliberate action to eliminate a potential threat becomes integral to FP. Fundamentally, FP activities should enable freedom of action in spite of the presence of threats in the area of operations. It is this dynamic and co-dependent relationship that requires FP to be considered at the outset of the planning process. Finally, this AJP provides the basis for developing FP plans, and for its effective implementation through FP directives, and instructions. It forms the cornerstone of NATO FP doctrine that is essential to the protection of personnel, facilities, materiel, operations, activities, and information, wherever NATO-led forces may be employed. In the context of this publication FP, as one of the joint functions, covers all aspects of protecting the joint force.

9. In the absence of a common threat to all regions, local threat levels may be established to focus FP efforts. NATO-led forces will be particularly vulnerable at the start of any operation when infrastructure is not yet in place and/or information on the situation is incomplete. FP should be based upon effective risk management which requires a commander to articulate their risk attitude. In military operations it is unrealistic to avoid all risks as this will adversely impact the achievement of the mission. Therefore, commanders must balance the risks to the Force against strategic and operational objectives, through analysis of identified threats and hazards. Commanders are ultimately responsible for mitigating those risks to an acceptable level.

10. Effective FP planning and execution fully integrates into the operations planning process from the outset. Commanders should establish FP awareness within their staff and

provide suitable advice and direction to subordinate commands and forces. While specific pre-deployment training will be required, Nations now need to prepare their personnel for immediate employment and to be capable of dealing with any threat or hazard, or combination of multiple threats and hazards, that could conceivably be encountered. Pre-deployment FP training for military and deployable civilian personnel, and, when applicable, contractors and locally employed civilians, is vital to the survivability of forces and the success of any mission. Individual training remains a national responsibility before any assignment to NATO; however, collective training of the Allied joint force, supported by a meaningful evaluation and assessment process, is the responsibility of the NATO commander. Although application of FP is dependent on the nature and circumstances of the threats and hazards as well as the requirements of any activity, FP principles always apply during both peacetime and during the execution of operations.

Intentionally blank

CHAPTER 1

FUNDAMENTALS OF FORCE PROTECTION

1.1. **Introduction**. The resilience of any NATO-led joint force is a principal consideration in strategic and operational planning and decision-making – with implications that extend well beyond the military mission and into issues such as public support and political cohesion. The Alliance and its forces remain vulnerable to a wide variety of threats and hazards. There are hazards inherent in all activities and at all locations, including environmental hazards such as disease and Toxic Industrial Hazards (TIHs). A threat may be described as creating the perception of being in some degree of danger based upon an overall assessment of the situation, taking into account such things as our own and the adversary's capabilities, previous adversary actions and any hostile intentions. External threats and insider threats may also exist in environments considered to be safe, such as home station or base or a forward operating base. Adversaries can be expected to exploit perceived Allied weaknesses and vulnerabilities, which requires a comprehensive and resilient strategy for the protection of forces. Therefore, all military units must be able to defend and protect themselves against prevailing threats and hazards across a range of military activities in order to achieve their tasks[3].

1.2. **Definition of Force Protection**. Force protection (FP) is defined as[4]:

> "*All Measures and means to minimize the vulnerability of personnel, facilities, materiel, operations, and activities from threats and hazards in order to preserve freedom of action and operational effectiveness of the force thereby contributing to mission success*."

1.3. **Force Protection Applicability**. FP is a joint function and essential to all operations[5]. All of the Joint Functions need to be considered by the Joint Force Commander (COM JFC) in determining the capabilities required for each activity. Nations have differing FP philosophies, policies, and priorities. In a multinational force these differences, where possible, should be reconciled taking into consideration national caveats. Then an overall combined joint FP approach should be established, along with appropriate Tactics, Techniques, and Procedures (TTPs), to facilitate unity of effort and enhance the effectiveness and resource efficiency of FP measures.

---

[3] Underpinning the fact that NATO considers Force Protection as an Essential Operational Capability (EOC).
[4] NATOTerm.
[5] The other joint functions are command and control, intelligence, manoeuvre; fires; information, sustainment and Civil-Military Cooperation (CIMIC). While each joint function is unique, they also have related capabilities and tasks that when considered in harmony, provide a solid framework for planning and conducting joint operations. For more on joint functions, see AJP-03, *Allied Joint Doctrine for the Conduct of Operations*.

1.4. **Force Protection Coordination**. Coordination is a FP fundamental during all phases of any activity and each operation. Both vertical and horizontal coordination among strategic, operational and tactical levels of command ensures understanding of the FP roles and responsibilities at each level and promotes synchronized and integrated FP planning, execution and responses both within Headquarters (HQ) and between units. Whilst FP measures, actions and tasks should be integrated and synchronized they should also be implemented based upon risks to the mission and the units themselves. Therefore, individual units may be required to implement different FP measures, tasks and activities within the same operational area. Ideally, there should be a corresponding FP staff assignment within strategic, operational, and tactical level HQ:

a. **Strategic Level Coordination**. At the strategic level, the Allied Command Comprehensive Crisis and Operations Management Centre (CCOMC) provides the necessary staff structure to coordinate FP. An officer from the CCOMC staff is normally designated to provide the commander with strategic FP advice and assessments, and coordinate the input of the staff specialists. If so designated on the commander's staff, an FP officer should incorporate and integrate FP planning into all activities. Subordinate commanders may, in addition to their command responsibilities, also act as advisers to the commander in their respective specialty areas.

b. **Operational Level Coordination**. All operational-level formations, units, and staff contribute to FP through their various disciplines and functions. Because NATO activity will be based on a comprehensive approach, synchronization of FP activities with allies, operational partners, and other actors is essential to ensure maximum effectiveness. This should be achieved through the creation of dedicated FP staffs and a FP Working Group.

c. **Tactical Level Coordination**. At the tactical level, if there is no existing FP structure (*or FP Subject Matter Expert (SME)*) the unit operations officer coordinates FP, in accordance with the commander's intent, with advice from SMEs representing the other joint functions and related capabilities[6]. In each HQ, a senior officer (e.g. Chief of Staff (CoS) level), should be designated as the FP Coordination Authority. This top-level authority will be supported by SMEs from multiple disciplines, including a dedicated FP Staff. Both the Joint Logistics Support Group (JLSG) and the Joint Support and Enabling Command (JSEC) should have incorporated in their Peacetime Establishment (PE) a robust FP organization.

---

[6] These may include, but are not limited to, the Intelligence Officer, Information Operations (Info Ops) Officer, Security Officer, Communication and Information Systems (CIS) Officer, Cyber Operations Officer (or Cyber and Electromagnetic Activities (CEMA) Officer), Information Security (InfoSec) Officer, Medical Officer, Safety Officer, Military Engineering officer, Chemical Biological Radiological and Nuclear (CBRN) Defence Officer, Military Police Officer etc.

1.5. **Force Protection Principles**. The Operations Planning Process (OPP) provides the framework for the identification of the FP requirements and procedures. FP then aims specifically to conserve the combat power of NATO-led forces from emerging threats (including fratricide) and hazards to all its elements. As such, FP should be guided by the following principles:

a. **Joint and Multinational Interoperability**. FP embraces all force components, including civilian support, within and outside the Joint Operations Area (JOA), and addresses all aspects of the threat. FP preserves interoperability and considers the concepts, policies, doctrine, and procedures of Allies, operational partners, and the Host Nation (HN) to ensure interoperability.

b. **Prioritisation**. Commanders are unlikely to have sufficient resources to address all risks to the force. FP balances the conflicting priorities of the need to preserve combat power and unit capabilities while maximizing operational freedom of movement. It is unlikely that the capability will exist to protect all force elements to the same degree. Priority should be given to the protection of friendly forces' centres of gravity, both tangible, such as Lines of Communications (LOC), and intangible, such as operational cohesion or political will as influenced by public opinion. FP requires the application of measures that need to be prioritized, based on the mission and the threat. For more on measures, see **Annex A**.

c. **Flexibility/Agility**. The aim of FP is to counter and mitigate the effects from threats and hazards. FP measures and means should be developed with the capability to respond to rapidly changing threats and hazards, within resource limitations. To be effective, FP requires a core policy that has the flexibility to allow the joint force to develop standards and procedures to meet individual, specific needs. Although all formations, units, and installations play a role in FP, specialized expertise and specialist units may be required for some of the specific FP fundamental elements discussed below.

d. **Defence in Depth**. FP should aim to create successive, mutually supporting layers of FP in all operational domains.

e. **All-Round Protection**. FP measures, actions and tasks should wherever possible provide all-round protection in every domain where there are threats and/or hazards.

f. **Proportionality**. All FP measures, actions and tasks shall be proportionate to the risk itself.

g. **Risk Management**. FP should focus on dynamically controlling the risks and issues emanating from threats and hazards materializing whilst maintaining the ability to operate effectively should they occur.

h. **Unity of Effort and Command**. To be effective FP requires a unity of effort among all actors in order to achieve a common objective. Unity of command ensures that FP roles and responsibilities are clear and unambiguous.

i. **Enabling Operations**. FP measures, actions and tasks should enable not hinder operations.

1.6. **Force Protection Process**. Based on the Force Protection Principles above, the Force Protection Process (for FP Risk Management) consists of the following[7]:

a. Establishing Context.

b. Risk Assessment (*further sub-divided into 3 elements*):

(1) Risk Identification;

(2) Risk Analysis;

(3) Risk Evaluation.

c. Risk Treatment (*further sub-divided into 2 elements*):

(1) Development and Implementation;

(2) Incident Response and Recovery.

d. Monitoring and Review.

e. Communication and Consultation.

1.7. **Force Protection Coordination Areas and Fundamental Elements**[8]

a. **Force Protection Coordination Areas**. The FP coordination areas are Active, Passive, and Recuperation:

(1) **Active**. The active coordination area involves measures, actions and tasks to deter, prevent, nullify, or reduce the effectiveness of the threat's

[7] These processes are described in Chapter 3.

[8] There are a significant number of capabilities that may contribute to the overall Force Protection effect dependent on the threat as identified in the present and perceived as developing in the future. Each of these capability areas has its own doctrine and procedures which are explained within specific subject matter joint and service doctrinal or policy publications.

action and to counter hazards. These are primarily proactive in nature with the core functions of find, fix, strike and exploit to provide protection against the identified threats and hazards before they occur. The employment of individual FP fundamental elements should be in accordance with the mission mandate, Rules of Engagement (ROE), and Standing Operating Procedures (SOPs). It is about seizing the initiative by deterring our adversaries and neutralizing their ability to impact or pose a threat to our activities.

(2) **Passive**. The passive area involves measures, actions and tasks to negate or minimise the effects of the threat's action and hazards on NATO capabilities by making them less vulnerable. Passive measures, tasks, and activities are proactively employed prior to any threat or hazard materializing. A force's ability to survive the effects of such threats and/or hazards should be enhanced by the anticipation of their use/occurrence. Furthermore, effective passive defence preparation is likely to reduce the threat's incentive to act.

(3) **Recuperation**. FP should include plans for NATO-led forces and installations to be able to resume their primary role following the effects of attack, hazards, or disasters. Recuperation covers those measures, actions and tasks necessary for the force to recover, restore essential capabilities, and continue activity, with the minimum of disruption and in the minimum possible time. Measures are therefore pre-planned responses that are reactively employed post-incident.

b. **Force Protection Fundamental Elements**. FP comprises a number of distinct but inter-related fundamental elements, as illustrated in Fig. 1-1, which may contribute to the overall delivery of FP. FP is not necessarily responsible for planning and conducting these fundamental elements activities, but should ensure they are included in and coordinated through the planning process. While some are focused on only one of the coordination areas discussed above, many of the elements can be used to implement FP measures, actions and tasks in any of the three coordination areas. The contribution of these fundamental elements will be determined by the Operating Environment (OE), for instance, by the threat, scale of the operation, climate, civil factors, the composition of the NATO-led force, and the availability of Host-Nation Support or support of local security forces. **Annex A** provides details on how the FP fundamental elements might be used to contribute to providing FP.

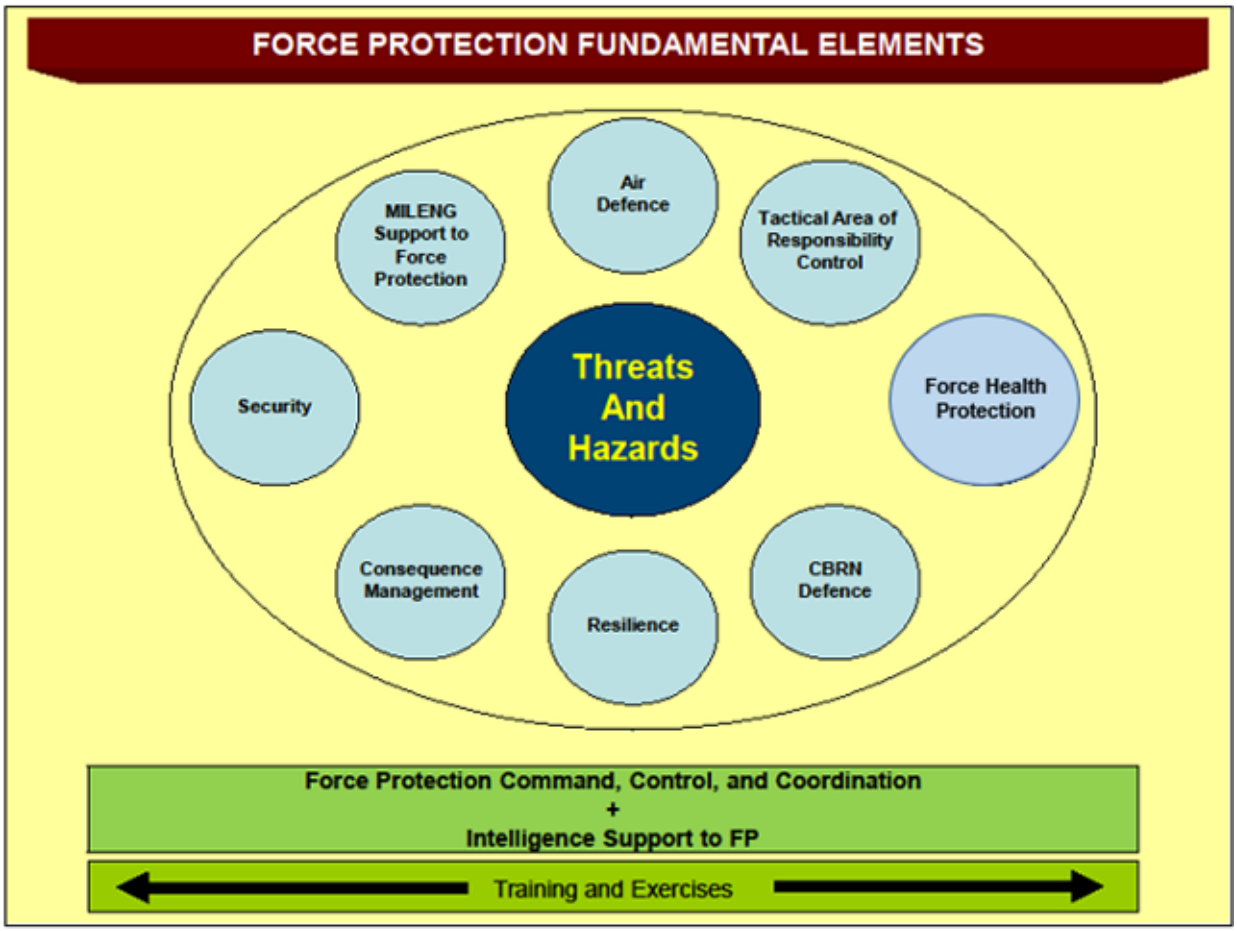

Figure 1-1. Force Protection Fundamental Elements

c. **Force Protection Command, Control, Communication, Coordination, and Integration**. FP measures, actions and tasks are achieved through a combination of individual skills, unit procedures and resources, together with specialist support. FP is ultimately the NATO commander's responsibility. NATO commanders may adopt different options to provide the necessary levels of command, control, communication and coordination to achieve FP measures, actions and tasks. Whatever options are selected, they must be both flexible, to rapidly respond to changes in the FP risk, and resilient, in order to continue to function despite any risk materializing. Where deemed necessary, a dedicated specialist FP cell may be established to address the requirements of the HQ. At all levels, a FP staff and/or FP working group will normally be established to identify and manage the FP risks and consequently plan, execute, coordinate and refine the FP measures, actions and tasks to mitigate those risks. As a minimum, any FP staff should be able to:

(1) Support the planning process and contribute to any prudent military analysis of emerging threats and hazards.

(2) Conduct FP Risk Management on behalf of the commander.

(3) Provide advice to the commander on the implications of identified threats and hazards to their forces in the assigned area of responsibility. Moreover, provide advice and recommendations to the commander on Alert States levels and any associated FP measures, actions and tasks.

(4) Coordinate FP efforts across staff directorates and in conjunction with any subordinate HQ whilst concurrently identifying emerging risks and FP capability shortfalls.

d. **Training**. Whilst individual and specialist FP training is a national responsibility conducted pre-deployment, the collective training and integration of the capabilities provided by the nations remains the responsibility of the Joint Task Force Commander (COM JTF) in the Joint Operations Area (JOA). At the core of FP planning is the requirement of the commander to prioritise, accept, and manage risk. This balance between mission accomplishment and FP risks is covered later in Chapter 3 of this publication.

e. **Intelligence Support to Force Protection**. Intelligence support to FP is required to identify and assess the level of risks to the Force, from threats and hazards, as part of the FP process. NATO commanders should ensure that FP intelligence requirements are identified and prioritized within the overall operations intelligence requirements.

