NATO STANDARD

AJP-3.14

ALLIED JOINT DOCTRINE FOR FORCE PROTECTION

Edition A Version 1

APRIL 2015

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

Published by the

NATO STANDARDIZATION OFFICE (NSO)

© NATO/OTAN

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

2 April 2015

1. The enclosed Allied Joint Publication AJP- 3.14, Edition A, Version 1, ALLIED JOINT DOCTRINE FOR FORCE PROTECTION has been approved by the nations in the MCJSB, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2528.

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

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

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

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATIONS BY NATIONS

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

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

NATION	DETAILS OF RESERVATIONS
BEL	1. Current Belgian legislation prevents some of its Armed Forces personnel of collecting, analyzing, monitoring and/or forwarding biometrics data. Whilst rectification of these limitations is ongoing, BEL reserves itself the right to not have (part of) its Forces act IAW STANAG 4175. 2. The structural design of the BEL Armed Forces does not fully reflect all attributions, listed as part of each of the 8 Force Protection fundamental elements. Therefore, BEL reserves itself the right to alter such attributions and/or merge 2 or more of the defined fundamental elements.
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.
LVA	In LNAF Fire Protection is not under responsibility of military engineers. In case of HNS, GBAD capability is very limited.
NLD	The Netherlands will reserve its position on the implementation of the Alert States. As described in para 0105.a, “a threat assessment (TA) based on accurate and timely all-source intelligence serves as the basis for the selection of the proper NATO security alert state and associated FP measures”. The position of the Netherlands is that based on a specific threat a corresponding specific alert measure of an Alert States will be considered, agreed and implemented, thereby not necessary increasing the overall Alert State.
TUR	1. As Turkish Armed Forces does not have authority to respond any security incidents that occur outside of base ; In case of security incident outside of base, local authority (local police and gendarmerie) will be notified and make them respond. 2. In case of deployment or mobile duty, route security is conducted by local authority and route clearance (the detection and, if found, the identification, marking and neutralization, destruction, or removal of mines or other explosive ordnance) will be conducted by personnel

	who was trained and authorized, after having permission of local authority. 3. Turkish Air Force is going to have ability by the beginning of 2016 for Collective Protection, Medical Countermeasures especially Toxic Industrial chemicals and materials (TIM and TIC). Also TOXIC Industrial Materials (TIM) to be used in hazard prediction and also decided upon by NATO states will be integrated into the CBRN Hazard Prediction programme in communications management module that is used by Turkish Air Force.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

TABLE OF CONTENTS

PREFACE

0001. North Atlantic Treaty Organization (NATO) forces routinely operate as expeditionary forces engaged in Allied joint operations which occur both within and outside of the territory of NATO Member States. The operational environment may have no discernible “front-lines” or “rear area” and an adversary may be expected to target Allied vulnerabilities anywhere with a wide range of capabilities. Security, one of the principles of operations, and protection, a key component of security, assumes an even higher importance in such an environment. This doctrine provides the framework for the comprehensive protection of personnel, assets, and capabilities. Although Allied Joint Publication (AJP)-3.14(A), *Allied Joint Doctrine for Force Protection* is primarily intended for use by commanders at the operational level during joint operations, it can be used as a reference at any level to include during peacetime, on national territory, and NATO infrastructure for host nations (HNs).

0002. The purpose of this publication is to describe the fundamental aspects of force protection (FP) and provide guidance on the planning and implementation of FP, primarily at the joint operational level, but it can be used at any level. FP is complex and starts with situational awareness and understanding. FP for Allied joint forces starts with preparation to deploy and continues during deployment, employment, and redeployment. FP covers not only military personnel of the joint force; it may also include some support to non-military personnel, contractors, civilians, or non-governmental organizations and their facilities.

0003. The importance of FP for NATO-led forces is reflected in Military Committee (MC) 400/3, *Military Committee Guidance for the Military Implementation of Alliance Strategy*, as a main capability area. FP is, therefore, a basic duty of all NATO personnel. Commanders are responsible for all aspects of FP for their assigned forces. Troop contributing nations are responsible for providing their own FP, as well as for contributing to and integrating into the wider FP plans of the Allied joint force to which they are assigned. NATO HNs, in concert with Allied commanders and contributing nations, are responsible for FP support for in-country NATO-led forces. Non-NATO HNs and local authorities in the area of operation may or may not be able to provide FP assistance to Allied forces.

0004. FP covers a diverse range of measures and capabilities. This publication addresses those capabilities that are deemed fundamental or core FP considerations, as well as other common measures within the FP spectrum. FP needs to balance the conflicting priorities of the need to preserve force capability 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 activity 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.

0005. NATO-led forces are particularly vulnerable during the onset of operations when infrastructure is not yet in place and information on the situation is incomplete. In the absence of a common threat to all regions, local threat levels may be established to focus FP efforts. Commanders should assess the vulnerability of their assets and facilities and provide FP measures, tasks, and activities as appropriate. FP should be based upon effective risk management – that of minimizing risk to forces. An unrealistic expectation to avoid all risk may impact adversely on the accomplishment of the mission and, if casualties should occur, undermine political and military resolve. Commanders, therefore, should balance the risk to their forces against mission imperatives.