1.8. **Cross-Cutting Topics Considerations**. The attitude of NATO-led forces toward the entire local population (women, men, adolescents and children (girls and boys)) and their authorities could significantly affect how they are regarded and ultimately, the success of an operation. The presence, posture and profile of the NATO-led force is important and members of that force should conduct themselves in a proper manner while considering local culture(s). A gender-balanced force is significant in order to engage with the entire population. Having such a team gives the force an added tool in reaching-out to women, men, girls and boys for the sharing of information and identifying indications and warnings of risks and hazards. Consequently, Allied forces should understand and respect the history, customs, gender conditions, traditions, and current environmental conditions in the operational area. It is essential for the NATO-led force to be aware of their own potential prejudice, for instance a biased view of women only obtaining passive roles in conflict. While at the same time, making sure international law and practices are followed and that any activity adheres to the Women, Peace and Security (WPS) agenda established by the United Nations Security Council Resolution (UNSCR) 1325[9]. In parallel, information on the background and the underlying motives of local stakeholders and interest groups

[9] See also AJP-01 Gender Annex.

gained through amongst other things, human terrain analysis (*to include gender analysis*[10]) and mapping may help to identify potential problem areas and provide opportunities for solving those problems at an early stage. Beyond the indigenous population and authorities, other actors of the International Community involved in a crisis are also of relevance to FP. Such International Organisations (IOs), Non-Governmental Organisations (NGOs) and foreign non-military governmental organisations are a potential source and recipient for sharing indications and warnings of any kind[11].

1.9. **NATO Policy for the Protection of Civilians**[12]. NATO's fulfilment of its responsibilities under this policy is subject to the legal basis for the specific NATO operation, mission or activity, and to the specific Council-approved mandate, without prejudice to FP and collective defence obligations. All feasible measures must be taken to avoid, minimize and mitigate harm to all civilians. When planning and implementing such measures, NATO should give consideration to those groups most vulnerable to violence within the local context. NATO recognizes that, in general, children constitute a particularly vulnerable group during conflict and women are often disproportionately affected by violence. Protection of Civilians (PoC) (persons, objects and services) includes all efforts taken to avoid, minimize and mitigate the negative effects that might arise from NATO and NATO-led military operations on the civilian population and, when applicable, to protect civilians from conflict-related physical violence or threats of physical violence by other actors, including through the establishment of a safe and secure environment. Conflicts are becoming increasingly hybrid in nature, protracted and urban, in such a context any commander must be aware of the increase risks he/she is assuming with regards to the safety of the civilian population. PoC policy requires the establishment of a clear communications and public information strategy to address PoC, it is essential that protection of the NATO Force is considered when developing this, or indeed any other, information or communications strategy[13]. The NATO Policy for the Protection of Civilians and related documents also stress the importance of cementing strong relationship with the Host Nation (HN) through the protection of their cultural property. Such relationship proved to be crucial to build confidence between military forces and HN/local population with consequential positive effects on FP.

1.10. **NATO Employed Civilians**. Commanders have a responsibility to provide FP for NATO-employed civilian contractors and, in certain circumstances, locally employed civilians.

---

[10] For further information see: *NATO Policy on Preventing and Responding to Sexual Exploitation and Abuse*, dated 18 September 2020.
[11] For further information see: MC 411/1, *NATO Civil-Military Cooperation Policy* and AJP-3.19, *Allied Joint Doctrine for Civil-Military Cooperation.*
[12] Endorsed by Heads of State at the NATO Summit in Warsaw in 2016.
[13] For further information see PO(2018)0227-AS1, *Military Committee Concept for the Protection of Civilians*.

1.11. **Captured Persons**. Commanders are responsible for ensuring the protection and respect of captured women, men, girls and boys (including prisoners of war, security internees and criminal detainees). Captured Persons (CPERS) operations are manpower, resource, and security intensive operations of significant importance at all levels and all range of military operations. They are typically tactical operations that have a significant strategic impact. Commanders are ultimately responsible for the care, custody, and control of CPERS and detained personnel. As such, CPERS operations may require intensive FP oversight in conjunction with Military Police, especially during large-scale conflicts where high number of CPERS on the battlefield can impact operations and pose a significant security threat.

1.12 **Gender Perspectives in Military Operations**. A gender perspective must be considered during all stages of NATO operations and missions with men and women participating equally to achieve comprehensive and enduring outcomes. This acknowledges that conflict impacts men, women, boys and girls differently which can have tactical through strategic implications for missions and operations. Developing a comprehensive understanding of the military OE, including the broader civilian setting, is critical to the effectiveness of the armed forces in the field. Furthermore, gender inequalities are often exacerbated during periods of crisis and conflict and, if not addressed, may continue after hostilities and, perpetuating instability. NATO is committed to fully implementing the United Nations Security Council Resolution 1325 on Women, Peace and Security and related Resolutions, across all three of its core tasks as a framework for integrating a gender perspective.

1.13. **FP and Strategic Communications**. Military operations remain inherently dangerous but, in an age of twenty-four-hour news, the Alliance has to be satisfied that its FP posture is sufficiently robust and agile to meet the complex array of threats and hazards. The Alliance must be able to provide evidence of its FP risk decision making processes, in relation to the identified threats and hazards.

Intentionally blank

CHAPTER 2

FORCE PROTECTION RESPONSIBILITIES AND COMMAND AND CONTROL

2.1. **Introduction**. Force Protection (FP) is a core responsibility at every level of command and commanders should balance FP measures, actions and tasks with achieving objectives. Vertical and horizontal coordination among strategic, operational, and tactical levels of command enables each level to implement FP measures, actions and tasks according to the mission and the risks posed by threats and hazards, while providing understanding of the intentions and FP capabilities of each level.

2.2. **Responsibilities**. Specific FP responsibilities are identified below:

a. **Strategic Commanders and Other NATO Military Commanders**. Commanders at the operational and tactical level (i.e. those commanders under NATO Operational Command (OPCOM)) are responsible for the FP of their respective Headquarters and assigned units and personnel. Note that National caveats to the NATO Rules of Engagement (ROE) profile may significantly limit the range of FP measures, tasks, and activities available to the commander.

b. **Supreme Allied Commander Europe**. While authorities may be delegated within the chain of command, the Supreme Allied Commander Europe (SACEUR) remains ultimately responsible and accountable for all aspects of FP for assigned forces.

c. **Troop Contributing Nations**. Troop Contributing Nations (TCNs) for NATO-led operations, both Nations and Partners, are responsible for providing their own FP and for contributing, within means and national caveats, to the wider protection of the NATO-led force to which they are assigned. TCNs should inform the NATO commander (and the Host Nation, where applicable) if their FP concepts, doctrine or capabilities differ significantly from that prescribed by NATO, the assigned commander, or are otherwise deficient. When TCNs are operating with the consent of a Host Nation, Status of Forces Agreements (SOFA), or equivalent agreements may also affect FP arrangements.

d. **Host Nations**. Host Nations (HNs) in concert with NATO, may be required to provide FP for forces located within their sovereign borders in accordance with supplementary agreements, established memoranda of understanding (MOUs), technical arrangements, Operation Plans (OPLANs), contingency

plans, and operation orders (OPORDs)[14]. However, FP will most likely need to take the form of a holistic, whole of Alliance approach for large, strategically important assets[15]. Additionally, HNs may provide, within their means, for FP of the NATO elements and assigned/attached personnel within their respective countries or operational areas, in accordance with the appropriate Status of Forces Agreements (SOFAs). When planning for HN provision or support to FP, commanders must consider HN FP capabilities, availability and standards and make necessary plans and arrangements to mitigate the risks of any shortfalls.

e. **NATO Military Forces**. Risk based FP measures, actions and tasks should be applied to all Headquarters (HQs), units and personnel. FP is a fundamental responsibility of all personnel at all times.

f. **Theatre/Area of Operations Responsibility**. FP responsibilities within any theatre of operations should be clearly assigned prior to an operation commencing. Operational level commanders, advised by FP staffs, should determine and outline FP measures, actions and tasks required to mitigate the FP risks and then assign to / deconflict the FP responsibilities of subordinate HQs and units.

g. **Critical Asset Protection Plan**. A number of staff elements (Theatre Ballistic Missile Defence (TBMD), Cyberspace) develop lists of assets that need to be defended. Combining these lists into a single Critical Asset Protection Plan (CAPP), (*or similarly named document*) is the responsibility of the NATO FP Staffs in the Joint Force HQs.

2.3. Force Protection Direction and Guidance

a. Commanders provide the necessary direction, guidance, and support to focus the staff on anticipated FP risks and any mitigation requirements. Most, but not all, FP fundamental elements already exist in military organizations, as do the Command and Control (C2) functions to implement the overall measures, actions and tasks. All FP fundamental elements should be considered (even though some may be pursuing other aims as a primary function) to achieve effects required for any given FP activity. At the operational level, it is the coordination and integration of all the FP fundamental elements that is vital to provide greater joint coherence. Although the COM JFC is responsible for the FP of the deployed NATO-led force, routine coordination and integration of FP

[14] NATO-led forces may have differing relationships with each Host Nation (HN) for Force Protection (FP). Many forces may reside within the confines of larger military installations, while others are in stand-alone facilities.
[15] See MC-0656, *Military Committee Policy for the Force Protection of Alliance Forces*.

across the joint force is normally conducted centrally by the J-3 operations staff or under a FP C2 element as discussed earlier in Chapter 1.

b. Commanders and staffs at all levels should continuously monitor risk and their own FP posture, and take corrective action when required. In this respect, the risk management process is a continuous one. Commanders define their FP requirements through directives and orders that may include:

(1) Intelligence requirements and priorities to identify threats and hazards.

(2) Risk identification, assessment and prioritization, including acceptance and accountability.

(3) Capabilities and resources.

(4) Manning (*incorporating the requirement for a gender-balanced force*), including readiness states and use of augmentees.

(5) Command and staff responsibilities.

(6) C2 and Communication and Information Systems (CIS).

(7) Warning and reporting requirements.

(8) Plans and procedures.

(9) Training and evaluation including exercises, frequency, and standards.

(10) Legal aspects and national caveats.

(11) Infrastructure protection standards and requirements.

c. FP guidance should be clearly and timely articulated in policies, orders, plans, directives, and instructions. ROE are a method of authorizing certain FP measures. Associated directives and instructions regarding ROE, and other coordinating instructions should be synchronized with FP measures, tasks, and activities. Maximum use should be made of standardized formats for OPORDs, OPLANs, and other forms of directives for disseminating FP specific guidance and information. In addition, the use of synchronization matrices and other decision support tools should be considered to assist in the integration of FP with other operational functions.

d. Ideally, the flow of FP related guidance and information between higher and lower-level HQ should be seamless. A common organizational structure,

doctrine and procedures, and integrated CIS all contribute to enhanced staff effectiveness and efficiency.

2.4. **Continuous Assessment**. Commanders and staff should use all available means and tools to continually assess the FP risks against the risk attitude established by the commander. Inspections, evaluations, assessment surveys and exercise provide the means to identify any shortfalls and deficiencies in the directed FP measures, actions and tasks. Within AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, there is a chapter dedicated to Operations Assessment, and Allied Command Operations (ACO) has a process for conducting FP Advisory Team (FPAT) visits[16]. Accurate and timely reporting and feedback are essential to ensure identified FP deficiencies are resolved. Finally, lessons learned and best practices identified should be shared across the Alliance through FP post operation/post exercise reports, briefings, doctrine development, training, and exercises[17].

2.5. **Functional Areas**. FP should be planned, coordinated, and integrated within the overall activity/operation. Each of the staff functions that support FP should be carefully considered and synchronized by the FP staff.

a. **Intelligence**.[18] The J-2 is responsible for providing accurate, timely, relevant and predictive intelligence to inform the FP process and maintain situational awareness leading to understanding. An integrated Allied joint Threat Assessment (TA) is the first step in the FP risk management process and should be provided by the strategic and operational level J-2 as part of the Operations Planning Process (OPP). Additional localized TAs may need to be conducted across the continuum of competition, where the threat may vary due to the ethnic, religious, cultural, or political affiliations of the civil population. The intelligence requirements for FP will be incorporated in the Intelligence Collection Plan (ICP) and should be written at the lowest classification level possible to provide for the maximum release to the widest range of forces.

b. **Operations**. The J-3[19] acts as the focal point through which the commander directs the conduct of any activity, ensuring unity of effort and the most effective use of resources. The J-3 provides the C2 organization necessary to conduct

---

[16] The Force Protection Advisory Team (FPAT) concept is discussed in detail in AD 80-25, *Allied Command Operations Force Protection Directive*.

[17] Where necessary, FP lessons should be fed into the broader NATO Lessons Identification process through the Joint Allied Lessons Learned Centre (JALLC).

[18] Including all specialized intelligence products, all intelligence collection disciplines and Joint Intelligence, Surveillance and Reconnaissance (JISR). For more detailed information concerning Medical Intelligence see AJP-4.10, *Allied Joint Doctrine for Medical Support*, and AJMedP-3, *Allied Joint Medical Doctrine for Medical Intelligence*.

[19] Note that dependent on situation, the J3 may have a staff officer who has Force Protection (FP) as a secondary responsibility, a dedicated FP staff officer or, an entire FP cell.

FP activity, monitors the current status of forces, and keeps the commander informed about the prevailing situation. The J-3 directs the following functional specialities to ensure effective delivery of FP:

(1) **Security**. Security, in the context of FP, encompasses primarily physical security measures, tasks, and activities necessary to achieve protection against Terrorism, Espionage, Subversion, Sabotage, and Organised Crime (TESSOC), cyber intrusion, insider threats, and direct and indirect attacks on personnel, equipment, installations, and Lines of Communication (LOC). It may also encompass Civil Unrest where this affects NATO's activity. Security covers physical and procedural measures directed at JFC level and integrated in the overall plan, but mainly applied at the local level. The J-3 should ensure that sufficient security forces are available to execute the security plans.

(2) **Cyberspace Operations**. Alliance assets and activity are vulnerable in all operational domains. NATO recognises cyberspace as a separate, discrete operational domain within the information environment and cyber defence now needs to be considered as a framework activity. Like the physical domains, Alliance assets and activity need to be protected within cyberspace and the contents of the Cyber Defended Assets List (CDAL) must be incorporated into the Critical Asset Protection Plan (CAPP) (*or similar list*). Given the complexity of operations within cyberspace, specialist staffs and assets will be required and close coordination between specialist cyberspace staff and FP specialists will be necessary to ensure Alliance freedom of action. See also AJP-3.20, *Allied Joint Doctrine for Cyberspace Operations.*

(3) **Chemical, Biological, Radiological, and Nuclear Defence**. The plans, procedures and activities intended to contribute to the prevention of Chemical, Biological, Radiological and Nuclear (CBRN) incidents, to protect forces, territories and populations against, and to assist in recovering from, such incidents and their effects. The CBRN staff plans and organises the activities to prevent, protect, and recover from adverse effects on operations and personnel resulting from CBRN incidents.[20] These include the use or threatened use of CBRN weapons and devices, the emergence of secondary hazards arising from counter-force targeting, or the release or risk of release of toxic industrial

[20] For more on Chemical, Biological, Radiological and Nuclear (CBRN) Defence, see AJP-3.8, *Allied Joint Doctrine for Comprehensive Chemical, Biological, Radiological, and Nuclear Defence*.

materials into the environment with possible adverse impact on the operation.[21]

(4) **Countering Air and Missile Threats**. Integrated Air and Missile Defence (IAMD) operations protect friendly forces and vital interests from air and missile attacks and include both active and passive measures. The JFC counters air and missile threats to ensure friendly freedom of action, provide protection, and deny enemy freedom of action. Counterair integrates offensive and defensive operations to achieve and maintain the JFC's desired degrees of control of the air and protection by neutralizing or destroying enemy aircraft and missiles, both before and after launch. An enemy's missiles and long-range aircraft can pose significant challenges that require integration of defensive capabilities across the joint force. The COM JFC and Commander Joint Force Air Component (COM JFAC) integrate air and missile defence capabilities and activities in the theatre of operations. The result is integration of offensive counterair attack operations, defensive counterair operations, and other capabilities as required to create the JFC's desired effects. See also AJP-3.3 Allied Joint Doctrine for Air and Space Operations.

(5) **Area Damage Control**. The J-3 coordinates damage control within the Joint Operations Area (JOA) by establishing damage assessment procedures and prioritizing all efforts in order to respond to the incident and minimize its effects. After an incident has been contained, the J-3 coordinates recuperation operations to restore maximum operational capability as quickly as possible. Incident response and recovery and consequence management are conducted in conjunction with area damage control. Incident response and recovery is discussed in Chapter 3 of this publication.

(6) **Electromagnetic Warfare**. The Signals Intelligence and Electromagnetic Warfare (EW) Operation Centre (SEWOC) and EW Coordination Cell (EWCC) are responsible for planning and synchronizing EW in support of the FP plan. The Electromagnetic Battlestaff (EMB) is the mechanism for the staff to coordinate Electromagnetic Operations (EMO) and Electromagnetic Warfare (EW) related activities within the battle rhythm[22].

---

[21] For more information concerning medical support to Chemical, Biological, Radiological and Nuclear (CBRN) Defence see AJP-4.10, *Allied Joint Doctrine for Medical Support* or AJMedP-7*, Allied Joint Chemical, Biological, Radiological, and Nuclear (CBRN) Medical Support Doctrine.*

[22] The Electromagnetic Battlestaff (EMB) encompasses the tasks and duties of Electromagnetic Warfare (EW) staff, Signals Intelligence (SIGINT) staff and Spectrum Management (SM) staff to integrate and harmonize EW, SIGINT and SM activities.

(7) **Secured Access to Space**. Alliance activity requires access to space-based assets. Connectivity to these assets through earth-based facilities needs to be protected. FP staffs will need to understand what space assets/activity are present within their area of responsibility and both plan and allocate sufficient resources in order to maintain Alliance access to space.