0006. Commanders should establish FP awareness within their staff and provide suitable advice and direction to subordinate commands and forces. FP should be fully integrated and coordinated in the operations planning process from the outset. Appropriate 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 operations, FP principles always apply during the execution of operations.

0007. Within the Allied Joint Doctrine Architecture, AJP-3.14 is directly subordinate to AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, which describes the fundamental operational aspects of joint operations and provides guidance on conducting joint operations.

CHAPTER 1 - FUNDAMENTALS OF FORCE PROTECTION

0101. **Introduction**. The survivability of any NATO-led joint force is a principal consideration in strategic 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 hazards and threats to include activity-related hazards such as road traffic accidents and fire, and exposure to environmental hazards such as disease and toxic industrial hazards (TIHs). A threat may be described as having the perception of being in some degree of danger based on an overall assessment of the situation, taking into account own and adversary's capabilities, previous adversary actions, hostile intentions, etc. 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, giving rise to the need for a comprehensive and resilient strategy for the protection of forces. Therefore, all military units must be able to defend and protect themselves appropriately against prevailing threats and hazards across a range of military activities throughout predominant campaign themes.[1]

0102. **Definition of Force Protection**. 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 thereby contributing to mission success.

0103. **Force Protection Applicability**. FP is a joint function and essential to all operations.[2] All of the joint functions need to be considered by the joint force commander (JFC) in determining the capabilities required for each operation. Nations have differing FP philosophies, policies, and priorities; however, the focus for FP is united: the protection of a national contingent itself plus supporting elements and enabling the force to conduct its mission unimpeded by the actions of an adversary. In a multinational force, differences should be reconciled, taking into consideration national caveats, and an overall combined joint FP policy should be established, along with appropriate tactics, techniques, and procedures (TTP), to facilitate unity of effort and enhance FP measures.

---

[1] In accordance with MC 400/3, *Military Committee Guidance for the Military Implementation of Alliance Strategy*, force protection is an element of the Main Capability Area (MCA) “protect”.

[2] The other joint functions are command and control, intelligence, manoeuvre and fires, information operations, sustainability, and civil-military cooperation. 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*.

0104. **Force Protection Coordination**. Coordination is a FP fundamental during the planning and execution phases of all campaigns and operations. Vertical and horizontal coordination among strategic, operational, and tactical levels of command allows each level to take appropriate FP measures according to the mission and threat, while providing understanding of the intentions and FP capabilities of each level. Vertical coordination ensures that the higher commander's intent with respect to the protection and conservation of assets is clearly understood, and reflected in orders and plans. Horizontal coordination assists in integrating and synchronizing the various inputs from the different staff disciplines during mission planning. Since each level of command is required to implement FP measures, tasks, and activities based on the mission and threat, the same measures, tasks, and activities may not necessarily be implemented by all units in the same theatre. Therefore, coordination across all levels should assist in providing adequate and synchronized FP. During mission execution, horizontal coordination between subordinate formations and the staff should be conducted so that FP measures, tasks and activities are integrated, synchronized, and implemented in a consistent and systematic manner. Ideally, there should be a corresponding FP staff assignment within strategic, operational, and tactical level headquarters (HQ).

a. **Strategic Level Coordination**. At the strategic level, the Allied Command Operations J-3 provides the necessary staff structure and the J-3 operations branch coordinates FP. An officer from the J-3 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 operations plans (OPLANs). 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 operations will be based on a comprehensive approach, synchronization of FP activities with allies, coalition partners, and other actors is essential to ensure maximum effectiveness. The J-3/J-5 staffs assist the operational commander in the coordination and planning of FP measures, tasks, and activities.

c. **Tactical Level Coordination**. At the tactical level, the unit operations officer is normally responsible for coordinating FP, in accordance with the commander's intent, with advice from the intelligence officer, information operations (Info Ops) officer, security officer, communication and information systems (CIS) officer, medical officer, engineers, and other

key stakeholders. However, some situations may require the designation of a dedicated FP officer and staff to coordinate FP requirements.[3]

0105. **Force Protection Principles**. The analysis of the mission and the commander's intent provide the starting point for the identification of the FP requirements and procedures. FP then aims specifically to conserve the fighting potential of NATO-led forces by countering the wider threat to all of its elements from adversary, natural and man-made hazards, and fratricide. As such, FP should be guided by the following principles:

R a. **Measured Assessment of the Threat**. A threat assessment (TA) based on accurate and timely all-source intelligence serves as the basis for the selection of the proper NATO security alert state and associated FP measures.[4] FP allows the commander to focus resources on the protection of assets that are critical to mission success. A continuous evaluation of threats and hazards is required to enable commanders to adjust force posture and protective measures, while maintaining economy of effort. The TA also provides the JFC with situational awareness (SA) that reduces the probability of surprise, enhances decision making, and enables effective management of the operational environment (OE) thus enhancing the overall effectiveness of the force.[5] It requires the fusion of information and intelligence from a variety of sources, both military and civilian.

b. **Risk Management**.[6] FP should be based on risk management, not risk elimination. Casualties, deliberate or accidental, are a reality of military operations, and the desire to avoid them totally may impact adversely on the accomplishment of the mission. This requires a balance between risk mitigation and mission accomplishment, resulting in risk acceptance known to the joint force and contributing nations' commanders. The willingness to accept risk is scenario-dependant. The risks from threats, hazards, and other vulnerabilities should be continuously re-evaluated to ensure appropriate FP at all times. Effective FP planning requires integrated hazard and threat identification, risk analysis, and risk management. Although it is not possible to protect every asset against every threat all of the time, those assets previously identified as "critical to the mission" must be protected.