(8) **Counter-Improvised Explosive Devices**[23]. Countering-Improvised Explosive Devices (C-IED) is an approach designed to mitigate that the threat of Improvised Explosive Devices (IEDs) that is prevalent worldwide. C-IED is not an end in itself but a multi-strand activity that contributes to a mission end state that will require a comprehensive approach that is multi-agency, joint and multinational. The C-IED approach treats IEDs as a systemic problem and aims to defeat the entire system (the personnel, resources and activities necessary to resource, plan, execute and exploit an IED event). To achieve this C-IED consists of three pillars: Attack the Network; Defeat the Device; and Train the Force[24].

c. **Military Engineering**[25]. Military Engineering (MILENG) is defined as a function in support of operations to shape the physical environment. The MILENG staff will identify tasks and allocate the proper MILENG capabilities in support of FP. MILENG contributes to the overall FP effort by providing advice on:

(1) Appropriate physical protective measures, developing, maintaining, and improving infrastructure (such as hardening and repairing of facilities, and routes);

(2) Enabling or preventing manoeuvre (conducting Explosive Ordnance Disposal (EOD)[26] activities, military search, support to Counter-Improvised Explosive Device (C-IED) activities and emplacing obstacles – Area Access Control);

(3) Supporting the survivability and sustainability of forces (conducting environmental protection measures, fire protection, field camp development and camouflage). Moreover, MILENG staff will provide

[23] For further information see AJP-3.15, *Allied Joint Doctrine for Countering-Improvised Explosive Devices*
[24] The three-pillared approach to Counter-Improvised Explosive Device (C-IED) is a practical example of a FP system that addresses multiple facets of a specific threat. A similar approach could be used to mitigate other complex threats whether related to an explosive threat or otherwise.
[25] See AJP-3.12, *Allied Joint Doctrine for Military Engineering.*
[26] For more information, see AJP-3.18, *Allied Joint Doctrine for Explosive Ordnance Disposal Support to Operations*.

advice on protective measures required to mitigate the effects caused by adverse natural hazards.

d. **Provost Marshal**. The Provost Marshal is the senior Military Police (MP) officer responsible for coordinating all police activities and provision of specialist advice to the commander and staff. MP (inclusive of gendarmerie-type forces) conduct five functions - mobility support, security, detention, police and stability policing[27]. The Provost Marshal may assist in developing and coordinating the execution of FP measures by MP units, such as security of critical sites, base and installation security, port (Air/Sea) security, rail security, and personnel security. The Provost Marshal also receives information from MP units regarding criminal activity, vulnerability assessment of installations, and is a key advisor on the execution of detention operations[28].

e. **Logistics**. At the operational level, the J-3, in close coordination with the J-4 and the FP Subject Matter Expert (SME) of the Joint Logistic Support Group[29] Headquarters (JLSG HQ), should coordinate FP requirements for logistic forces and facilities, as well as providing the necessary support to satisfy the needs of all FP measures, tasks, and activities. The JLSG HQ will usually establish logistic installations and facilities (the Joint Logistic Support Network (JLSN)) that will require a robust FP organization including assigned/subordinated FP assets. COM JLSG will be responsible for the FP for designated JLSG nodes within the JLSN as agreed during the OPP and as directed by COM JTF. Other FP requirements must be coordinated between the JLSG and the components[30]. FP staff located in the JLSG HQ are responsible for all FP assets subordinated to JLSG HQ. One feature of the modern non-linear, non-contiguous operations area is the absence of any relatively safe rear area. For the coordination of Rear Area Security NATO has set up the Joint Support and Enabling Command (JSEC). The JSEC FP branch coordinates all FP related issues in close cooperation with the JLSG FP cell.

f. **Contracting Authority**. A theatre head of contract, as part of the JLSG, is required to ensure the contracts with civilian companies providing logistics support directly to NATO and Nations meet FP requirements. The J-8 is

---

[27] Stability policing activities are conducted with the aim of establishing a safe and secure environment, restoring public order and security, and establishing the conditions for meeting longer term needs with respect to governance and development (in particular through security sector reform). This can include both the re-establishment of law and order and reinforcing the Rule of Law (police, courts, corrections, etc.). Under a comprehensive approach, a combination of military and non-military actors, such as indigenous and international police forces, could be employed to achieve this goal. More detailed information as to Stability Policing (SP) tasks and actors can be found within AJP 3.22, *Allied Joint Doctrine for Stability Policing*.

[28] For more on the Provost Marshall and military police functions, see AJP-3.21, *Allied Joint Doctrine for Military Police* and ATP-3.7.2, *NATO Military Police Guidance and Procedures*.

[29] See also AJP-4.6, *Allied Joint Doctrine for the Joint Logistic Support Group*.

[30] See also AJP3.13, *Allied Joint Doctrine for the Deployment of Forces.*

responsible for the necessary budget and financial rules and regulations to conclude such contracts.

g. **Medical**.[31] The medical advisor, supported by medical staff, advises the commander on any medical implications of their actions or decisions and any health- related issues affecting the force or operation. The medical advisor/medical director will determine and implement the appropriate medical support requirements for the operation. The medical staff will provide a SME to support the FP staff. This will ensure the coordination of FP and medical activity.

h. **Plans**. Although planning is normally a function of the J-5 or J-3/5, the FP officer, if assigned to the commander's staff, should be part of the planning team so that FP planning can be incorporated and integrated into all plans. Force composition and organization should reflect the required FP fundamental elements that are needed to implement the operation plan. The J-5 or J-3/5 staff assists the commander in preparing OPLANs and planning for future operations. The J-5 synchronizes planning efforts within the staff with all other relevant functional specialties, and coordinates with higher, subordinate, and adjacent commands, as well as civil authorities. For more on planning, see Chapter 4.

i. **Civil-Military Cooperation**. The Civil Military Cooperation[32] (CIMIC) staff establish and maintain cooperation with the civilian population and institutions such as national and local governments, International Organizations (IOs), and Non-Governmental Organizations (NGOs). By engaging non-military actors, commanders are able to encourage collaborative analysis, integrated planning and interaction in the JOA, thereby supporting unity of purpose and effort. From a FP perspective, a balance must be struck between accessibility to military facilities for civil actors and Operations Security (OPSEC). Note also that civilians with whom the joint force will deal are likely to pursue their own agenda and may view cooperation with the Joint Force as jeopardizing their own independence. CIMIC activities might have an effect on the general threat to forces and thus the FP posture level; this is further discussed in Chapter 4.

j. **Safety Officer.** The Safety Officer advises on all safety matters and providing safety (*including occupational health and safety*) input to the J-3 Force Protection Assessment and the risk management process.

---

[31] For more information see AJP-4.10, *Allied Joint Doctrine for Medical Support*, and AJMedP-4, *Allied Joint Medical Force Health Protection Doctrine*.

[32] For further information see: MC 411, NATO Civil-Military Cooperation Policy and AJP-3.19, Allied Joint Doctrine for Civil-Military Cooperation.

k. **Explosive Safety Officer**. NATO operational missions often involve the use of munitions. Munitions and munition-related processes present a significant, inherent risk and potential consequences include loss of personnel and assets, mission degradation, and political implications. NATO Explosives Safety and Munitions Risk Management (ESMRM) policy requires that munitions used during NATO operations comply with NATO explosives safety requirements. When those requirements cannot be met, the conduct of a Risk Assessment is required to identify munitions-related risks in support of the NATO commander's risk decision. The Explosive Safety Officer (ESO) provides explosives safety management and oversight of the commander's ESMRM program.

l. **Strategic Communications**[33].

(1) **Information Operations (Info Ops)**. Info Ops[34] staff elements analyze, plan, assess and integrate information activities to create desired effects in support of FP. Info Ops leads the overall military counter-propaganda effort.

(2) **Psychological Operations** (**PsyOps)**. PsyOps can make a significant contribution to the protection of Allied Forces. Conversely, ill-conceived PsyOps activity can have an adverse or negative impact on FP. Therefore, close coordination between FP and PsyOps staffs at all levels is essential[35].

(3) **Public Affairs**[36]. Dissemination of information relating to FP measures is necessary to reinforce their application. The Public Affairs Officer (PAO) (through the Director of Communications) is responsible to the commander for the planning and execution of military public affairs activities, including media, internal information and community relations. Specific rules related to the media, issued by the appropriate command authority, must be disseminated. PA will play a major role in the event of a significant FP incident/failure.

m. **Legal Advisor**. The legal advisor advises the commander on legal issues affecting the conduct of the operation including those related to FP. JFC plans and policies are reviewed to ensure compliance with international law, local law, SOFAs, and Military Committee policy as they relate to the use of contracted

---

[33] Strategic Communications (StratCom), see also Chapter 1, Paragraph 1.11 and MC 0656, *MC Policy for the FP of Alliance Forces*.
[34] See AJP-10.1, *Allied Joint Doctrine for Information Operations*, for further guidance.
[35] For further detail on the conduct of Psychological Operations (PsyOps) see AJP-3.10.1, *Allied Joint Doctrine for Psychological Operations (PsyOps).* Note that this document is likely to be renumbered to AJP-10.2.
[36] To be conducted in accordance with AJP-10, *Allied Joint Doctrine for Strategic Communications.*

support. Specific concerns include the legal status of NATO and third country national contractor personnel hired outside of the operational area as they relate to FP measures, actions and tasks.

n. **Other Special Staff**. Other members of the special staff including the Finance Officer, Political Advisor, Cultural Advisor, and Gender Advisor[37] should be involved in FP planning. They can provide counsel on specific FP implications in their respective areas of expertise.

2.6. **Communication and Information Systems**. Effective C2 is directly dependent upon available/survivable communications and information, and the availability of reliable as well as resilient supporting CIS. In addition to physical attacks against CIS and facilities, CIS are susceptible to denial of service, espionage, electromagnetic warfare and attacks in or through cyberspace. Commanders should develop and implement robust defence and protection measures to safeguard their CIS and ensure the confidentiality, integrity, and availability of their CIS and any data stored or processed within it

2.7. **Interface with Host Nations**. NATO-led forces may have differing relationships with each HN for FP. Many forces may reside within the confines of larger military installations, while others are in stand-alone facilities. Commanders should establish liaison with local military and civil authorities, particularly where FP is a shared task between the commands and the HN, as detailed in the SOFA/MOU.

2.8. **Information Management**. Information Management is an important enabler in support of FP. The purpose of information management is to provide commanders and staffs at all levels with timely and accurate information about the FP situation so that mitigating measures, actions and tasks can be implemented. Information Management should make full use of existing information management procedures and processes[38].

2.9. **Alert States**. NATO intelligence and security organizations are responsible for assessing the threat and for advising on the necessary threat-driven alert state; however, it remains the commander's operational responsibility to determine the protective measures to be adopted. The strategic commander directs the alert states for all NATO forces within the area of operations or joint operational area. Subordinate commanders may subsequently use their discretion in imposing heightened security measures for each alert state; however, lower alert states may not be applied without specific approval from higher authority. The need to maintain a balanced approach to FP within each NATO region or command may dictate that commanders establish corresponding alert states throughout their operational areas. While the potential for

---

[37] See Bi-SC 40-01 for description of the role of Gender Advisor (GENAD) and responsibilities under United Nations Security Council Resolution (UNSCR) 1325.
[38] E.g. Chemical, Biological, Radiological and Nuclear (CBRN) warning and reporting (W&R)

conflicting alert states exists, commands should strive to adhere to NATO-directed alert states and coordinate the measures with adjacent commands where necessary.[39]

[39] See AC/237-D, *NATO Crisis Response System Manual* (NCRSM) and AJP-2.2, *Counter-Intelligence and Security Procedures* for further information on alert states.

CHAPTER 3

FORCE PROTECTION PROCESS

3.1. **Introduction**. NATO Force Protection (FP) utilizes the risk management process which is an integral element of the Operations Planning Process (OPP) as described in both AJPs 3 and 5. This enables commanders and staffs to manage FP risks. The risk management process requires the identification and analysis of the threats and hazard to the force and an assessment of the force's vulnerability to those threats and hazards, in order to identify the level of risk. An understanding of emerging FP risks enables the commander and staffs to make informed decisions on whether measures, tasks and activities are required to treat the risks to a level which is acceptable to the commander.

3.2. **Threats and Hazards Overview**. Threats and hazards posing risks to the Alliance and its forces form part of the day-to-day Operating Environment (OE). FP should be logical, comprehensive and effective to minimize the vulnerabilities of personnel, materiel, infrastructure, and information in peacetime, during training and exercises, and while engaged in operations. Forces should be able to defend themselves from all forms of attack and protect themselves from hazards. NATO-led forces, including supporting forces, need to constantly reassess all aspects of their FP.

a. **Threat Environments**[40]. In the absence of a common threat to all regions, local threat assessments will help focus FP efforts. Threats may range from mental threats[41], lawlessness, terrorism, insurgency, and insider threats, through developing aggressor nations to major opposing forces. The terrorist threat may involve a full spectrum of activities ranging from intelligence gathering and kidnapping to large-scale mass-casualty attacks. The Alliance will need to be able to deploy the necessary countermeasures in order to prevent, protect and recover in case of Chemical, Biological, Radiological and Nuclear (CBRN) incidents. Both conventional as well as unconventional threats should be considered by commanders and staffs when planning and implementing FP measures, effects, actions and tasks. NATO-led forces face an increased vulnerability to unconventional threats as well, including those conducted in cyberspace. The potential threat may be described in terms of five generic environments.

---

[40] For more on threat levels, see AD 65-11, *Allied Command Operations* (*ACO) Standing Policy and Procedures for Intelligence Production Management*.
[41] For the purpose of this publication, 'Mental Threats' are defined within the Lexicon – Part 2.

(1) **Negligible Threat Environment**. There is no known entity with the capability and intention of conducting adverse actions against NATO interests in the country or location of current operations.

(2) **Low Threat Environment**. The low threat environment recognizes that a general threat may exist and envisions an inherent risk of peacetime incidents, such as accidents, crime, disease, and fire, as well as increased threats which could include lawlessness, sabotage, and other irregular or asymmetric threats. Within a low threat environment, the possibility of air and missile attack may be extremely remote. An actor has been identified who may possess either the capability or intention of hostile action against NATO forces or individuals. Although possible, there are no specific indications of use of CBRN materials, weapons and devices. Toxic Industrial Material (TIM) release is possible; although infrastructure[42] and security levels are robust. The possible use of explosive ordnance (including IEDs) should be taken into account.

(3) **Medium Threat Environment**. Recognizes that there are indications of hostile intentions based on intelligence without concrete information on the specific nature, target, or timing established. Adversary propaganda portrays NATO in a generally negative light and attempts to capitalize on any operational setbacks. Forward NATO formations and vital facilities could face both conventional and unconventional threats across the area of operations. An actor has been identified as possessing conventional and/or CBRN capabilities with possible intention of targeting NATO forces or individuals. There is an increasing risk of TIM release due to a decay of industrial infrastructure and/or a degradation of the security of industrial infrastructure. Enemy use of IEDs may be a major concern.

(4) **High Threat Environment**. Recognizes that a hostile act against members of the international community, including NATO is likely based on intelligence. Adversary propaganda likely targets audiences in the area of operations and TCNs alike and may be increasing in its intensity. Specific timings and targets have not been identified. An actor has been identified possessing conventional and/or CBRN capabilities with probable intentions of targeting NATO forces or individuals to include use of CBRN materials, weapons and devices and will likely attempt use them in the near term. Release of TIM may occur with little additional warning due to weakness of industrial infrastructure and/or insufficient security of industrial infrastructure. Although enemy employment of CBRN weapons and devices could be low, the risks posed by

[42] In this context the term infrastructure comprises industrial installations, storage sites, transportation networks, pipelines, medical research and educational facilities.

environmental hazards and CBRN incidents exists. Enemy use of IEDs is a major concern.

(5). **Critical Threat Environment**. Recognizes that a hostile act against members of the international community, including NATO is imminent or has occurred. Adversaries will not only attempt to communicate to target audiences in the area of operations, but also to audiences in NATO and non-NATO contributing nation to discredit HN and NATO-led forces, capabilities, and justification for action. Critical assets such as air and sea ports of debarkation, C2 facilities, and key personnel may be targeted. An actor has been identified as possessing conventional and/or CBRN weapons and devices with clear intentions to use them within a specific time frame and/or against a specific target. There is an immediate risk of a CBRN attack by state, non-state or faction within a state actor and/or an immediate risk of release of a CBRN substance, without warning, due to damage to industrial infrastructure and/or a lack of security of industrial infrastructure. Enemy use of IEDs remains a major concern.

b. **Hazards**[43]. The nature of the Alliance is such that it may be called upon to respond to natural disasters (e.g. earthquake, tsunami, drought, fire, hurricane etc.) or disease epidemic/pandemic. In addition, natural disasters may occur in a region where NATO is conducting military operations. In both cases, natural disasters may lead to man-made disasters; a well-known example of such (11 March 2011) would be the Fukushima Daiichi Nuclear Power Plant in Okuma, Japan. In this example an earthquake caused a tsunami which in turn, flooded the pumps providing cooling to the reactors and caused nuclear meltdowns, hydrogen-air explosions and the release of radioactive material. Weather, climate, altitude, terrain, vegetation, animals and pests, food and water sources, sanitation, communicable diseases, noise, psychological and physical stressors, biological agents, natural and synthetic chemicals, particulates and interaction with the local population (e.g. sexually transmitted diseases) all present hazards to personnel (military and civilian) whilst engaged in NATO activity. It is also worthy of note that hostile activity may, either as an intended or unintended consequence, create a hazard if adversary activity causes an incident such as a release of a Toxic Industrial Material (TIM).

3.3. **Alert State Management**. The strategic commander will normally direct the Alert State to be implemented (see also Paragraph 2.9). The Alert State message will usually direct those Alert Measures that are to be implemented by subordinate commands.

---

[43] This section and indeed this document only recognizes the consequences of Hazard as they affect Force Protection (FP). Root Cause Analysis may enable commanders to better categorize, prioritize and tailor FP measures.

Subordinate commands are to implement those Alert Measures as directed by the strategic commander and can also choose if the situation requires it within their command, implement further Alert Measures and even declare a higher Alert State. The principle at all times is that subordinate commanders cannot reduce the Alert State or choose not to implement mandated Alert Measures but, they may raise the Alert State or increase Alert Measures locally. If a local commander for whatever reason is unable to implement the Alert State and any associated Alert Measure(s), this is to be immediately communicated up the chain of command with an explanation of the local situation. Note that Alert States and Measures should be considered dynamic in that they can rise and fall/increase and decrease over time. In addition, it should be noted that maintaining a high Alert State and multiple Alert Measures for a protracted period of time will likely reduce their effectiveness due to complacency, particularly if there is no, or only very limited adversary action and/or such action is very geographically isolated. Finally, when considering the issue of Alert States and associated Alert Measures, it should be remembered that these will need to be managed across the continuum of competition from Base Line Activities and Current Operations (BACO), through the full spectrum of conflict.

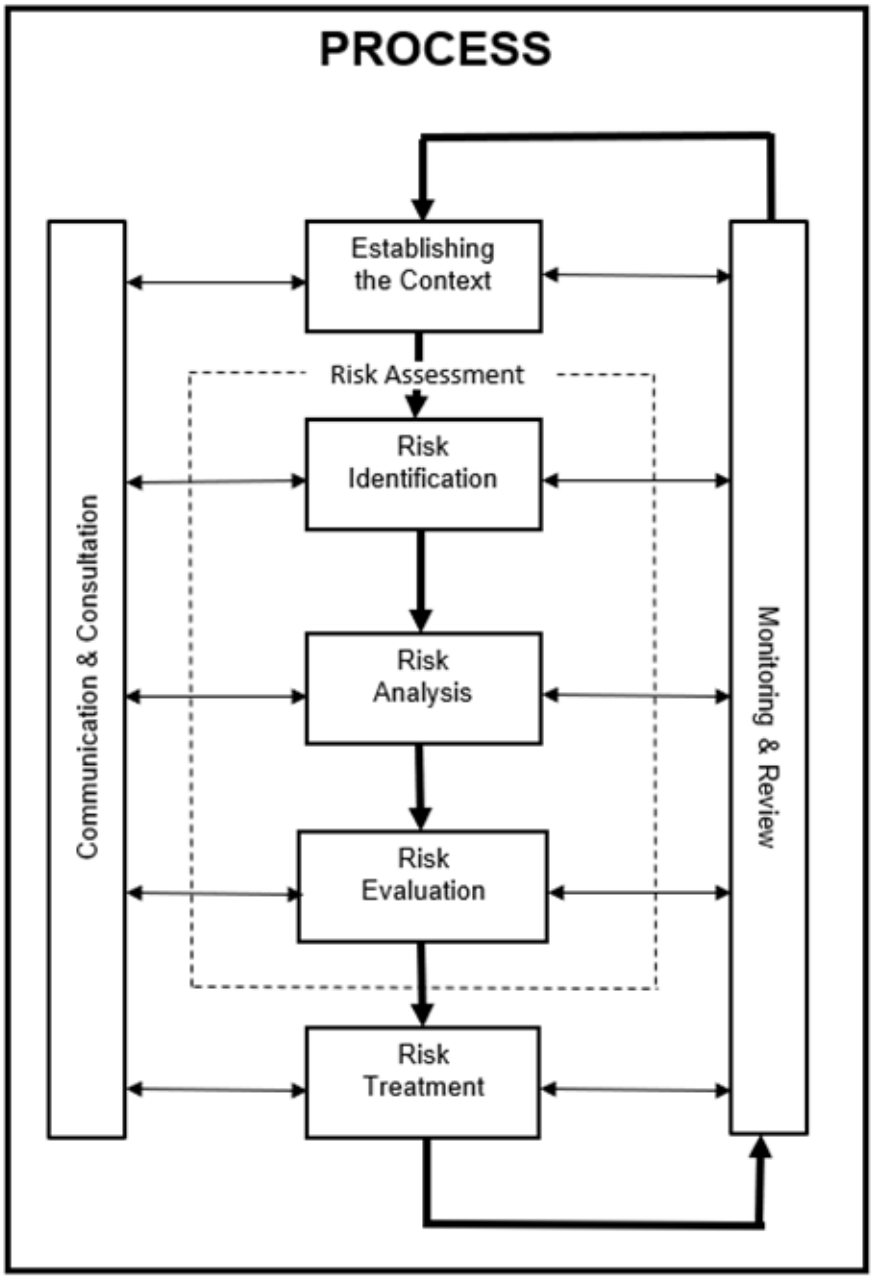

Figure 3-1. Risk Management Process as applied to FP
(*formerly called the 'Force Protection Model'*)

3.4. **Force Protection Application of Risk Management**. The function of FP is to treat the risks posed by threats and hazards to a level that is acceptable to the commander. The Risk Management Process provides FP staff and commanders at all levels with a logical process aimed at identifying and implementing measures, actions and tasks, as well as the ability to effectively respond to incidents should they occur. It also

provides a mechanism for the continuous review of FP activity. Specific steps in the process are below:

a. **Establishing Context (Operations Planning Process)**. As part of the Operations Planning Process (OPP), it is essential that FP staffs understand the context of the activity and what must be done for mission success, so that they can subsequently identify the FP risks[44]. It is paramount, therefore, that the FP staffs are present and contribute throughout the entire OPP.

b. **Risk Assessment**.

(1) **Risk Identification**. The Aim of this step is to generate a comprehensive list of FP risks based on those events that might create, enhance, prevent, degrade, accelerate or delay achieving objectives. Conducted in accordance with AIntP-17, *Joint Intelligence Preparation of the Operating Environment (JIPOE)* contributes to FP risk identification and therefore, the FP staff should participate in the JIPOE process[45].

(2) **Risk Analysis**.

i. **Criticality Assessment**[46]. The criticality assessment involves the identification of those assets and capabilities that are critical to achieving mission success. They are drawn from the mission statement, mission analysis, tasks, constraints, restraints, assumptions and the Course of Action (COA) selected in the OPP[47]. A criticality assessment is a valuation and inventory, both quantitative and qualitative, of assets. These assets include personnel, materiel, facilities, information, and activities that if divulged, lost, injured, corrupted, or damaged, would jeopardize the success of the mission. The assets are assessed in terms of importance, effect and recoverability, and prioritized in terms of criticality to the mission. Concerns should be addressed from the point of view of degradation of asset confidentiality, availability, integrity, and value. The critical asset assessment identifies the impact should the risk materialize. It also prioritizes the assets which require a threat, hazard and vulnerability assessment. Assets critical to the mission should be prioritized

[44] This might also extend to confirming roles within Force Protection (FP) Risk Management (Risk Owner, Risk Manager, Risk Advisor etc.).
[45] See also AJP-2.1, *Allied Joint Intelligence Procedures*.
[46] For more on criticality, threat, and vulnerability assessments, see Allied Command Operations (ACO) Force Protection Directive AD 80-25.
[47] This is not an exhaustive list and other factors may require consideration.

and combined into a single list by the FP staffs.

ii. **Threat and Hazard Assessment**. MC 161, *NATO Strategic Intelligence Estimate* is the basic intelligence guidance that provides the general Threat Assessment (TA) framework.[48] Such assessments, complemented by current intelligence (to include Counter-Intelligence (CI) and indications and warnings) and law enforcement assessments, allow commanders at all levels to assess any threats and hazards within their respective operational areas and therefore focus the direction of FP measures, effects, actions and tasks. Note that commanders at all levels must understand where NATO's Centre(s) of Gravity lie and the tactics that any adversaries will use to target the Centre(s) of Gravity. NATO Headquarters, the Strategic Commands, and subordinate commands analyze and disseminate threat information and make local TAs available to all commands within their operational areas and areas of interest.

FP uses a risk management process incorporating an assessment of the threat. A TA is the intelligence assessment of threats and operational hazards to Allied assets in a defined geographic location (country or region). TAs will determine the capabilities and intentions of an identified individual, group or organization and whether they are likely to carry out the defined threat. A TA is part of the intelligence process that supports the threat warning process and risk management decisions. An overall integrated TA is required from the intelligence directorate (J-2), in coordination with the operations directorate (J-3), plans directorate (J-5), and Civil-Military Cooperation (CIMIC) (J-9) directorate, as one of the intelligence products provided in accordance with the OPP. Additional localized TAs will need to be conducted, particularly in Non-Article 5 Crisis Response Operations (NA5CRO), that consider Terrorism, Espionage, Sabotage, Subversion and Organized Crime (TESSOC), insider threats, cyberspace operations, environmental hazards, the ethnic or political

[48] Military Committee (MC) 161, *NATO Strategic Intelligence Estimate*, provides NATO-agreed intelligence on threats/risks faced by the Alliance. MC 161, together with MC 400/4, *NATO's Military Strategy Comprehensive Defence and Shared Response*, and MC 0590, *NATO Chemical, Biological, Radiological and Nuclear (CBRN) Reach Back and Fusion Concept*, along with other supporting NATO MC assessments, incorporate developing assessments on terrorism and Chemical, Biological, Radiological and Nuclear (CBRN) hazards and incidents.

affiliations of the population, and other cultural and historic concerns that may impact friendly operations.

The TA identifies known adversaries and enemies along with their capabilities, most likely and most dangerous courses of action, and their overall intentions. The threat analysis includes different assessments as described in AJP-2.

The TA should address the full range of threats and attack possibilities and identify likely weapons and delivery tactics. Specific attention should be paid to any emerging threats (e.g., current proliferation of Unmanned Systems, in all domains, which can either be used as weapons, weapon delivery systems or surveillance platforms).

The Intelligence Collection Plan (ICP), which is based on the commander's Critical Information Requirements (CCIRs)[49] and Priority Intelligence Requirements (PIRs), is prepared by the J-2 or the appropriate command intelligence staff. It will reflect the FP intelligence requirements with consideration of specific capabilities offered by intelligence collection assets (e.g., human intelligence may offer unique insights on the threat intent and have to be exploited accordingly). The ICP is continuously monitored and adjusted as the situation and threat changes and is conducted within legally established parameters for collection. Analysts will utilize the collected data, information, JISR results and intelligence (acquired from military, security, political, social, CI, and criminal intelligence sources and agencies etc.) to create fused intelligence products to satisfy the respective FP intelligence requirements.

iii. **Hazards**. The concept of the TA as described above must also be extended to include an assessment of hazards both environmental and occupational that could have an impact on the mission. Further identification and assessment of hazards might also be extracted from the Joint Intelligence Preparation of the Operating Environment (JIPOE). Irrespective of whether it is the TA or a separate Hazard Assessment that is used as the vehicle to assess hazards, all identifiable hazards should be considered as part of the FP process.

---

[49] For more information on Commander's Critical Information Requirements (CCIRs) see AJP-2 *Allied Joint Doctrine for Intelligence, Counterintelligence, and Security* and AJP-3 *Allied Joint Doctrine for the Conduct of Operations*.

iv. **Vulnerability Assessment**. Vulnerability is an inherent exploitable weakness in an asset. Vulnerabilities include deficiencies in planning, preparedness, training, awareness, warning, physical security, hardening, redundancy/back up, and response capability. A Vulnerability Assessment (VA) is a process used to determine the susceptibility of assets to attack (likelihood) or degradation due to hazards, identified in the TA. VAs are accomplished by multi-disciplinary subject matter experts who conduct operational analyses and assess the vulnerability of personnel, materiel, information, facilities, and other assets. The result of a VA is the identification of deficiencies or weaknesses that render critical assets, areas or special events vulnerable to a range of known or likely threats or hazards. Again, for any VA to be valid, those conducting the work must understand where NATO's Centre(s) of Gravity lie and the tactics that any adversaries will use to target the Centre(s) of Gravity.

(3) **Risk Evaluation**. The purpose of risk evaluation is to assist in making FP decisions about which risks need treatment and the priority for treatment. Armed with the result of risk analysis, an Evaluation of the risks can be made. These risks can then be prioritized. Once risk Evaluation has been completed the commander/risk owner has the responsibility to make a decision on risk treatment. Note that the risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls.

c. **Risk Treatment**. The aim of risk treatment is to reduce the level of risk to a level which is acceptable to the commander/risk owner. The following steps are provided for guidance:

(1) **Develop and Implement Force Protection Measures, Effects, Actions and Tasks**.

i. Risk decisions are the commanders' responsibility. The commander at the highest level (i.e., strategic commander or Joint Force Commander (JFC)) usually makes an initial risk response decision, implements overarching FP measures, actions and tasks and establishes commander's guidance concerning the willingness to accept risk; subordinate commanders subsequently do the same for their individual forces. Those measures, actions and tasks that provide protection to the entire force are generally the responsibility of the strategic commander or highest-level JFC as the Risk Owner for the missions' risk decisions; others will be the responsibility of the appropriate subordinate JFC, component

commanders, or other delegated subordinate commanders (*with the necessary Delegated Authority*).

ii. During this step, FP measures, actions and tasks are developed and analyzed as threats and hazards are re-assessed to determine any residual risk. This analysis compares proposed controls or measures with the amount of risk reduction achieved. Risk decisions are always based on the residual risk. This analysis continues until an acceptable level of risk is achieved or until all risks are reduced to a level where benefits outweigh the potential cost. Once developed, the FP measures, effects, actions and tasks are implemented and can be integrated into Standard Operating Procedures (SOPs), written and verbal orders, mission briefings, and staff estimates. This is usually achieved by converting FP controls into clear and simple executable orders, establishing proper authorities and accountabilities, and providing the necessary support to implement, whilst remaining fully aware of any residual risk.

iii. FP measures, actions and tasks, generally fall into the categories described in **Annex B**. Note that measures should not be considered as just reactionary, but can be introduced both as pre-emptive measures or as proactive activity (e.g., framework patrolling, Counter-Intelligence (CI) operations, targeting adversaries). For more specifics on measures, actions and tasks as they apply to the FP fundamental elements, see **Annex A**.

(2) **Incident Response and Recovery**[50].

i. **Response and Recovery Coordination**. It should be noted that incidents although apparently tactical in nature can have strategic impact. Therefore, commanders should consider the need for the coordination of response and recovery activities both vertically as well as horizontally.

ii. **Incident Response**. Incident response includes measures to neutralize, isolate, contain, and resolve a specific threat or hazard event. The objectives of incident response are to stop the incident and to minimize its effects on mission success, to limit the number of casualties, to facilitate recovery, and to take all measures in order to regain operational capability as soon as possible.

[50] For more on response and recovery operations, see *Allied Command Operations (ACO) Force Protection Directive* 80-25.

Effective incident response may require the coordination of the activities of a number of disciplines including, but not limited to, security, health and safety, MILENG, firefighting, search and rescue, Public Affairs (PA), Explosive Ordnance Disposal (EOD), and CBRN. Response actions should follow process and procedures outlined in response plans. Incident response includes:

(a) Immediate action by first responders, such as quick reaction forces, security forces, fire departments, EOD force elements[51] or hazardous material teams.

(b) Establishing an emergency operations' centre.

(c) Implementing measures to contain, isolate, alleviate, or terminate the incident and alert higher HQ and adjoining units.

(d) Implementing operational continuity and alert plans.

(e) Implementing additional protective measures.

(f) Gathering information, assessing damage and preserving evidence for prosecution.

(g) Releasing internal and external information updates.

(h) Coordinating information activities through Info Ops to degrade adversary's ability to exploit successful attack, to demonstrate HN's response, and to reassure audiences of NATO's commitment to their protection.

(i) Implementing medical measures, commensurate with the major incident medical management and support approach. This includes medical and casualty[52] evacuation procedures.

iii. **Recovery**. Recovery operations involve the coordination and implementation of measures intended to mitigate the damage, loss,

[51] For more information see ATP-3.18.1, *Allied Tactical Publication for Explosive Ordnance Disposal*.
[52] With regard to medical systems, a casualty is any person who is lost to the organization for reasons of having been declared wounded, injured, diseased or dead.

hardship, and suffering caused by a natural, accidental, or deliberate threat and/or hazard event. Recovery operations include measures, actions and tasks to restore essential capability, protect health, and provide safety and emergency relief. Effective recovery operations may require the coordination of the activities of a number of disciplines including, but not limited to, military engineering, security, EOD, medical, logistics, safety, CBRN defence activities, transportation, communications, and PA. In addition, recovery may be facilitated by pre-positioned stores or mitigation materials within the installation. Recovery operations include all necessary steps to restore a maximum operational capability after an incident has been contained.

d. **Monitor and Review**. Regardless of whether an incident has occurred, monitoring and review is required to validate the effectiveness of overall FP measures, actions and tasks, to make necessary adjustments, to ensure that risk controls are implemented and enforced to standard, and that a feedback mechanism is in place. It also validates the adequacy, scope, and effectiveness of selected FP measures, actions and tasks in supporting the objectives and desired outcomes. Monitoring and review should occur throughout the process to provide the ability to identify weaknesses and to make changes or adjustments to controls based on performance, changing situations, conditions, or events. Commanders must review actions and processes to ensure that lessons learned and best practices are recorded.

e. **Communication and Consultation**[53]. Communication and consultation with commanders and staff should take place during all stages of the FP risk management process. It is important to address perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts and concerns. Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information.

3.5. **Specific Considerations – Cyberspace**. The considerations discussed in the previous paragraph apply equally to operations in cyberspace and cyberspace specialists must be involved in both planning and applying how the principles discussed here can be applied in cyberspace[54].

3.6. **Specific Considerations - Explosive Safety and Munitions Risk Management**. Logistics functions[55] involving military munitions and munitions related operations (e.g., maintenance, explosives loaded aircraft parking, bomb/missile build-up,

[53] In order to ensure that other locations are aware of what has occurred elsewhere and can prepare themselves accordingly.
[54] See also AJP-3.20, *Allied Joint Doctrine for Cyberspace Operations.*
[55] The phases of the NATO Consumer Logistics Process include Reception, Storage, Transportation, Distribution, Maintenance, Retrograde and Disposal (source ALP 4.2, *Land Forces Logistics Doctrine*).

distribution, storage) pose inherent and significant risk to the operation/mission. Where compliance with Allied Ammunition Storage and Transport Publication (AASTP)-1 and/or AASTP-5 cannot be met, the Explosive Safety and Munitions Risk Management (ESMRM) risk assessment/risk management process described in Allied Logistics Publication (ALP)-16 shall be followed.