[3] This includes static locations such as deployed operating bases and compounds, airports, and seaports.
[4] For more on security alert states, see AJP-2.2, *Counter-Intelligence and Security Procedures*.
[5] For more details, see AJP-3, *Allied Joint Doctrine for the Conduct of Operations*.
[6] The risk management process is an integral part of the overall FP planning process and a comprehensive risk assessment is essential to guide risk management decision-making and prioritization. For more on the risk management process, see Annex B of this publication.

c. **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, coalition partners, and the host nation (HN) to ensure interoperability.

d. **Prioritisation**. FP balances the conflicting priorities of the need to preserve force capability 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 force centres of gravity, both tangible, such as lines of communications (LOCs), 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.

e. **Flexibility**. FP policy and measures should be developed with the capability to respond to a rapidly changing threat, within resource limitations. The aim of FP is to counter and mitigate the effects from threats and hazards. To be effective, FP requires a core policy that has the flexibility to allow the operational forces 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.

0106. **Force Protection Coordination Areas and Fundamental Elements**[7]

a. **Force Protection Coordination Areas**. The FP coordination areas are active, passive, and recuperation.

(1) **Active**. The active coordination area involves measures, tasks, and activities to deter, prevent, nullify, or reduce the effectiveness of an enemy attack and to counter hazards. These are primarily proactive in nature with the core functions to provide a defence against a perceived or actual threat, and when necessary, find, fix, and strike threats and hazards before they are realised, with the intention to further exploit the situation wherever possible. The employment of individual FP fundamental elements should be in

[7] 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.

accordance with the mission mandate, Rules of engagement (ROE), and standing operating procedures (SOPs). It is about taking the battle to the aggressor and either deterring hostile intent or neutralising the ability to attack or pose a viable threat.

(2) **Passive**. The passive area involves measures, tasks, and activities to negate or minimize the effects of enemy attacks and hazards on NATO assets by making them more survivable. Passive measures, tasks, and activities should be proactively employed prior to any attack or hazard materializing. They are designed to protect the force from the operational, tactical, and physiological consequences arising from the use of both conventional and chemical, biological, radiological, and nuclear (CBRN) weapons and devices or the release of toxic industrial material (TIM). A force's ability to survive the effects of such weapons or devices should be enhanced by the anticipation of their use. Furthermore, effective passive defence preparation will be likely to reduce an aggressor’s incentive to use such measures.