Intentionally blank

CHAPTER 4

FORCE PROTECTION PLANNING CONSIDERATIONS

4.1. **Planning Overview**. Force Protection (FP) Planning identifies and establishes measures, effects, actions and tasks to mitigate risks to a level which is acceptable to the commander in order to preserve freedom of action and the operational effectiveness of the force. Therefore, FP must be fully integrated and coordinated within the NATO Operations Planning Process (OPP) from the outset. Inputs that the FP planner may provide could come from a variety of the FP fundamental elements as well as other joint functions. It is therefore essential that a FP staff officer be a member of the planning and working groups at all levels. In the planning of an activity, the strategic level will provide FP direction and guidance to the operational level as early as the Strategic Planning Directive (which really starts the operational level planning). FP requirements are clearly identified, including the specific FP response measures, effects, actions and tasks to be accomplished under the various threat categories. Forces are normally particularly vulnerable to attack during deployment; Reception, Staging and Onward Movement (RSOM) and redeployment.

a. The FP Process is described in Chapter 3.

b. FP specific orders, plans, directives, instructions, procedures, and other forms of direction must be developed as outputs of the OPP. For NATO Operation Plans (OPLANs), FP is addressed in the Coordinating Instructions section of the Main Body of the plan and Annex J, Force Protection[56].

(1) The development of the FP posture is intimately related to the issue of Rules of Engagement (ROE) development. Therefore, FP staffs need to be involved in the consideration of the ROE requirement, within the OPP.

(2) The FP staffs need to consider the applicable NATO Lessons Learned[57] and incorporate these, where applicable, into subsequent activity. Equally, Lessons Identified must be communicated through the Chain of Command (vertically as well as horizontally) to ensure incidents cannot be repeated and/or if reoccurring, can be dealt with swiftly, efficiently and effectively. After all incidents a debrief should be conducted and a formal learning account compiled.

---

[56] See Allied Command Operations (ACO) *Comprehensive Operations Planning Directive* (COPD).
[57] See AJP-3, *Allied Joint Doctrine for the Conduct of Operations* for further detail on the NATO Lessons Process.

4.2. **Plans and Procedures**. NATO-led forces should have specific plans and procedures to manage the preparation and generation of FP measures, effects, activities and tasks to include any anticipated enhancements to peacetime FP measures, effects, activities and tasks to meet escalating threats. These plans should establish the FP organization, C2 and Communication and Information Systems (CIS) requirements, operational areas and resources, and should allow for the conduct of sustained operations in all the possible threat environments. These plans should also include, where necessary, the relevant FP aspects of the Host Nation's (HN's) plans. Additionally, during the conduct of certain operations, such as Non-Combatant Evacuation Operations (NEO), NATO-led forces will be required to provide FP for civilians, family members, and others. As discussed throughout this publication, a variety of capability areas develop lists of assets and activities that are vital to NATO activity. These various lists should be combined into a Critical Asset Protection Plan (CAPP) (*or similarly named document*) by the FP staffs in the Joint Force headquarters. At this level, the CAPP underpins FP planning.

4.3. **Developing Force Protection Procedures**. FP procedures specify when, where and under what circumstances FP measures, effects, activities and tasks should be employed. FP procedures should be designed for simplicity and speed to ensure effectiveness under duress. Procedures, including those actions to be taken in response to changes in alert states, such as fire and bomb threat evacuation, potential Chemical, Biological, Radiological and Nuclear (CBRN) hazard and/or post incident management measures, or protective security, should be considered when developing FP plans. In developing FP procedures, commanders should be cognizant that some measures, effects, activities and tasks may affect the civilian population and in different ways for women, men, boys and girls[58]. These will be subject to legal advice and will need to incorporate the requirements of international and HN law, and any Status of Forces Agreements (SOFAs).

4.4. **Planning Measures, Tasks, and Activities**. Specific FP operational considerations and planning measures, tasks, and activities, such as base security considerations and physical security measures, are set forth in ACO Directives 80-25. Additionally, guidance for air operation FP planning is provided in ATP-3.3.6, *NATO Force Protection Doctrine for Air Operations*. Details on FP planning for maritime forces and infrastructure in ports and anchorages can be found in ATP-74, *Allied Maritime Force Protection* and ATP-94, *Harbour Protection*. At the time of writing, the Land Component is in the process of developing a Land FP ATP.

4.5. **Integration of HN[59] and NATO FP Capability**. The initial planning process identifies NATO requirements for FP and considers which requirements the HN can support

[58] A Gender Advisor (GENAD) should be consulted in order to ensure proper consideration of Gender Perspectives.
[59] See also Host Nation Force Protection (FP) Capability below.

on behalf of NATO. When planning for HN provision, or support of FP, commanders must take into consideration shortfalls in ability, availability or standard of execution from HN services, and make necessary plans and arrangements to mitigate such shortfalls[60]. The use of HN partners to provide FP support for NATO-led forces has both advantages (such as enhanced knowledge of the threat and reduced footprint of deployed forces) and disadvantages (such as increased risk of insider threats, espionage, or sabotage). Some HN partners may lack the capabilities needed to ensure the FP of NATO-led forces. Therefore, the capability of any HN FP support is an essential FP issue that Allied planners should carefully consider. Particular concern should be directed towards potential vulnerabilities associated with HN intelligence, law enforcement, safety and security personnel support. NATO-led forces may have differing relationships with each HN for FP within the area of operations/theatre of operations. Commanders are responsible for developing plans to cover local civil and military authority involvement, since local FP will likely be shared between their command and the HN. The commander should be aware however, that International Organizations (IOs) and Non-Governmental Organizations (NGOs) may not follow NATO FP guidance. In any area, the threat may develop/change over time[61] or indeed, threats may migrate geographically. It should also be acknowledged that the presence of NATO forces in an area may be the catalyst that leads to the development and/or migration of a threat.

4.6. **Integrated FP Capability**. FP will most likely need to take the form of a holistic, whole-of-Alliance approach for large, strategically important facilities where, due to size and/or complexity, no one nation can be expected to take the lead in either providing a national, doctrinal approach to FP and/or, to resourcing the considerable capabilities likely to be required. While Troop Contributing Nations (TCNs) should adhere to the NATO approach to FP, there remains a significant national FP responsibility. Notwithstanding this, experience has demonstrated that:

a. Few nations are capable on their own of providing the full spectrum of capability likely to be required, particularly in complex, high-threat environment and/or over a protracted period.

b. Likely threat scenarios show there is a need for an approach that facilitates TCNs working together under a single unified C2 organization, to create a single, coherent FP effect.

---

[60] For further information see Allied Joint Publication (AJP)-3.16, *Allied Joint Doctrine for Security Force Assistance*.

[61] Threats may increase, decrease or change over time. In some situations, threats may be cyclical or follow discernible patterns (e.g., increase or decrease with the changing of the seasons).

c. The range of capabilities required to deliver FP can be considerable and an approach that creates a framework for the integration of capabilities from multiple nations is required.

d. Some NATO Host Nations (HNs) through a simple function of scale will be unable to provide necessary levels of FP without significant reinforcement.

e. Non-NATO HNs and local authorities in any deployed theatre of operation may or may not be able, or willing, to provide FP assistance to Allied forces.

f. The protection of the force across cyberspace must always be considered.

4.7. **Incident Response Planning**. FP related incidents may occur that will require immediate consideration outside of the routine battle rhythm; these may be dealt with by a multi-disciplinary Crisis Action Team[62]. Staff need to consider the vertical and horizontal implications of the incident and its impact on activity/mission. Throughout the FP Risk Management Process will apply.

4.8. **Recovery Planning**. Recovery planning consists of the same steps that would be taken by a military force under operational conditions. Following the initial response, the NATO commander would initiate requisite actions in accordance with the recovery plan to restore the operational readiness of individuals, units, and facilities as quickly as possible.

4.9. **Force Manning Planning**. Manning plans for NATO activities have to consider maintaining the safety and protection of that activity. The potential for hazards and threats to change and/or migrate means that FP activity in support of NATO activity and associated manning plans should remain under constant review. Any commander who identifies that sufficient FP resources **are not** available to treat the risks identified, should communicate this risk through their chain of command. This may include, if appropriate, communicating the level of Risk to the nations.

4.10. **Strategic Communication Considerations**. Commanders and their FP subject matter experts should always consider the wider Strategic Communication (StratCom) implications of implementing changes to FP posture, particularly in a multi-national environment. Although such changes may appear to be tactical in nature, they may well have far-reaching implications at the strategic-political level for the TCNs and the HN. If there is reason to believe that any change will have ramifications for the mission or the wider strategic narrative, commanders and their FP staff, including the StratCom

[62] A Crisis Action Team (CAT) will consist of a core of specialists designated by the commander and usually led by the senior FP specialist. However, other Subject Matter Experts may be called upon to join the CAT if their input is deemed beneficial in response to a specific or unusual incident.

Adviser and Public Affairs Officer, should ensure the chain of command is informed in advance of any FP change.

4.11. **Media and Force Protection**. Modern communications and media can have a very dramatic impact on FP planning and execution at all levels. Civil authorities can be obliged to account, almost in real time, for the loss of life, perceived lack of resources, and campaign design which can draw them into matters below the strategic level and into military operational and tactical matters. Equally, tactical activities played in the presence of the international media can also have a strategic effect. Modern information and communication technologies allow journalists, members of the civilian population, and members of the participating combatants, to record and disseminate material to a potentially worldwide audience. The effect of this use of media can magnify the impact of any FP incident/issue. The manner in which the Alliance responds to media reports and public reaction could affect the reputation and the credibility of the NATO-led forces. This can have a particular impact on FP as the reputation of a force provides a deterrent effect; if this is sufficiently eroded, it is more likely that further attacks will be launched. Additionally, local and international media, when invited or embedded, can unintentionally give insights into detailed information relevant for opposing forces. This possibility should be addressed and considered in FP planning and StratCom guidance.

4.12. **Civil-Military Cooperation and Force Protection**. Civil-Military Cooperation (CIMIC) activities have the potential for promoting acceptance of NATO operations, thereby helping to reduce incidents against the NATO-led force and contributing to the overall FP effort. This can be achieved through trust and confidence that can be developed by unbiased liaison with all relevant actors and equally balanced support to different recipients. Further, CIMIC may receive information through its liaison that can be useful for improving FP, such as information on the overall acceptance of the Joint Force amongst the population or certain groups and warnings on current threats[63]. A gender-balanced CIMIC staff will be required to ensure that the force can engage with the entire local population (women, men, girls and boys).

4.13. **International and Non-Governmental Organizations**. NATO-led forces conduct operations as a contribution to a wider comprehensive approach[64] that requires coordination and cooperation with national governmental organizations, IOs, NGOs, and the private sector. In such complex multi-agency situations, it is unlikely that absolute consistency will be achieved between civilian and military activities. Commanders should nonetheless encourage, as far as is militarily sensible, a comprehensive response; consideration should therefore be given to offering FP

---

[63] For more on Civil-Military Cooperation (CIMIC), see AJP-3.19, *Allied Joint Doctrine for Civil Military Cooperation*.

[64] For more on a comprehensive approach, see AJP-01, *Allied Joint Doctrine,* or AJP-3, *Allied Joint Doctrine for the Conduct of Operations*.

advice to those organizations that may have a role in the mission. Additionally, depending on the situation, consideration should be given to including locally employed civilians working for Allied forces and other personnel such as the media in FP planning. Finally, good situational awareness on internal security in the HN is paramount for the intelligence assessment. Relationships with international police organizations operating in the area of operations, through the Provost Marshal Office, are required. Gender perspectives must be considered and if available a Gender Advisor (GENAD) consulted.

4.14. **NATO International Civilians, Civilian Contractors and Staffs**.

a. **Civilian Contractors**. The NATO policy on contractor support to operations sets out broad principles and policies for the use of contractor support to operations. In broad terms, the responsibility for FP of civilian contractors will vary depending on the nature of the operation, the terms of the contract, and other legal requirements[65].

b. **Civilian Staffs**. These staffs provide essential support in many mission areas and their loss, or degradation in performance, could significantly impede meeting operational requirements. Care should be taken to avoid involving NATO civilians or contractors in FP activities or training that could be interpreted as taking a direct part in hostilities. Legal advice should be obtained on limitations to civilian participation in FP. Furthermore, consideration will need to be given to the Rules of Engagement (ROE) required to ensure that civilian staff and employees (to include contractors) can be protected.

c. **Education and Training**.

(1) Relevant FP and FP-related education and training applies equally to military and civilian personnel under authority of the NATO commander. Appropriate individual protective measures should be applied to all personnel employed in direct support of NATO activities.

(2) The responsibility for the provision of FP and related education and training depends on the status of the respective individuals. While the responsibility for NATO International Civilians and civilian contractors employed directly by NATO/ Nations resides with the NATO/national commander, the responsibility for civilian contractors employed by a company operating under a NATO or national contract needs to be clarified in the contract[66].

---

[65] AC/305-D(2016)0009-REV1, *NATO Policy on Contractor Support to Operations.*

[66] C-M(2002)50, *Protection Measures for NATO Civil and Military Bodies, Deployed NATO Forces, and Installations against Terrorist Threats*, provides a comprehensive description of who is responsible for providing

4.15. **Battlespace Management and Battlespace Spectrum Management**. Battlespace and Battlespace Spectrum management (BM/BSM) are the means by which friendly force activity is coordinated and deconflicted. From a FP perspective, these activities provide mechanisms through which both Fratricide and Mutual Interference can be prevented. BM/BSM activity of relevance to FP includes, but is not limited to the following:

a. **Fratricide**. Fratricide is the accidental destruction of own, allied, friendly, or neutral forces and its prevention is part of the FP process. This prevention is assisted by accurate combat identification, which is the use of identification measures to reduce friendly fire and increase the operational effectiveness of forces and weapon systems. Identification measures may include combining SA, target identification, and specific TTPs with effective battlespace management[67]. Additionally, with increasing competition for use of the electromagnetic spectrum, the need to minimise mutual interference through the effective management of the operating environment and electromagnetic spectrum becomes an essential part of both maintaining combat effectiveness and minimising fratricide[68]. Although the risk of fratricide is greatest in warfighting, it remains present at all times and is increased in multinational operations. Incidents of 'friendly fire' could have detrimental effects on morale and force cohesion in Alliance operations. Credibility, as well as the public's support, may be eroded due to such fratricide incidents; therefore, commanders at all levels should take all necessary steps to prevent its occurrence.

(1) **Use of Geospatial Information (GI)**. Historical examples exist[69] of fratricide between two NATO Nations, operating on NATO led operations, with conflicting GI and geospatial referencing systems. Such incidents are mitigated by strict adherence to NATO Geospatial Policy[70] which mandates the use of Designated Geospatial Information for all NATO activity, in an effort to ensure allies operate off the same map.

b. **Mutual Interference**. Prevention of mutual interference involves measures to minimize the interference between friendly forces and units. Interference can

---

Force Protection (FP) training for any category of civilian, irrespective of where they may be employed or deployed.

[67] For broader discussion on Battlespace Management, see AJP-3, *Allied Joint Doctrine for the Conduct of Operations*.

[68] Operating Environment and Electromagnetic Spectrum Management are responsibilities of Electromagnetic Warfare Coordination Cell (EWCC), Signals Intelligence and Electromagnetic Warfare Operations Centre (SEWOC) or Electromagnetic Battlestaff (EMB).

[69] 3600/SHIGS – 270458, *Geospatial Support to NATO Led Operations*, dated 26 May 2010. Supreme Headquarters Allied Powers Europe (SHAPE) Chief of Staff (COS) letter sent in response to a fratricide incident on a NATO operation.

[70] See MC 296/3, *NATO Geospatial Policy*.

be physical (collision, weapon hit) or occur in the electromagnetic and acoustic spectrums. Mutual interference can be prevented by separating activities either in space, in time or in (electromagnetic or acoustic) frequency[71].

(1) **Airspace Control**[72]. JFC normally designates COM JFAC as the airspace control authority responsible for operation of the airspace control system and development of the airspace control plan. This plan directs–implementation and coordination of the procedures governing airspace planning and organization to minimize risk and allow for the efficient and flexible use of airspace. Airspace control involves safety measures such as airspace control measures, airspace management, weapon control orders, and fire support coordination measures[73]. All users of the airspace within the theatre must adhere to the guidance provided by the airspace control plan, airspace control orders, the area air defence plan and special instructions to assure integration and minimize the risk of fratricide. Airspace control requires a combination of positive and procedural controls that rely on proper identification of the users. Positive control requires radar or other sensor tracking and direct communications between the airspace controller and the user. Airspace control plan, airspace control orders and special instructions establish procedural controls through coordination measures and amplifying guidance.

(2) **Waterspace Management**. A system of procedures for the control of antisubmarine weapons to prevent inadvertent engagement of friendly submarines[74].

(3) **Prevention of Submarine Mutual Interference**. A system of procedures to prevent, on the one hand, submerged collisions between friendly submarines, between submerged submarines and friendly ship towed bodies or between submerged submarines and any other underwater object, and, on the other hand, interferences with any underwater event[75].

---

[71] See AJP-3, *Allied Joint Doctrine for the Conduct of Operations*

[72] The Airspace Control Authority is the commander designated to assume overall responsibility for the operation of the airspace control system in a designated airspace control area. See AJP 3.3, *Allied Joint Doctrine for Air Operations*. Airspace Control is the implementation and coordination of the procedures governing airspace planning and organization in order to minimize risk and allow for the efficient and flexible use of airspace (NATOTerm).

[73] See AJP-3.3.5, *Doctrine for Joint Airspace Control*.

[74] See ATP-18, *Allied Manual of Submarine Operations*.

[75] See ATP-1 Volume I, A*llied Maritime Tactical Instructions and Procedures*.

(4) **Prevention of Electromagnetic and Acoustic Interference**. Mutual interference can occur with electromagnetic devices, such as radars, radios and jammers, as well as with acoustic devices such as sonars. Prevention of interference is normally based on separation in time or in frequency. Measures include the radar frequency plan, the active sonar interference avoidance plan, the joint restricted frequency list, and radio and non-ionizing radiation hazards management.