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

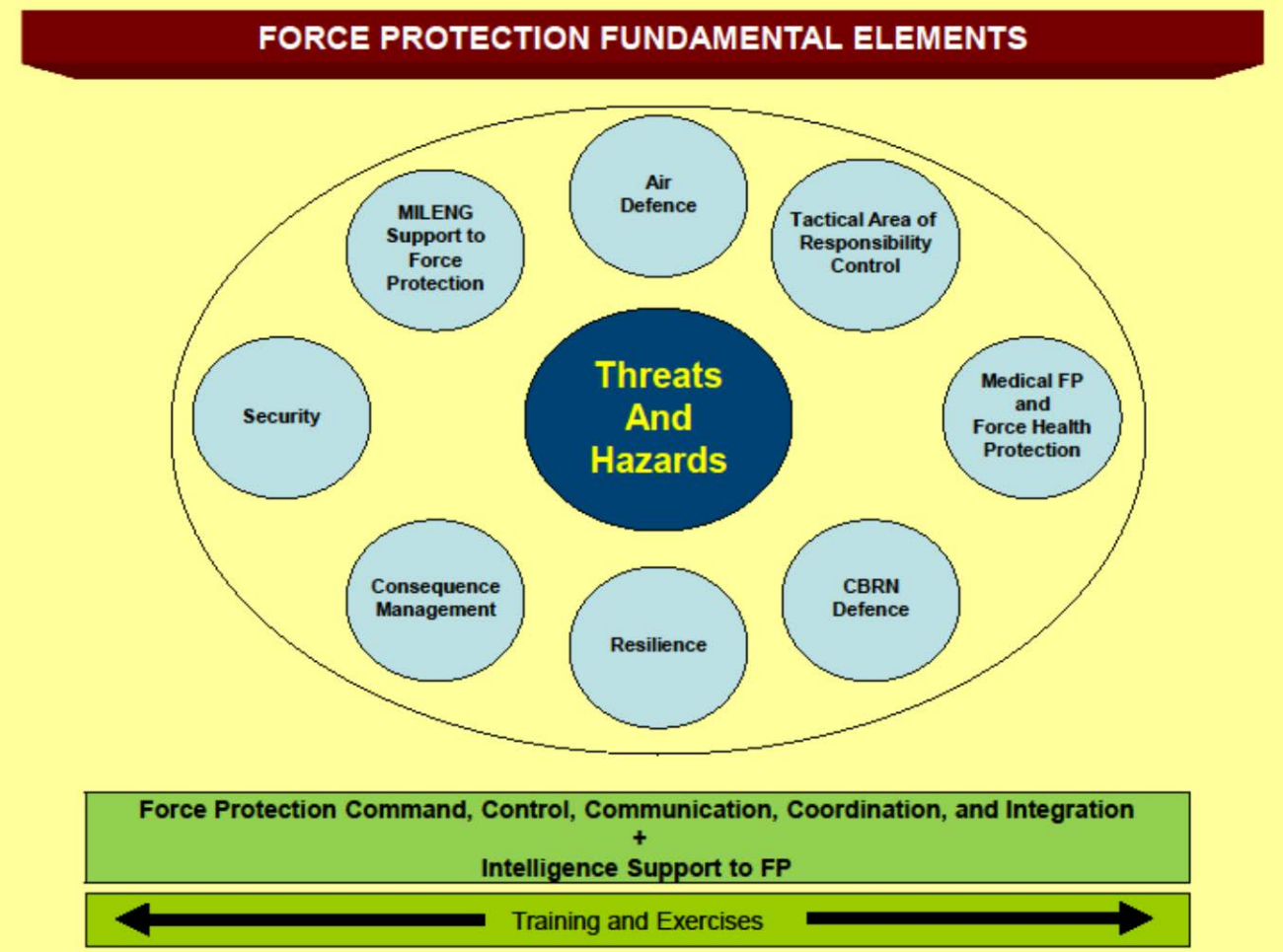


Figure 1.1 - Force Protection Fundamental Elements

b. **Force Protection Fundamental Elements**. FP comprises a number of distinct but inter-related fundamental elements, as illustrated in figure 1.1, which may contribute to the overall FP function. While some are focused on only one of the coordination areas discussed above, many can potentially provide FP measures, tasks, or activities in any of the three coordination areas. The contribution of these fundamental elements will be determined by the OE, for instance, by the threat, scale of the operation, climate, civil environment, the composition of the NATO-led force, and the availability of host-nation support (HNS) or support of local security forces. Annex A provides details about how the FP fundamental elements contribute to providing FP for the joint force.

c. **Force Protection Command, Control, Communication, Coordination, and Integration**. FP is a combination of individual skills, unit procedures and resources, and specialist support. However, it is ultimately the NATO commander's responsibility, and there are different options which provide

a means to achieve FP command, control, communication, coordination, and integration (C4I). FP functions require NATO forces to have robust and flexible command and control (C2) capabilities to provide effective FP C4I to minimize any disruption to operations. Where appropriate, FP cells may be established to address the requirements of the HQ. Since FP organizational structure is developed based on the threat, command and unit FP C4I should also be able to surge to handle any future additional capability. During NATO operations at the strategic or operational level, a FP staff officer or FP working group will normally be established to coordinate the planning and execution of all FP requirements. Additionally, a FP C2 element may be necessary to coordinate the employment of the individual capabilities and disciplines. The size of this element will be defined by the scale of the operation and may vary from a single FP officer through a small FP cell to a large and complex FP HQ element. In this way, FP can be fully integrated and seamlessly delivered thereby providing maximum effectiveness in a resource efficient manner.

d. 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 NATO commander in the area of operations. At the core of FP planning is the requirement of the commander to prioritise, accept, and manage risk. This balance between risk and mission accomplishment is covered later in Chapter 3 of this publication.

0107. **Civil Environment Considerations**. The attitude of NATO-led forces toward the civil population and their authorities could significantly affect how they are regarded and ultimately, the success of an operation. It is therefore important for members of the NATO-led force to conduct themselves in a proper and appropriate manner while considering and respecting the local culture. Consequently, Allied forces should understand and respect the history, customs, traditions, and current environmental conditions in the operational area in accordance with theatre policy. In parallel, information on the background and the underlying motives of local stakeholders and interest groups 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 organizations (IOs), non-governmental organizations (NGOs) and foreign non-military governmental organizations are a potential source and recipient for sharing indications and warnings of any kind.

INTENTIONALLY BLANK

CHAPTER 2

FORCE PROTECTION RESPONSIBILITIES AND COMMAND AND CONTROL

0201. **Introduction**. Commanders are responsible for FP within their operational areas. FP demands, above all, the effective coordination of all FP fundamental elements and related assets. The commander provides clear FP direction and guidance to the staff and subordinate forces to initiate operations planning and provide consistency in applying FP measures, tasks, and activities. It is essential that authorities, responsibilities, and accountabilities for FP be clearly articulated at all levels of command.

0202. **Responsibilities**. FP is a core responsibility at every level of command and commanders should balance protection with mission accomplishment. Specific FP responsibilities are identified below:

a. **Commands**. While authorities may be delegated within the chain of command, the strategic commander (SC) remains ultimately responsible and accountable for all aspects of FP for assigned forces. National caveats to the NATO ROE profile may significantly limit the range of FP measures, tasks, and activities available to the commander.

b. **NATO Military Forces**. FP measures should be applied to HQ and subordinate commands, elements, and command/assigned units, and applied by all personnel. To be effective, FP should be clearly understood as a fundamental responsibility of all personnel at all times.

c. **Troop Contributing Nations**. Troop contributing nations (TCNs) are responsible for providing their own FP, and for contributing to the wider protection of the NATO-led force to which they are assigned. TCNs should inform the JFC if their FP concepts, doctrine, or capabilities differ significantly from that prescribed by NATO, the assigned command, or are otherwise considered deficient.

d. **Host Nations**. HNs, in concert with the JFC, may be responsible for FP for TCN forces located within their sovereign borders in accordance with supplementary agreements, established memoranda of understanding (MOUs), technical arrangements, OPLANs, contingency plans, and operation orders (OPORDs). 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 of FP, commanders must take into consideration shortfalls in ability, availability, reliability, or standard of execution from HN services, and make necessary plans and arrangements to mitigate such shortfalls.

e. **Theatre/Area of Operations Ownership and Responsibility**. The responsibility for actions or reactions to events throughout the entire theatre/area of operation should be assigned upon arrival in the area of operations. As such, commanderst, in close coordination with FP staff elements, determine the FP measures, tasks, and activities required and then assign responsibility to the appropriate contributing fundamental elements or other assets, thereby de-conflicting responsibilities.

0203. **Force Protection Guidance and Direction**

a. Commanders provide the necessary direction, guidance, and support to focus the staff on anticipated FP requirements. Most, but not all, FP fundamental elements already exist in military organizations, as do the C2 functions to implement the overall measures, tasks, and activities. All measures, tasks, and activities within the FP spectrum should be considered, even though some may be pursuing other aims as a primary function to create effects required for a given operation. 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 JFC is responsible for the FP of the deployed NATO-led force, routine coordination and integration of FP 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 threats, vulnerabilities and their own FP posture, and take appropriate corrective action when required.. In this respect, the threat analysis process is a continuous one. The FP posture of Allied and friendly forces is also an important component of overall situational awareness and understanding at all levels of command, and should be included in the common operational picture, while respecting the sensitivity of this information. Commanders define their FP requirements through appropriate directives and instructions that may include:

(1) Threat / risk assessments and prioritisation, including risk acceptance and accountability.

(2) Capabilities and resources.

(3) Manning, including readiness states and use of augmentees.

(4) Command and staff responsibilities.

(5) C2 and CIS.

(6) Warning and reporting requirements.

(7) Plans and procedures.

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

(9) Legal aspects and national caveats.

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.

0204. **Continuous Assessment**. Commanders and staffs should use all available means and tools to identify FP deficiencies and shortcomings. Some examples include operational and FP inspections, evaluations, assessments, surveys, and exercises. 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.

0205. **Staff Functional Disciplines**. FP should be planned, coordinated, and integrated within the overall operation. Each of the functional specialties that support FP should be carefully considered and synchronized by the appropriate staff element as described below.

a. **Intelligence**. The J-2 is responsible for providing accurate, timely, and relevant intelligence to meet the JFC's security requirements within the JOA to maintain situational awareness and understanding.[8] An integrated Allied joint TA is the first step in consolidating threat and risk assessments for FP and should be coordinated by the strategic and operational level J-2 as part of the operations planning process (OPP). Additional localized TAs may need to be conducted, particularly in crisis response operations (CRO), 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. The ICP is a detailed breakdown of how each intelligence requirement is to be satisfied. Normally in matrix or table form, it indicates by which means an intelligence requirement can be best satisfied, the frequency of coverage required and the type of product expected. This includes the capability to fuse biometrics enabled intelligence and suspicious activity reports from military security, law enforcement, and counterintelligence (CI) organizations with level intelligence, surveillance, and reconnaissance collection activities.[9]

b. **Operations**. The J-3 acts as the focal point through which the JFC directs the conduct of an operation, ensuring unity of effort and the most effective use of resources. The J-3 provides the C2 organization necessary to conduct FP operations, monitors the current status of forces, and keeps the JFC informed about the prevailing situation. The J-3 directs the following functional specialties within the J-3 staff to ensure FP within the JOA.

(1) **Security**. Security, in the context of FP, encompasses those measures, tasks, and activities necessary to achieve protection against terrorism, espionage, subversion, sabotage, and organized crime (TESSOC), cyber intrusion, insider threats, and direct and indirect attacks on personnel, equipment, installations, and LOC. Security covers physical and procedural measures directed at the

[8] Including intelligence surveillance target acquisition and reconnaissance (ISTAR) and command and control, intelligence, surveillance and reconnaissance (C^2ISR). 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*.

[9] The collection, use (to include fusion with other intelligence), storage and dissemination of biometric data are controversial in many nations, and national legislation might limit individual TCNs from taking part in, or contribute to, this process. Information about national reservations is of importance in the planning of FP in operations.

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) **Chemical, Biological, Radiological, and Nuclear Defence**. The CBRN defence staff plans and organizes the activities to prevent, protect, and recover from adverse effects on operations and personnel resulting from CBRN incidents.[10] 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 materials into the environment.[11]

(3) **Air Defence**.[12] Air defence operations protect friendly forces and vital interests from air and missile attacks and include both active and passive measures. Active air defence involves defensive actions taken to destroy, nullify, or reduce the effectiveness of air and missile attacks. Passive air defence includes other measures to minimize the effectiveness of such attacks through individual and collective protection of friendly forces and critical assets. Air defence may include counter-rockets artillery and mortar (C-RAM).