4.16. **Use of Non-Lethal Force in Force Protection**. Use of non-lethal force[76] can be employed in a FP role if authorized by the mission ROE. Use of force has to be in accordance with applicable international law, especially, but not limited to, (*in situations of armed conflict when international humanitarian law applies*) the principles of honour, distinction, military necessity, proportionality and humanity. When using force, it may be necessary to distinguish whether the effects of force will be different between women, men, girls and boys and whether any gender-related security risks exist. Non-lethal effects provide an additional level of escalation and can be used in a FP role to minimize civilian casualties and reduce collateral damage. Proper employment can assist the commander in creating more time and space to act (*by disabling rather than injuring/killing*) and aid in the discrimination of hostile from non-hostile individuals. Proper training in the use of non-lethal force is a primary consideration prior to their employment.

4.17. **Weapon System Support for Force Protection**. Weapons systems not in direct use for FP, but available in the area of operations can be used in a FP role to observe or engage the enemy. Proactive operations and a clear presence of weapon systems will have a deterrent effect on an enemy. Use of weapons systems that can operate from NATO bases in the area of operations provides a flexible capability without deploying to forward locations, thus reducing the forward footprint, which in turn decreases the demands on FP means. The appropriate ROE must be authorised to enable weapon systems to be used in the FP role.

4.18. **Insider Threat[77] Considerations**. Insider threat, can undermine NATO FP plans as well as the cohesion of NATO-led forces. Strategically, they can threaten not only the Alliance's objectives, goals, and exit strategy, but also undermine the overall efforts of the international community. Tactically, the breakdown of trust, communication, and cooperation across the joint force, host nation and civilian partners can affect military capability. Minimising the insider threat, especially by proper preparation and training of forces, is critical to mission success. However, more stringent FP measures, tasks, and activities that are overtly heavy handed must be well balanced yet culturally sensitive enough to not send the wrong message to the very people and organisations the Alliance is trying to protect. Adversaries may view attacks against NATO forces as

[76] See also: https://www.nato.int/cps/en/natohq/official_texts_27417.htm
[77] Note that threats from 'insiders' are not necessarily always 'kinetic' in nature.

a particularly effective tactic, especially when using co-opted, allied, coalition or HN forces to conduct these attacks. NATO should ensure that their FP plans take into account the potential for these types of attacks and plan appropriate countermeasures as the situation dictates.

4.19. **Terrorism Espionage Subversion Sabotage and Organised Crime**. For discussion on TESSOC, see 'Security' in Chapter 2. A robust Counter-Intelligence (CI) capability can be used to identify and mitigate against TESSOC. See also CI in Annex A.

4.20. **Use of Remotely Controlled Systems in Force Protection**. Two main types of remotely controlled systems can be used in support of FP:

a. Static systems that include, but are not limited to, Closed-Circuit Television (CCTV), seismic sensors, radars and Intrusion Detection Systems (IDS).

b. More mobile systems such as remotely controlled air, surface or subsurface vehicles.

Both types of capability can be used in the FP role to observe possible enemy areas and avenues of approach, prevent enemy sanctuary and freedom of movement, identify danger areas as well as safe routes for own forces, and provide convoy protection. Additionally, the ability to operate in distant locations, with control stations a safe distance away from possible threats or hazards, reduces the forward footprint which, in turn, lessens demands on FP means.

4.21. **Force Protection Training**.

a. **General**. NATO training, exercise, and evaluation policy is prescribed in MC 0458/3. The focus of NATO training, including exercises and evaluations, as well as national training programs, is on achieving, maintaining, and enhancing effective military capabilities. Effective FP training is a building block of effective FP. NATO-led forces should be capable of fulfilling prescribed FP measures, tasks, and activities effectively and in accordance with NATO standards and requirements. Collective training is normally the responsibility of the NATO commander. NATO-led forces and civilian personnel should be familiar with the essential elements of their respective FP plans and procedures, including the C2 organization and responsibilities, coordination, local alarms, and reporting arrangements. Additionally, NATO staffs train in accordance with the plans and arrangements for the integration of augmentees and reserve forces to meet the mission requirements. NATO-led forces should conduct, as a minimum, annual FP training in accordance with the relevant NATO Standardization Agreement or command authority. In the absence of such direction, it should be conducted at the discretion of the nominated NATO Commander. It should be noted that this paragraph applies equally to NATO International Civilians (NIC).

b. **Force Protection Training for Key Leaders**. Commanders play an important role in the both the FP and risk management processes. It is therefore, essential NATO Key Leader Training (KLT) provided to commanders include at least an overview of the NATO FP process and their roles and responsibilities within that process[78]. Ideally, any KLT will include a comprehensive FP package that will be tailored to the threats and hazards identified in any particular theatre of operations.

c. **Pre-Deployment Training**. In the context of expeditionary operations, advance preparations through Pre-Deployment Training (PDT) are vital to ensuring that all personnel can fulfil their role in a deployed environment. PDT is normally theatre-specific and is a national responsibility building upon the foundation of individual FP training.[79] It is highly desirable that deploying forces undergo cultural awareness training as part of the deployment process.

d. **Theatre Induction and In-Theatre Training**. Upon deployment, theatre induction training reinforces some of the PDT on arrival in theatre and is critical to the integration of FP procedures on a multinational level. All personnel should be briefed, as a minimum, on the threats, hazards, procedures, and alarms that are unique to the deployed location. During operations within a JOA, personnel may require additional training that could be the result of a changing operating environment or refresher training as well as collective training. Commanders should plan for and provide the required resources for such training, especially for extended deployments.

---

[78] To include their responsibilities under United Nations Security Council Resolution (UNSCR) 1325, *Resolution on Women, Peace and Security*.

[79] As a minimum, this should include Individual Common Core Skills (ICCS) (e.g., weapon handling, first aid, emergency fire-fighting, Improvised Explosive Device (IED) awareness and use of individual Chemical, Biological, Radiological and Nuclear (CBRN) protection equipment).

Intentionally blank

ANNEX A

Force Protection Fundamental Elements

A.1. **Overview**. NATO Force Protection (FP) comprises a number of fundamental elements which can achieve the desired objective. The relative contribution of these will be determined by the threat, scale of the operation, climate, and the civil factors of the operating environment. In a low-threat level environment, security and health (to include safety) protection may be the only FP Fundamental Elements required. At higher threat levels, this may be increased to include countering air and missile threats, Military Engineering (MILENG) support to FP (to include Explosive Ordnance Disposal (EOD)), and Chemical, Biological, Radiological and Nuclear (CBRN) defence. However, some threats may exist at all threat levels and therefore there may be a requirement to apply comprehensive protection measures, activities and tasks across the continuum of activity. Below is a discussion of the measures, effects, activities and tasks within the FP fundamental elements. It is not meant to be all inclusive or an exhaustive list, nor is it meant to segregate the measures, effects, activities and tasks and activities in only one particular competency. The intent of this annex is to describe the fundamental elements all together, provide the types of measures, activities and tasks involved, and explain how they can contribute to the overall FP plan.

A.2. **Tactical Area of Responsibility Control**.

a. **Introduction**. To facilitate the coordination of FP in a designated area against threats and hazards a Tactical Area of Responsibility (TAOR) [80] can be established. The principal reason for a TAOR is to provide defence in depth. This is to prevent both direct and indirect attacks being targeted at mission essential equipment, infrastructure (to include facilities) or personnel. If a TAOR is established, the establishing authority should place the TAOR under the control of a single commander. The area around any operating location dictates what FP measures, tasks, and activities need to be applied in order to counter prevalent threats and hazards and seek to achieve a secure operating environment. Most deployed NATO locations are not sited to take account of tactical considerations. This will affect the size of any TAOR, which will need to be large enough to take account of threats and likely avenues of attack against assets using any location from which to mount operations as well as the defence of the base itself.

[80] A Ground Defence Area (GDA) may be a discreet Tactical Area of Responsibility (TAOR) in its own right or, included within a larger TAOR. For more on GDA see ATP-3.3.6, *NATO Force Protection Doctrine for Air Operations*.

b. TAOR control includes all actions to gain control over the situation in the TAOR such that friendly forces have freedom of operation and adversaries do not.

(1) **Counter-Surface to Air Fire**. Actions to prevent the engagement of air platforms from the ground.

(2) **Counter-Surface to Surface Fire**. Actions to prevent the engagement of vessels from another vessel or from the shore.

(3) **Counter-Indirect Fire**. Actions to prevent or reduce the effectiveness of indirect fire attack on any force.

(4) **Countering-Improvised Explosive Devices**. Actions to achieve the desired efforts against the IED system to prevent or reduce the effectiveness of IED attack on the force (may include operations in the littoral). Countering-improvised explosive devices (C-IED) may have an immediate effect on FP, as well as long term effects in preventing the use of IEDs.[81]

(5) **Counter-Direct Fires**. Actions to prevent or reduce the effectiveness of direct fire attack on the force.

(6) **Countering Class 1 Unmanned Air Systems**. TAOR control measures to defeat the Class 1 UAS threat (within the TAOR), similar to those measures undertaken to defeat Rocket, Artillery and Mortar (RAM) attacks (see Counter-Indirect Fire).

(7) **Counter-Reconnaissance**. Actions to prevent or reduce the effectiveness of reconnaissance of the force, activity or asset by an adversary.

(8) **Influence**. Actions taken to cause a change in the character, thought, or action of a particular entity.

(9) **Counter-Intruder and Perimeter Defence**. Prevention of unauthorised personnel gaining access to any NATO installation.

(10) **Counter-Small Unmanned Aerial Systems (CsUAS)**. NATO commanders must be able to protect their installations and forces and missions from the threat of small Unmanned Aerial Systems. This is inherently a protection priority.

---

[81] For more on Counter-Improvised Explosive Device (C-IED), see AJP-3.15, *Allied Joint Doctrine for Countering-Improvised Explosive Devices.*

(11) **Defence of Maritime Forces**.

(a) Anti-surface warfare is the defence of maritime forces against attack from ships and vessels.

(b) Anti-submarine warfare is the defence of maritime forces against attacks by submarines and torpedoes.

(c) Naval Mine Countermeasures (MCM) form the defensive part of naval mine warfare. Naval MCM protect maritime forces against the threat of naval mines.

(d) Defence in harbours and anchorages against threats from land, air, and sea or waterside. It includes the defence against underwater threats such as swimmers, divers and all kinds of explosive ordnance threat such as, but not limited to, underwater IEDs, torpedoes, naval mines and explosives. Conducted in coordination with port security measures, tasks, and activities.

(e) Defence from fast inshore attack craft in the littorals.

A.3. **Integrated Air and Missile Defence**[82]. Air defence operations are normally the responsibility of an Air Defence Commander who integrates and coordinates the air defence assets of each force component into a coherent joint air defence plan. This includes establishing weapons control procedures and measures for all defensive counter-air weapon systems and forces, coordination with regional and Host Nation (HN) air defence systems, and the exchange of information necessary to support civil defence activities. Air defence operations protect friendly forces and vital interests from air and missile attacks and include both active and passive measures. Area Air Defence (AAD) involves any direct defensive action taken by Surface Based Air and Missile Defence (SBAMD) units and non-dedicated and non-Air Defence units to destroy, nullify, or reduce the effectiveness of enemy air and missile attack against friendly forces and critical elements. Passive Air and Missile Defence (PAMD) includes all other measures taken by all forces to minimise the effectiveness of hostile air and missile attacks, through individual and collective protection of friendly forces and critical assets. Below are several air defence measures, tasks, and activities related to or overlapping with FP.

a. **Tactical Ballistic Missile Defence**. Defence against ballistic, cruise and air-to-surface missile attack.

---

[82] For more on Integrated Air and Missile Defence, see AJP-3.3, *Allied Joint Doctrine for Air and Space Operations* and AJP-3.3.1, *Allied Joint Doctrine for Counter Air Operations*.

b. **Surface Based Air Defence**. Defence from the surface against attack from the air.

c. **Maritime Air Defence**. Above water warfare employs maritime assets to counter the enemy surface and air threat. It is all actions to defend the maritime force against attack by airborne weapons launched from aircraft, ships, submarines, and land-based sites or to destroy the enemy fleet. In a joint operation the use of land-based Commander (COM) Air Component Command (ACC) Joint Force Air Component (JFAC) or COM Land Component Command (LCC) land component commander forces for anti-air warfare and anti-surface warfare in support of COM Maritime Component Command (MCC) objectives are important factors which necessitate close cooperation between naval, air, and land forces.

d. **Counter-Rocket, Artillery, and Mortar**. Counter-Rocket, Artillery, and Mortar (C-RAM) consists of three basic components - sense, warn, and intercept. Actions to detect, and warn base personnel of, attack using indirect fires. To sense and warn, 'intercept' may be added, which involves engagement of incoming munitions; in such circumstances, fire control is essential to prevent fratricide and fall of shot must be considered.

e. **Countering Class 1 Unmanned Air Systems**. Air Defence activity to defeat the Class 1 UAS threat, similar to those measures undertaken to defeat attacks from the air and/or Rocket, Artillery and Mortar (RAM) attacks (see also SBAD and C-RAM).

f. **All Arms Air Defence**. The low-level air defence of a unit using small arms; fire control is essential to prevent fratricide and fall of shot must be considered.

A.4. **Chemical Biological, Radiological, and Nuclear Defence**. The aim of Chemical Biological, Radiological, and Nuclear (CBRN) defence in support of FP is to help to prevent the CBRN incidents, protect NATO forces from the effects of CBRN incidents, and to take recovery actions, so that NATO forces are able to avoid contamination or accomplish the mission and maintain freedom of action in a CBRN environment. Consequently, CBRN defence measures, tasks and activities can be both active and reactive in nature by preventing CBRN incidents as well as by recovering from the consequences of CBRN incidents. CBRN defence in support of FP does not cover offensive actions to nullify, eliminate, or disable CBRN weapons or their delivery systems, however, the principles and capabilities described here may be employed by commanders during Countermeasure (CM) operations designed to prevent CBRN incidents. CBRN defence can be divided into five components which are inter-related and underpinned by the principles of FP. These components below include:

a. **Detection, Identification and Monitoring**. Detection, identification, and monitoring capabilities embrace: the discovery, characterization and measurement of CBRN substances; the identification of associated hazards.

This includes delineation of areas of contamination and allows monitoring of changes over time[83].

b. **CBRN Knowledge Management**. CBRN knowledge management is the collation, storage, analysis and dissemination of CBRN-related information and knowledge in order to contribute to situational awareness and to provide advice for the planning, preparation, and execution of operations. It enables the rapid collection, evaluation, and dissemination of data that characterizes CBRN incidents, together with the advance modelling, simulation and prediction of resulting hazard areas. It includes sensor integration, network management and following systematic information collection; issuing of critical warning messages; exchange of CBRN information; reach back capability; analysis; storage, exploitation, and the provision of CBRN assessments; and advice for operations planning prior, during, and after CBRN incidents. CBRN information management includes Warning & Reporting (W&R). In-theatre CBRN W&R system for incidents and the resulting hazards prediction has to be in place in accordance with ATP-45 so that the risk to the joint force is minimised. This system needs to provide information to commanders and staffs at all levels with timely and accurate information about the CBRN situation to take appropriate mitigating CMs. CBRN reporting links should, in principle, be established vertically and horizontally to ensure timely warning to adjacent units. Procedures for sharing of W&R with other organisations and HN authorities should be established and disseminated.

c. **Physical Protection**. Individual and collective protection intended to enhance the survivability of personnel and materiel in a CBRN environment and allows, with possible reduction of operational capability, them to continue to operate in a CBRN environment. Measures, tasks, and activities to protect facilities and equipment, such as through original design or hardening, are included[84].

d. **Hazard Management**. Hazard management preparatory and responsive measures, tasks, and activities limit the operational impact of CBRN incidents and should be an integral part of operational planning and, as much as possible, be prepared well in advance ensuring the principles of pre-hazard precautions and hazard control through avoidance, control of spread, exposure control and decontamination. This will also present a danger to deployed forces, and although the specific characteristics of substances and scale of hazard areas will vary compared with those of typical CBRN weapons, the same principles and measures of CBRN defence will provide the basis for action.

---

[83] See also AJP-3.8, *Allied Joint Doctrine for Comprehensive Chemical, Biological, Radiological, and Nuclear Defence*.
[84] Ibid.

e. **Medical Countermeasures and Casualty Care**. Medical CMs are designed to diminish the susceptibility of personnel to the lethal and damaging effects of CBRN substances, evacuate and subsequently to treat any effects arising from exposure to such hazards. The treatment and evacuation of conventional casualties in a CBRN environment is included. The medical contribution to CBRN defence covers all five of the enabling components[85]

A.5. **Resilience Overview**. The principle of resilience is firmly anchored in Article 3 of the Alliance's founding treaty:

"In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."

a. **Resilience**. Measures, tasks, and activities to increase friendly forces' ability to continue to perform specified functions during and after an attack or incident.

(1) **Dispersal.** The spreading or separating of troops, materiel, establishments, or activities to reduce vulnerability.

(2) **Redundancy**. Arrangements such that despite denial of assets, the desired effect can still be created.

(3) **Counter-Surveillance**. Counter-surveillance includes all measures, tasks, and activities (active or passive) to counteract hostile surveillance. This may include camouflage, concealment, and deception measures, which use natural or artificial materials on personnel, objects or tactical positions. The aim of counter-surveillance is to confuse, mislead or evade the enemy; to protect own forces from observation or surveillance; or to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.

(4) **Physical Protection**. Achievement of protection against weapon or hazard effects by physical means.

(5) **Personnel**. All personnel irrespective of rank/status, or role should be capable of contributing to FP[86]. Their knowledge should include any asset sectorisation (or compartmentalisation) and Command and Control (C2), own asset/workplace protection and contribution to FP of the asset

---

[85] See also AJMedP-7, *Allied Joint Chemical, Biological, Radiological, and Nuclear (CBRN) Medical Support Doctrine*.