(4) **Area Damage Control**. The J-3 coordinates damage control within the 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. Incidence response and recovery is discussed in Chapter 3 of this publication.

(5) **Information Operations**.[13] Info Ops staff elements are responsible for analysis, planning, assessment, and integration of information activities in order to create desired effects in support of

[10] For more information concerning medical support to CBRN Defence see AJP-4.10, *Allied Joint Doctrine for Medical Support* or AJMedP-7, *Allied Joint Medical Doctrine for Support to Chemical, Biological, Radiological and Nuclear (CBRN) Defensive Operations.*
[11] For more on CBRN Defence, see AJP-3.8, *Allied Joint Doctrine for Chemical, Biological, Radiological, and Nuclear Defence*.
[12] See AJP-3.3 *Allied Joint Doctrine for Air and Space Operations* and AC/336-D (2011)0033 final *NATO Air and Missile Defence Policy (AMD)* for further guidance.
[13] See AJP-3.10, *Allied Joint Doctrine for Information Operations*, for further guidance.

FP. Info Ops is leading the overall military counter-propaganda effort.

(6) **Electronic Warfare**. The signals intelligence and electronic warfare (EW) operation centre (SEWOC) and EW coordination cell (EWCC) are responsible for planning and synchronizing EW in support of the FP plan.

(7) **Explosive Ordnance Disposal**. The clearance of unexploded explosive ordnance (UXO) including improvised explosive devices (IEDs), by explosive ordnance disposal (EOD) forces, requires a broad spectrum of EOD procedures and related equipment including electronic countermeasures which will depend upon the type of device, proximity to NATO Forces or infrastructure and the speed required to restore operational capability of fixed installations. The capabilities provided by EOD forces should be coordinated at the strategic level by the specialist EOD staff in the MILENG Operations Branch in SHAPE and, at the operational level, by the J-3 or the special EOD Staff in the Combined Joint Explosive Ordnance Disposal Cell (CJEODC) within the Engineer Operations Branch.[14]

c. **Military Engineering**. MILENG is the engineer activity undertaken to shape the physical OE. The joint force engineer at the joint force HQ will identify the requirements for MILENG support to FP in accordance with engineer tasks. The MILENG staff will also support the execution of recovery operations under the direction of the J-3. Military engineering support to FP tasks should include hardening of facilities; repairing airfields and routes; erecting barriers; providing cover and concealment; determining stand-off distances; route, airfield, and port clearances; mobility and countermobility measures; support to C-IED activities; as well as coordinating fire protection and supporting EOD activities.

d. **Provost Marshal**. The provost marshal (PM) is a military police officer (special staff advisor who may also be afforded a command function) who provides advice directly to the commander and staff regarding all issues

[14] The affiliation of EOD to a single service or MILENG varies within NATO nations, therefore command status of all EOD forces participating in an operation, coordinating authorities and tasking authorities will be clearly defined both in operation orders and within national and international directives. CJEODC will be established in the operational joint force HQ as the focal point for all EOD matters. It is responsible for advising the JFC and coordinating EOD matters with troop contributing nations and other organizations. The JFENGR remains the primary advisor on all mobility support issues and the coordinating authority for MILENG and EOD assets across all components (see paragraph 0112 of AJP-3.12, *Allied Joint Doctrine for Military Engineering*, for more details).

related to military and civilian police activities. The PM and staff participate throughout the entire staff planning process to coordinate military police functions (mobility support, security, detention, police and stability policing) at all levels and during all phases of an operation or campaign.[15]

e. **Logistics**. The J-4, in close coordination with the joint logistics support group (JLSG), should coordinate with the J-3 on 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 that require assigned FP assets, in addition to FP required for LOC. One feature of the modern non-linear, non-contiguous operations area is the absence of any relatively safe rear area. If the threat to logistic forces and facilities and LOC is anything other than low, and particularly if adversary main forces threaten support operations, the JFC may appoint a joint security coordinator. The joint security coordinator's staff coordinates the activities of all resources assigned to protect support operations and LOC, including units assigned to FP missions.

f. **Contracting Authority**. An appropriate 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 in accordance with the overall TA. The J-8 is responsible to care for the appropriate budget and financial rules and regulations to conclude such contracts.

g. **Medical**.[16] The medical advisor is responsible for advising the commander about the existing health threats and hazards, their probable impacts and the prevention and response measures required.

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. FP should be integrated and reflected in all plans. The J-5 synchronizes FP planning efforts within the staff with all other relevant functional specialties, and coordinates with higher,

[15] For more on the PM and military police functions, see AJP-3.2.3.3, *Allied Joint Doctrine for Military Police*.
[16] For more information see AJP-4.10, *Allied Joint Doctrine for Medical Support*, and AJMedP-4, *Allied Joint Medical Force Health Protection Doctrine*.

subordinate, and adjacent commands, as well as civil authorities. For more on planning, see Chapter 4.

i. **Civil-Military Cooperation**. The civil-military cooperation (CIMIC) staff is responsible for establishing and maintaining cooperation with the civilian population and institutions such as national and local governments, IOs, and NGOs. Civil actors 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. Therefore, a balance must be struck between accessibility to military facilities for civil actors, FP, and operations security (OPSEC). 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 is responsible for advising on all safety matters and providing safety input to the J-3 Force Protection Assessment and the risk management process.

k. **Public Affairs**. Dissemination of information relating to FP measures is necessary in order to reinforce their application. The public affairs (PA) officer 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.

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

m. **Other Special Staff**. Other members of the special staff including the finance officer, political advisor, cultural advisor, and gender advisor should be involved in FP planning. They can provide counsel on specific FP implications in their respective areas of expertise.

0206. **Communication and Information Systems**. Effective C2 is directly dependent upon available communications and information, and the availability of reliable supporting CIS. In addition to physical attacks against CIS and facilities, CIS are susceptible to espionage, electronic warfare, and cyber attacks. Commanders should, therefore, develop and implement robust defence and protection

measures to safeguard their CIS and ensure the confidentiality, integrity, and accessibility of stored data.

0207. **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 appropriate liaison with local military and civil authorities, particularly where FP is a shared task between the commands and the HN, as facilitated in the appropriate agreements.

0208. **Force Protection Information Management**. The purpose of FP information management is to provide commanders and staffs at all levels with timely and accurate information about the FP situation so that appropriate mitigating measures, tasks, and activities can be implemented. FP information management should make full use of existing information management procedures and processes, such as CBRN warning and reporting (W&R), and procedures for sharing of W&R with other organizations and HN authorities should be established and disseminated. Additionally, it is essential that the FP staff officer, cell, or element is in the loop for all information management issues to include the warning of impending actions and reporting of incidents.

0209. **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 SC directs appropriate 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 conflicting alert states exists, commands should strive to adhere to NATO-directed alert states and coordinate the measures with adjacent commands where necessary.[17]

[17] See AC/237-D (2012)0001, *NATO Crisis Response System Manual* (NCRSM) and AJP-2.2 for further information on alert states.

INTENTIONALLY BLANK

CHAPTER 3

FORCE PROTECTION PROCESS

0301. **Introduction**. The NATO FP process utilizes a FP model (illustrated in figure 3.1 and discussed in paragraph 0303) which is a schematic representation of the functions, assets, controls, measures, and mechanisms, by which commanders and staffs may plan FP and respond to incidents, hazards, or attacks. It is not intended to replace the OPP, but rather to provide FP planners with a methodology to plan and implement FP measures, tasks, and activities at the operational level. It consists of sequential and iterative sub-functions built around a threat and hazard, vulnerability, and risk assessment process. Other elements of the model include the assets being protected, the measures, tasks, and activities used to safeguard those assets, and procedures to continuously supervise and review the FP capability and posture.

0302. **Threat Environments**.[18] Threats, hazards, and risks to the Alliance and its forces form part of the day-to-day 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. NATO-led forces, including supporting forces, need to constantly revalidate all aspects of their FP. In the absence of a common threat to all regions, local threat assessments may help focus FP efforts. Threats may range from 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. Operational forces should be able to defend against conventional attacks and to protect themselves from natural disasters. When CBRN incidents or toxic hazards occur, they should be able to take appropriate countermeasures. The asymmetric nature of terrorist tactics should be considered by commanders and staffs when planning and implementing FP measures, tasks, and activities. NATO-led forces face an increased vulnerability to other asymmetric threats as well, including those conducted in cyber. The potential threat may be described in terms of five generic environments.

a. **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.

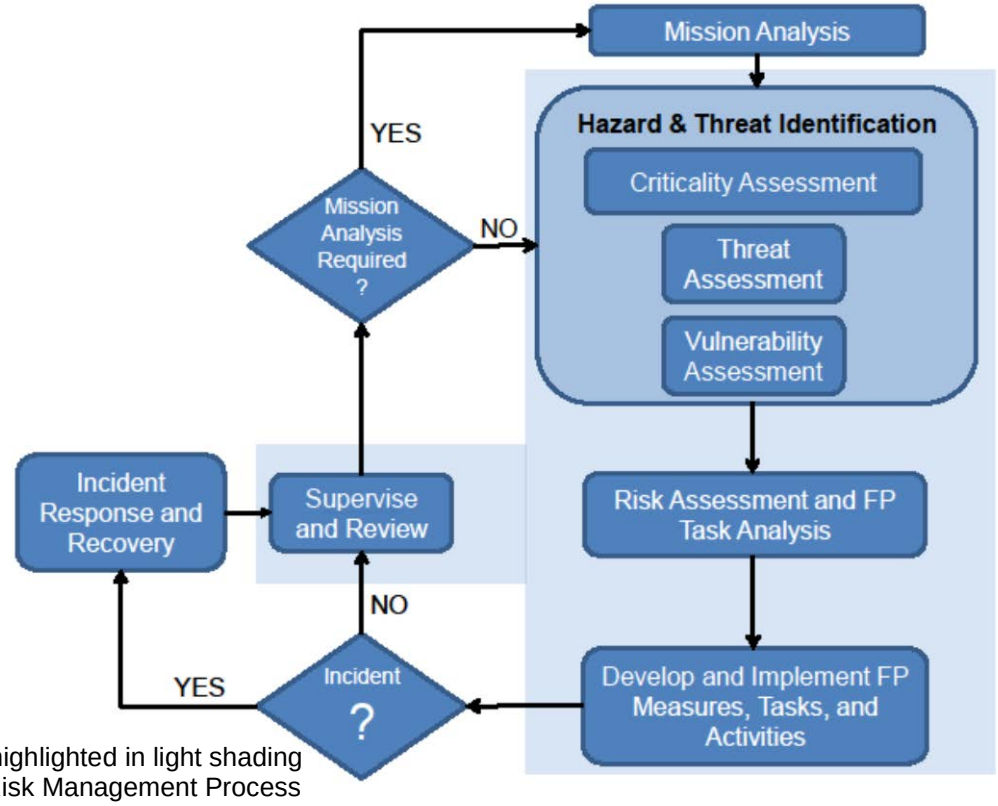
[18] For more on threat levels, see AD 65-11, *ACO Standing Policy and Procedures for Intelligence Production Management*, 12 July 2010.