[86] This paragraph should be read in the context of Joint activity. The contribution of all personnel to effective FP applies equally in all domains and locations (e.g., concepts apply equally to a base or a vessel at sea etc.).

(including the role of commanders), sector/workplace control of entry (to include boarding and loading), guards and sentries (including guard commanders), responses to alarms, warnings and information, post attack reconnaissance, Unexploded Explosive Ordnance (UXO) detection and marking, CBRN detection and individual (immediate) decontamination, cordons, reporting, FP C2, incident C2, combined incident teams, and the rules/processes for the inclusion of contractors and locally employed civilians.

b. **Collaborative Resilience**. Collaborative Resilience (CoRe) is an emerging concept within NATO and is described as:

(1) "Society's ability to resist and recover easily and quickly from shocks combining civilian, economic, commercial and military factors. It is, in sum the combination of civil preparedness and military capacity[87]. Resilience is the ability to survive and overcome strategic shocks[88], which critically impair the ability to conduct successful operations by stretching military capabilities beyond the point of failure. Therefore, being resilient to shocks, which cannot be overcome by adapting internally, is achieved by the ability to incorporate additional capabilities or capacity from non-military resources and direct them to the desired operational objective."

(2) NATO's CoRe vision is:

"An Alliance able to sustain successful operations by preparing for, absorbing, recovering and adapting to surprise or strategic shock, through harmonized and resilient structures, systems and processes, enabled by a persistent collaboration across civil, military and private stakeholders".

(3) Hence, CoRe speaks to each of the four areas of the Resilience Cycle (Prepare, Absorb, Recover, and Adapt) in order to allow the Alliance to collectively:

(i). Recognize, assess and quantify NATO military forces' dependencies on national civilian critical infrastructure and services;

---

[87] NATO Topic Paper, *Resilience and Article 3*, https://www.nato.int/cps/ic/natohq/topics_132722.htm.
[88] A shock is considered as a sudden, surprising event with military consequences whether these are intended or unintended.

(ii). Understand how military operations can induce and be disrupted by shortfalls in required civilian capabilities, infrastructure and assets, both public and privately owned.

(iii). Develop guidance to enhance national resilience levels to support NATO military operations in a Collective Defence scenario.

(4) CoRe applies throughout the entire spectrum and scale of military operations, from Baseline Activities and Current Operations (BACO) to Maximum Level of Effort (MLE). Thus, the respective FP organization should be able to preplan resilience measures in the FP planning process.

A.6. **Military Engineering Support to Force Protection**. Military Engineering (MILENG) support to FP is one of the eight defined FP fundamental elements, respectively, it contributes to all the Force Protection Coordination Areas and to the whole risk management process applied to FP; moreover, MILENG also provides support to many other joint functional areas as well as to other FP fundamental elements. Additionally, MILENG supports the efforts to coordinate the activities of a large number of FP specialist areas, each with their own plan and priorities. In particular, MILENG supports many consequence management measures tasks and activities to include EOD, restoration of essential services and facilities, as well as fire safety. MILENG support to FP is divided into eight sub-categories:

a. **Protective Infrastructure**. This includes all the infrastructure, material, tasks and activities that contribute to FP. It encompasses professional and technical expertise for planning, designing, coordinating construction and maintenance of appropriate infrastructure, hardening facilities, perimeter security systems, bases' surveillance systems, determining stand-off distances and field fortifications[89].

b. **Fire Protection**. Fire protection includes the design and construction of fire prevention and suppression systems within infrastructure. It includes the development, implementation and monitoring of a fire safety programs within any NATO facility, including training, exercises and the evaluation of the Fire Protection Plans as well as fire response capabilities in coordination with other logistics capabilities and FP fundamental elements[90].

c. **Explosive Ordnance Disposal**. EOD[91] comprises those particular actions taken by specially qualified personnel for countering Explosive Ordnance (EO)

---

[89] See also ATP-3.12.1, *Tactical Doctrine for Engineering.*
[90] Firefighting is primarily a Consequence Management function.
[91] See also AJP-3.18, *Allied Joint Doctrine for Explosive Ordnance Disposal Support to Operations* and/or ATP-3.18.1*, Allied Tactical Publication for Explosive Ordnance Disposal*.

threats. EOD force elements dispose of EO that threatens friendly forces, vital points or high-value assets, and provide operational analyses and assess the vulnerability of personnel, materiel, facilities and other assets with reference to EO threats. As subject matter experts, EOD staff or EOD force elements can provide training on ordnance hazards and recognition, explosive ordnance awareness, explosive ordnance reconnaissance procedures and personnel protective measures.

d. **Support to C-IED activities**. MILENG makes a significant contribution to C-IED[92]. C-IED is an all-arms responsibility and aims to defeat an adversary's IED System. The approach has three mutually supporting and complementary pillars of activity which are: Attack the Networks; Defeat the Device; and Prepare the Force. MILENG personnel, due to their training in military search, or in specialist roles such as support to geomatics, may be involved in C-IED operations. MILENG support may include engineering advice and protective works. EOD specialists contribute significantly to C-IED activity, primarily in the '*Defeat the Device*' pillar. However, work also includes supporting technical exploitation that will provide information critical to C-IED '*Attack the Networks*' activity[93]. Lastly, EOD staff and EOD force elements can provide explosive ordnance expertise to support the '*Prepare the Force*' pillar.

e. **Camouflage, Concealment, and Deception**. This includes the planning, design, construction and maintenance of physical concealment and deception structures.

f. **Military Search**. Military Search[94] is an essential element of FP, both protecting coalition assets and enabling freedom of action and movement. Military search provides assurance of potential 'high-level' targets during pre-planned events.

g. **Route and Area Clearance**. Route Clearance[95] is a mobility task, under the MILENG Support to Joint Functions manoeuvre and fires, of which some components fall under FP. It targets physical hindrance to movement on road networks or itineraries and areas to facilitate freedom of movement.

h. **Area Access Control (AAC)**[96]. An AAC obstacle system is a C2 system for various sensors and effectors in order to control access to, or create an obstacle in, a specific land-based operational area. AAC is a capability that will be

---

[92] See AJP-3.15, *Allied Joint Doctrine for Countering-Improvised Explosive Devices.*
[93] See AIntP-15, *Countering Threat Anonymity; Biometrics in Support of NATO Operations and Intelligence* and *AIntP-10 Technical Exploitation* for detail.
[94] ATP-3.12.1.1, *Allied Tactical Doctrine for Military Search.*
[95] ATP-3.12.1.3, *Allied Tactical Doctrine for Route and Area Clearance*.
[96] Standards Recommendation (STANREC) 2642, Allied Procedural Publication (APP-34), *Testing and Interoperability of Area Access Control Obstacle System*.

employed to execute counter-mobility and survivability tasks. Survivability tasks will include enhancing FP at base camps, facilities, and other infrastructure, while allowing access for friendly personnel or equipment.

A.7. **Consequence Management**. Consequence Management[97] includes measures, tasks, and activities taken to mitigate the damage, loss, hardship and suffering caused by catastrophes, disasters or hostile actions. It also includes measures to restore essential services, protect public health and safety, and provide emergency relief to affected populations.

a. **Post-Attack Reconnaissance**. Timely and safe post-attack area or base-wide determination, reporting and actions on damage, UXO, and CBRN contamination.

b. **Explosive Ordnance Disposal Support**. EOD and support to C-IED activities are often required to contribute to incident response and recovery activities. See A006.c. above.

c. **Restoration of Essential Services and Facilities**. This involves making the necessary and immediate repairs to facilities so that normal services and operations may resume. It includes airfield damage repair, restoration of aircraft operation surfaces, and restoration of port or harbor facilities.

d. **Fire Prevention, Fire Fighting, and Crash Rescue**. Fire safety, including the provision of fire protection measures, firefighting resources, alarms and procedures, is implemented to safeguard the force from avoidable loss. Fire personnel provide advice on specialist issues including those that arise during the planning and construction of temporary infrastructure, particularly accommodation and headquarters. Firefighting is a recuperative activity once an incident has taken place, either through an accident or deliberate means. Where contractors are employed to provide firefighting cover, FP staffs should ensure that the full range of firefighting capabilities required is available through the contract to include, where applicable, the ability to deploy to an off-base incident. Firefighting and crash rescue are essential elements of air operations whilst an ability to fight fires afloat is essential for effective FP of port facilities; in both cases they must be linked to FP arrangements. Fire services may include the ability to deal with toxic industrial hazards.

e. **Joint Personnel Recovery**. Personnel Recovery (PR) is the sum of military, diplomatic, and civil efforts to effect the recovery and reintegration of isolated personnel. PR encompasses a variety of recovery options and apabilities. It is

---

[97] For more on Consequence Management, see NSA(JOINT)0478(2009)1/CBRN, AJP-3.8, *Allied Joint Doctrine for Comprehensive Chemical, Biological, Radiological, and Nuclear Defence*, AJP-4.10, *Allied Joint Doctrine for Medical Support*, and MC 472, *NATO Military Concept for Defence against Terrorism*.

a joint responsibility which should also be addressed at component command level and below. The operation's Joint Force Commander (COM JFC) and staff must conduct a thorough mission analysis that considers all available PR options and capabilities to successfully plan recovery operations within the Joint Operation Area (JOA). The situation and environment will define the capabilities needed for PR missions, although, it is likely that the forces available will only have a limited PR capability. However, forces assigned to PR duties must be able to undertake any PR execution task, within means and capabilities. It should be noted that FP force elements operating within a TAOR may be called on to perform PR tasks. Should this be the case, then wherever possible, these force elements should be trained in accordance with AJP-3.7, *Allied Joint Doctrine for Recovery of Personnel in a Hostile Environment* [98].

f. **Strategic Communication**. Strategic Communication (StratCom) (and therefore Military Public Affairs (PA)), protects Alliance cohesion, reputation and its relations with HNs, Allies and Partners. It should therefore be a consideration in FP planning both in terms of Resilience and in response to an incident.

A.8. **Force Health Protection** [99]. In a medical context, FP is the conservation of the fighting potential of a force so that it is healthy, fully combat-capable and can be applied at the decisive time and place. It consists of actions taken to counter the debilitating effects of the environment, occupational health risks, Environmental and Industrial Hazards (EIH), disease and selected special weapon systems through preventative measures for personnel, systems and operational formations. Force Health Protection (FHP) is therefore the sum of all efforts to reduce or eliminate the incidence of Disease and Non-Battle Injuries (DNBI) to enhance operational effectiveness. The FHP contribution to FP is the responsibility of the Medical Advisor/Medical Director and the Medical Staff. FHP measures, tasks and activities fall into six main areas (*all applicable in CBRN as well as conventional circumstances*):

a. Deployment Health Surveillance;

b. Communicable Disease Control and Prevention (including Infection Prevention and Control);

c. Occupational and Environmental Health;

d. Hygiene and Sanitation;

---

[98] See also Allied Personnel Recovery Publication (APRP)-3.3.7.7, *NATO Personnel Recovery Tactics, Techniques and Procedures (TTPs).*
[99] For further information on FHP see AJP-4.10, *Allied Joint Doctrine for Medical Support and AJMedP-4, Allied Joint Medical Force Health Protection Doctrine*.

e. Food and Water Safety[100];

f. Mental and Physical Health/Preparedness.

The six areas above are described in detail in AJMedP-4, Allied Joint Medical Force Health Protection Doctrine.

A.9. **Security**[101]. Security enhances freedom of action by limiting vulnerability to hostile activities and threats and covers a range of activities that contribute directly and indirectly to FP. It aims to minimize attacks on personnel, information, equipment and installations through the application of physical, procedural and technical measures. Security in NATO encompasses entry control, Operations Security (OPSEC), counter-intelligence, information, CIS Security and Information Assurance, physical, personnel, and air transportation security. Such security programs interact with related programs for counter-crime and law enforcement, and road traffic and recreational safety. Safety and security remain as individual and collective responsibilities throughout the whole threat spectrum. As NATO moves through crises to conflict, war-fighting elements of FP will apply increasingly; however, the basic elements of security remain essential to delivering FP effects. MP units, when available, are well suited to support FP security operations. MP security activities directly contribute to and enhance wider area security, which reduces the force's vulnerability to hostile activities and threats through active and passive measures to include convoy and special load security, critical sites security, close protection, reconnaissance, law enforcement, crime prevention, and investigations.

a. **Access Control**. Actions to ensure that only authorised personnel, equipment, and supplies enter. Access control may include exit control (e.g., for counter-intelligence or counter-crime).

b. **Operations Security**[102]. The process which gives a military operation or exercise appropriate security, using passive or active means, to deny the adversary knowledge of the dispositions, capabilities and intentions of friendly forces.

c. **Counter-Intelligence**. Those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in Terrorism, Espionage, Sabotage, Subversion and Organized Crime (TESSOC).

---

[100] Responsibility for the safety of food and water is a Force Health Protection (FHP)/Force Protection (FP) responsibility.
[101] See AJP-2, *Allied Joint Doctrine for Intelligence, Counterintelligence, and Security*, AJP-2.2, *Counter-Intelligence and Security Procedures* and AJP-3.10.2, *Allied Joint Doctrine for Operations Security and Deception*.
[102] For further information see AJP-3.10.2, *Allied Joint Doctrine for Operations Security and Deception*.

d. **Security of Information**. That part of security concerned with measures designed to safeguard relevant data of every description which may be used in the production of intelligence, to safeguard it against espionage, sabotage, damage and theft.

e. **CIS Security/Information Assurance**. Computer Network Defence (CND) protects against Computer Network Attack (CNA) and computer network exploitation. CND is action taken to protect against disruption, denial, degradation, or destruction of information resident in computers and computer networks or the computers and networks themselves. Cyber Defence includes:

(1) Prevention and Resilience.

(2) Incident detection.

(3) Warning and Reporting.

(4) Incident assessment and investigation.

(5) Reaction and recovery in cyberspace.

f. **Defensive Cyber Operations/Cyber Security**. Defensive Cyber Operations (DCO) include defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace. Cyber Security (CS) is the application of security measures for the protection of communication, information, and other electromagnetic systems and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability and non-repudiation[103]. See also CIS Security/Information Assurance above.

g. **Protective Security**. Protective security is the organized system of proactive measures instituted and maintained at all levels of command with the aim of guarding against and reducing the risk of TESSOC.

(1) **Physical Security**. That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorised access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage and theft.

(2) **Personnel Security**. That part of security concerned with measures designed to safeguard personnel. This also needs to include what is now being termed 'Digital Force Protection (DFP)'. The purpose of DFP being

[103] See AJP-3.20, *Allied Joint Doctrine for Cyber Operations*.

to give personnel the tools and knowledge they need to safeguard themselves, their information and ultimately, the organisation they work for.

(3) **Security of Information**. That part of security concerned with protection all forms of NATO information. It includes, but is not limited to, controlling classified documents using an approved registry system.

(4) **Security Procedures**. That part of security that denies an adversary insight into friendly tactics, techniques, and procedures.

(5) **Digital Force Protection**. The role that an individual plays within Protective Security with respect to protecting information and systems should not be neglected. The risk of compromise to information by a system can be mitigated with technology and to some extent by procedures. However, information compromised by an infected personal computer or by an inappropriate social media post is much more difficult to mitigate, but can be just as damaging. This perspective should be considered or the security of activity will be at risk of compromise. In the contemporary operating environment, DFP is just as important as other elements of FP (e.g., NATO differentiates between FP for medical and FP for IAMD; FP of the digital footprint requires equal treatment).

h. **Transport Security**. That part of security concerned with measures designed to safeguard transport operations, to prevent sabotage, damage and theft. Transport security describes the measures undertaken to screen passengers and cargo before, during and after transportation on NATO or NATO-chartered platforms. Due to the legal and procedural requirements involved, it is a specialist task normally conducted by Military Police or FP personnel. Transport security involves prevention of adversary and criminal actions against transport operations, but also prevention of carriage or loading by friendly and neutral personnel of dangerous and prohibited goods on different means of transport[104].

i. **Use of Stability Policing Assets in Force Protection**. Stability policing is a set of police-related activities intended to reinforce or temporarily replace the indigenous police in order to contribute to the restoration and/or upholding of public order and security, rule of law, and the protection of human rights. Stability policing assets are composed of police forces with military status and military police forces with a police background. They perform a wide spectrum of police activities well suited during recovery or for recuperation. As such, the

[104] See AJP-4.4, *Allied Joint Movements and Transportation Doctrine* and AJP-3.13, *Allied Joint Doctrine for the Deployment of Forces*.

stability policing assets are capable of performing the following tasks: public order control, patrolling, information gathering, criminal intelligence support, training, monitoring, mentoring and supporting of local police forces, policing and law enforcement, including combating organised crime and terrorism, war crime investigations, and crime prevention. Stability policing assets are integrated in the military structure and operate under the same ROE as the rest of the NATO-led force. The Provost Marshal is an essential advisor on all Policing matters, to include Stability Policing [105].

j. **Host Nation Security of Immediate Area Around Basing Operations**. Evaluation, integration, and additional training for HN security forces must take place to ensure base security is implemented and validated.

k. **Underwater Force Protection**. Underwater FP protects friendly ships and friendly waterside infrastructure against attacks by torpedo's, naval mines, swimmers, divers, submersibles, and underwater IEDs. Active measures include anti-submarine warfare and naval MCM by ships, harbour protection measures by ships and specialist maritime units, and the use of portable diver detection sonars. Passive measures include ship signature management and the use of physical obstructions such as booms and nets.

l. **Sub-Surface Force Protection**. An intelligent, capable and adaptable adversary will exploit every opportunity to attack the NATO force. This might include digging or tunnelling in order to gain access to a facility or target Alliance activity. Equally, pits, ducts and watercourses may be exploited by an adversary if they are not correctly secured and protected.

m. **Counter-Crime and Policing[106]**. That activity alongside security which seeks to prevent undermining of the physical, moral, or intellectual components of fighting power by organised or petty crime or failure to adhere to military law, regulations and discipline.

n. **Road Safety[107]**. Road safety contributes to maintaining the combat effectiveness of the force by preventing injuries and deaths in road traffic accidents and maintaining freedom of action on the roads. Road safety is thus an important element of FP. Road and driving standards, coupled with fatigue and/or ignorance and/or indiscipline can lead to significant attrition, and is often a major cause of injuries and deaths on operations. It includes elements of education and enforcement to create the desired protective effect.

---

[105] For further information on Policing, see AJP-3.21, *Allied Joint Doctrine for Military Police* and for Stability Policing see AJP-3.22, *Allied Joint Doctrine for Stability Policing*.
[106] For further information see AJP-3.21, *Allied Joint Doctrine for Military Police*.
[107] For further information see AJP-3.21, *Allied Joint Doctrine for Military Police*.

Intentionally blank

ANNEX B

Categories of Force Protection Measures, Actions and Tasks

B.1. **Procedural**. These involve operational or administrative procedures:

a. Operational measures such as Standard Operating Procedures (SOPs), boundaries, reporting, and Rules of Engagement (ROE).

b. Administrative measures such as written policies and instructions.

c. Business processes.

B.2. **Personnel**. These involve personnel security measures, such as:

a. Administrative measures including security clearances, screening, passwords, and access codes, in accordance with the access required to valued assets.

b. Physical protective measures such as body armour and individual and collective protective equipment. Physical protective measures, normally specified in SOPs, may also include special measures that are established to protect designated personnel.[108]

c. Collective physical protective measures such as alert states, timely warning and reporting, effective alarm systems, collective protection systems, and (hardened) protective shelters.

d. Health and safety measures such as vaccinations, prophylaxes, infectious disease briefings, mass casualty and quarantine plans, and local environmental advice.

e. Educational and training measures. These are based on the individual and collective knowledge and skills of individuals and units. They are implemented through individual and collective training.

B.3. **Materiel**.

a. Physical security measures, tasks, and activities to prevent unauthorized

[108] Depending on the threat, specially trained bodyguards and protection personnel and/or teams may be provided for the protection of designated and/or targeted personnel.

access such as security badges. Biometric[109] and forensic data to screen personnel for identity prior to installation access or while conducting patrol outside installations.

b. Physical protective measures such as splinter protective applique materials and CBRN protective coverings.

c. Engineering and technical measures to reduce risks such as selecting better or more appropriate materials, identifying suitable substitute materials or equipment, and adapting new technologies to existing systems.

d. Physical security measures to prevent unauthorized access to weapons or ammunition.

B.4. **Infrastructure**.

a. Physical security measures such as facility guards, fences, sensors, gates, lighting, and entry control points. Physical security safeguards against destruction, espionage, sabotage and organized crime.

b. Protective measures such as field fortifications, protective shelters, hardened buildings, barriers, and creating stand-off distances. This includes the defence, protection, and safe management of own ammunition storage areas. Development of protective infrastructure is one element of passive air and missile defence. Additionally, individual hardened sleeping cubicles will further protect sleeping personnel during indirect fire, missile, or air attacks.

c. Collective physical protective measures, such as active air and missile defence can help counter air and missile threats. Representative threats include aircraft, helicopters, remotely controlled systems, ballistic missiles and land attack cruise missiles. Furthermore, air defence assets able to counter rockets, artillery, and mortars can enhance protection for infrastructure, facilities and personnel.

B.5. **Information**.

a. The security of information is safeguarded by complementary procedural, personnel, physical, and information security measures. Communication and

---

[109] The NATO Biometrics Framework Policy National Requirements Statement (NRS) is a tool for Allies to communicate any national restrictions or caveats from a legal and technical perspective. The NRS allows Allies to provide relevant input on legal parameters to their participation in NATO Biometrics. Allies collecting biometric information during NATO Operations are encouraged to submit an NRS.

Information Systems (CIS) security, Information Security (INFOSEC), and cyber defence, include security measures to protect information processed, stored or transmitted in communication; to protect information and other electromagnetic systems against loss of confidentiality, integrity, or availability, whether accidental or intentional; and to prevent loss of integrity or availability of the systems themselves. This includes preventing the unauthorized use of storage media such as flash drives and other Universal Serial Bus (USB) devices. Measures include, but are not limited to communications security, emission security, and computer systems security.

b. Other activities that contribute to the security of information include electromagnetic protection (a part of Electromagnetic Warfare (EW)) and Operations Security (OPSEC).

c. Deception involves the active measures taken to create doubt, confusion or false certainty in the mind of adversary, or potential adversary, decision makers regarding NATO plans, capabilities, and intent. This in turn will cause the adversary to act in a way that favors NATO's operation. Deception measures play a critical role in Force Protection (FP) by delaying adversary actions or causing them to occur at the wrong location, thus increasing the security of friendly forces.

Intentionally blank

LEXICON PART 1 – ACRONYMS AND ABBREVIATIONS

AAAD	All Arms Air Defence
AASTP	Allied Ammunition Storage and Transport Publication
AAW	Anti-Air Warfare
ACC	Air Component Command
ACO	Allied Command Operations
AJP	Allied Joint Publication
ALP	Allied Logistics Publication
BACO	Baseline Activities and Current Operations
BSM	Battlespace Management
CAPP	Critical Assets Protection Plan
C2	Command and Control
CBRN	Chemical, Biological, Radiological and Nuclear
CCIR	Commanders Critical Information Requirement
CCOMC	Comprehensive Crisis and Operations Management Centre
CCTV	Closed Circuit Television
CDAL	Cyber Defended Assets List
CI	Counter-Intelligence
C-IED	Counter-Improvised Explosive Device
CIMIC	Civil-Military Cooperation
CIS	Communication and Information Systems
CJEDOC	Combined Joint Explosive Ordnance Disposal Cell
CJTF	Combined Joint Task Force
CM	Countermeasure
CNA	Computer Network Attack
CND	Computer Network Defence
COA	Course of Action
COM JFAC	Commander Joint Force Air Component
COM JFC	Commander Joint Force Command
CoRe	Collaborative Resilience
CoS	Chief of Staff
COPD	Comprehensive Operational Planning Directive
CPERS	Captured Persons
CS	Cyber Security
C-RAM	Counter-Rockets, Artillery and Mortars
CR-SGBV	Conflict-Related Sexual and Gender-Based Violence
C-UAS	Counter-Unmanned Aircraft System
DCO	Defensive Cyber Operation
DFP	Digital Force Protection
DNBI	Disease and Non-Battle Injuries

ECM	Electromagnetic Countermeasures
EIH	Environmental and Industrial Hazards
EMB	Electromagnetic Battlestaff
EO	Explosive Ordnance
EOC	Essential Operational Capability
EOD	Explosive Ordnance Disposal
ESO	Explosives Safety Officer
ESMRM	Explosives Safety and Munitions Risk Management
EW	Electromagnetic Warfare
EWCC	Electromagnetic Warfare Coordination Centre
FHP	Force Health Protection
FP	Force Protection
HN	Host Nation
HNS	Host-Nation Support
HQ	Headquarters
IAMD	Integrated Air and Missile Defence
IC	International Community
ICCS	Individual Common Core Skills Training
ICP	Intelligence Collection Plan
ICP	Incident Command (or Control) Post (use specific to FP)
IDS	Intruder Detection System
IED	Improvised Explosive Device
IEDD	Improvised Explosive Device Disposal
Info Ops	Information Operations
INFOSEC	Information Security
IO	International Organization
ISAF	International Security Assistance Force (Afghanistan)
JFAC	Joint Force Air Component
JFC	Joint Force Command
JIPOE	Joint Intelligence Preparation of the Operating Environment
JLSN	Joint Logistics Network
JLSG	Joint Logistic Support Group
JOA	Joint Operations Area
JPR	Joint Personnel Recovery
JSEC	Joint Support and Enabling Command
KLT	Key Leader Training
LCC	Land Component Command
LOC	Lines of Communication

MC	Military Committee
MCC	Maritime Component Command
MCM	Mine Counter-Measures
MILENG	Military Engineering
MLE	Maximum Level of Effort
MOU	Memorandum of Understanding
MP	Military Police
NATO	North Atlantic Treaty Organization
NA5CRO	Non-Article 5 Crisis Response Operations
NCRSM	NATO Crisis Response System Manual
NEO	Non-Combatant Evacuation Operations
NGO	Non-Governmental Organization
NIC	NATO International Civilian
OE	Operating Environment
OPSEC	Operations Security
OPLAN	Operation Plan
OPORD	Operations Order
OPP	Operations Planning Process
PA	Public Affairs
PDT	Pre-Deployment Training
PE	Peacetime Establishment
PIR	Priority Intelligence Requirement
PM	Provost Marshal
PoC	Protection of Civilians
POLAD	Political Advisor
PR	Personnel Recovery
PsyOps	Psychological Operations
ROE	Rules of Engagement
RSOM	Reception, Staging and Onward Movement
SA	Situational Awareness
SBAMD	Surface-Based Air and Missile Defence
SC	Strategic Commander
SEA	Sexual Exploitation and Abuse
SEWOC	Signals Intelligence/Electromagnetic Warfare Operations Centre
SME	Subject Matter Expert
SOFA	Status of Forces Agreement
SOP	Standard Operating Procedures
StratCom	Strategic Communications

TA	Threat Assessment
TAOR	Tactical Area of Responsibility
TBMD	Theatre Ballistic Missile Defence
TCN	Troop-Contributing Nation
TESSOC	Terrorism, Espionage, Subversion, Sabotage, and Organised Crime
TIH	Toxic Industrial Hazard
TIM	Toxic Industrial Material
TTP	Tactics, Techniques and Procedures
USB	Universal Serial Bus
UXO	Unexploded Explosive Ordnance
W&R	Warning and Reporting
WMD	Weapons of Mass Destruction

LEXICON PART 2 – TERMS AND DEFINITIONS

Area Damage Control
Measures taken before, during or after hostile action or natural or man-made disasters, to reduce the probability of damage and minimize its effects.
(NATOTerm – NATO Agreed)

Asymmetric Threat
A threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain a disproportionate result.
(NATOTerm – NATO Agreed)

Chemical, Biological, Radiological, and Nuclear 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.
(Definition for the purposes of this publication only)

Consequence Management
Actions taken to maintain or restore essential services and to lessen the effects of natural or man-made disasters.
(NATOTerm – NATO Agreed)

Countering-Improvised Explosive Devices
The collective efforts to defeat an improvised explosive device system by attacking networks, defeating devices, and preparing a force.
(NATOTerm – NATO Agreed)

Counter-Intelligence
Those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion, or terrorism.
(NATOTerm – NATO Agreed)

Conflict-Related Sexual and Gender-Based Violence
Any sexual and/or gender-based violence against an individual or group of individuals, used or commissioned in relation to a crisis or an armed conflict.
(NATOTerm – NATO Agreed)

Cyberspace
The global domain consisting of all interconnected communication, information technology and other electromagnetic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.
(NATOTerm – NATO Agreed)

Electromagnetic Countermeasures
Measures to prevent or reduce an adversary's effective use of the electromagnetic spectrum through the use of electromagnetic energy.
(NATOTerm - NATO Agreed)

Electromagnetic Warfare
Military action that exploits electromagnetic energy to provide situational awareness and create offensive and defensive effects.
(NATOTerm - NATO Agreed)

Explosive Ordnance Disposal
The detection, accessing, uncovering, identification, mitigation, rendering safe, recovery, exploitation and final disposal of explosive ordnance, regardless of condition. Note: Explosive ordnance disposal extends to explosive remnants of war and stockpiles, or other explosive ordnance that has become hazardous by damage or deterioration.
(NATOTerm – NATO Agreed)

Force Protection (1)
All measures and means to minimize the vulnerability of personnel, facilities, equipment and operations to any threat and in all situations, to preserve freedom of action and the operational effectiveness of the force.
(NATOTerm – NATO Agreed)

Force Protection (2)
All measures and means to minimize the vulnerability of personnel, facilities, equipment, materiel, operations, and activities from threats and hazards in order to preserve freedom of action and operational effectiveness of the force, thereby contributing to mission success.
(MC-0656)

Host Nation
A nation which, by agreement: a. receives forces and materiel of NATO or other nations operating on/from or transiting through its territory; b. allows materiel and/or NATO organizations to be located on its territory; and/or c. provides support for these purposes.
(NATOTerm – NATO Agreed)

Host-Nation Support
Civil and military assistance rendered in peace, crisis or war by a host nation to NATO and/or other forces and NATO organizations that are located on, operating on/from, or in transit through the host nation's territory.
(NATOTerm – NATO Agreed)

Incident Response
Measures taken to neutralize, isolate, contain, and/or resolve a specific threat or act to minimize its effects on mission success, individuals, units, and facilities.
(Definition for the purposes of this publication only)

Information Operations
A staff function to analyse, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and audiences in support of mission objectives.
(NATOTerm – NATO Agreed)

Information Operations Staff Element
A staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and audiences approved by the North Atlantic Council in support of Alliance mission objectives.
(*This is a new term and definition being processed for NATO Agreed status via terminology tracking file 2007-0400.*)

Insider Threat – Generic Description
An insider threat is a malicious threat to an organisation that comes from people within the organisation, such as employees, former employees, contractors or business associates, who have inside information concerning the organisation's security practices, data and computer systems.
(Wikipedia)

Insider Threat – ACO Definition
An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and CIS. The threat may involve fraud, theft of information, intellectual property, or the sabotage of CIS. Note: Threats from 'insiders' are not necessarily kinetic inn nature.
(SHAPE)

Insider Threat – US National Definition
A person, known or suspected, who uses their authorized access to Department of Defense facilities, systems, equipment, information or infrastructure to damage, disrupt, operations, commit espionage on behalf of a foreign intelligence entity or support international terrorist organizations.
(US Department of Defence)

Insider Threat – Cyber Related
An insider can be a member of an organization, an associate (contractor, business partner or guest), anyone with authorization to perform certain activities, anyone who is authenticated by the system (including unauthorized users using valid credentials), or an unwilling or coerced accomplice to an external actor. A person who has stopped being an associate or member of a certain organization can still be considered as an insider if that person's credentials have not been properly revoked or the person is (mis)using previously acquired knowledge.
(NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) paper: 'Insider Threat Detection Study')

Insider
An insider is a person who has a position of trust within an organization or access to personnel, facilities, and equipment. Insiders could be fellow non-NATO coalition personnel, TCN personnel, host-nation security force personnel, trusted host nation civil government personnel or anyone granted access to NATO personnel, facilities, and equipment.
(ATP-3.16.1)

Mental Threats
Mental is of or involving the mind or an intellectual process. A threat is a statement of an intention to cause pain, injury, damage or other hostile action. Threatening behaviour includes: Verbal, written or psychological harassment. Threats of a sexual nature. Threats to kill.
(Definition for the purposes of this publication only)

Military Engineering
A function in support of operations to shape the physical operating environment.
(NATOTerm – NATO Agreed)

Operations Security
The process which gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities and intentions of friendly forces.
(NATOTerm – NATO Agreed)

Physical Security
That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, documents and information and to protect them against espionage, sabotage, terrorism damage, and theft.
(NATOTerm – NATO Agreed)

Protect Capability
The capability to minimize through a common multinational and holistic approach to FP, the vulnerability of personnel, facilities, materiel and activities to any threat and in all situations, to include towards the effects of Weapons of Mass Destruction, whilst ensuring the Allies freedom of action and contributing to mission success. During deployed operations, it includes lines of communication and lines of supply and cyber space.
(MC-400/3)

Recuperation
Covers those measures necessary for the force to recover from the effects of attack, restore essential services, and enable operations to continue, with the minimum of disruption.
(Definition for the purposes of this publication only)

Remote Controlled
(of a machine or apparatus) controlled from a distance by means of radio or infrared signals transmitted from a device.
(COED)

Remotely Operated System
A remotely operated system is defined as any systems teleoperated by a means that does not restrict its motion with an origin external to the device. This is often a radio control device, cable between control and system, or an infrared controller. A remote-control system (RCS) differs from a robot in that the RCS is always controlled by a human and takes no action autonomously.
(Definition for the purposes of this publication only)

Resilience
The ability of an entity to continue to perform specified functions during and after an attack or an incident.
(NATOTerm - NATO Agreed)

Risk
The probability and severity of a potential loss linked to hazards and threats.
(Definition for the purposes of this publication only)

Force Protection Risk
Those threats or hazard-based events that may occur that could result in loss of life, life-changing injury/illness or loss of capability and thus, have an effect on Mission Accomplishment.
(Definition for the purposes of this publication only)

Risk Assessment
The identification and assessment of threats and hazards as part of the first two steps of the risk management process.
(Definition for the purposes of this publication only)

Risk Management
The process of identifying, assessing, and controlling risks arising from operational factors, and making informed decisions that balance risk cost with mission benefits.
(NATOTerm – NATO Agreed)

Risk Attitude
The specified amount and type of risk that the organization may or may not take, relative to objectives.
(This is a new term and definition being processed for NATO Agreed status via terminology tracking file 2022-0155.)

Route Clearance
The detection and, if found, the confirmation, identification, marking and neutralization, destruction or removal of explosive ordnance and non-explosive obstacles threatening a defined route to allow a military operation to continue with reduced risk.
(NATOTerm – NATO Agreed)

Rules of Engagement
Directives to military forces, including individuals, that define the circumstances, conditions, degree, and manner in which force, or actions which might be construed as provocative, may be applied.
(NATOTerm – NATO Agreed)

Security Alert State
An alert state or state of alert is an indication of the state of readiness of the armed forces for military action or a state against terrorism or military attack.
(Definition for the purposes of this publication only)

Sexual Exploitation and Abuse
Occurs when people abuse a position of power against people with less power or an inability to consent. Usually refers to actions committed by members of an organization (often with a protection mandate) against members of the local civilian population.
(NATO Military Guidelines on the Prevention of, and Response to, Conflict-Related Sexual and Gender-Based Violence)

Intentionally blank

AJP-3.14(B)(1)

Published by the Ministry of Defence
This publication is available at www.gov.uk/mod/dcdc