b. **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. A State or non-State actor has been identified who may possess either the capability or intention of targeting NATO forces or individuals. Although possible, there are no specific indications of use of CBRN. TIM release is possible; however, industrial infrastructure and security levels are robust. The possible use of IEDs and other explosive devices should be taken into account.

c. **Medium Threat Environment**. The medium threat environment assumes the adoption of the low threat FP measures, tasks, and activities and recognizes that there are indications of attack planning 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 areas could be attacked using conventional weapons against vital facilities. The threat faced over the entire NATO area of interest may range from unconventional warfare to limited conventional attacks. A State or non-State actor has been identified as possessing both conventional and CBRN capabilities with possible intentions of targeting NATO forces or individuals. There is an increasing risk of TIM release due to a decay of industrial infrastructure or a degradation of the security of industrial infrastructure. Enemy use of IEDs may be a major concern.

d. **High Threat Environment**. The high threat environment assumes the adoption of the medium threat FP measures and recognizes that an attack is likely based on intelligence that an organization, nation, or group has been identified as possessing both the capability and intention to target members of the international community, including NATO, and will likely attempt to do so in the near term. Adversary propaganda likely targets audiences in the HN and may be increasing in its intensity. Specific timings and targets have not been identified. A State or non-State actor has been identified as possessing both conventional and CBRN capabilities with probable intentions of targeting NATO forces or individuals to include CBRN, and will likely attempt to do so in the near term. Release of TIM may occur with little additional warning due to weakness of industrial infrastructure or insufficient security of industrial infrastructure. Although enemy employment of nuclear weapons could be low, the risks posed by environmental hazards and CBRN contamination exist. Enemy use of IEDs is a major concern.

e. **Critical Threat Environment**. The critical threat environment assumes the adoption of the high threat environment FP measures and recognizes that a specific threat exists or that an incident has occurred. Adversaries will not only attempt to communicate to target audiences in the HN, 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. A State or non-State actor has been identified as possessing both conventional and CBRN capabilities with clear intentions of targeting NATO forces or individuals within a specific time frame or against a specific target. There is an immediate risk of CBRN or TIM release, without warning, due to damage to industrial infrastructure or a lack of security of industrial infrastructure. Enemy use of IEDs remains a major concern.



Note: Area highlighted in light shading depicts the Risk Management Process

Figure 3.1 - Force Protection Model

0303. **NATO Force Protection Model**. As introduced in paragraph 0301, the FP model provides FP planners and commanders with a logical process aimed at identifying and implementing measures, tasks, and activities; effectively

responding to incidents should they occur; and a review process to successfully manage FP at the lowest practical level. Imbedded within this model are several existing decision-making processes to include mission analysis and risk management.[19] Specific steps in the model are below.

a. Identify the specified and implied tasks, and mission essential actions, through **mission analysis**.[20] This is initially done in conjunction with the OPP mission analysis; however, FP planners will later focus on the FP tasks in support of the overall mission.

b. **Hazard and Threat Identification**[21]

(1) Identify those assets and capabilities that are critical to mission success (**criticality assessment**).

(2) Determine likely threats and hazards to personnel and those assets that are critical to mission success (**threat assessment**).

(3) Identify vulnerabilities that could be exploited by threats and the impact of incidents on the force's effectiveness and Allied political will, thereby affecting mission success (**vulnerability assessment**).

c. Identify the specific FP tasks that were developed during the mission analysis, determine sub-tasks, and identify and evaluate associated risks (**risk assessment and FP task analysis**).

d. Develop and implement appropriate FP measures, tasks, and activities to reduce risk to a level acceptable to the commander and calculate the residual risk or gaps. Then monitor their effectiveness in order to manage the mission (**develop and implement FP measures, tasks, and activities**). Willingness to accept risk is likely to be influenced by diplomatic and political constraints.

e. Identify and implement incident response and recovery actions, including the development and implementation of an emergency response and recovery plan (**incident response and recovery**). Coordinate with local and HN authorities to ensure response plans are harmonized.

---

[19] For more on the risk management process, see Annex B.
[20] For more on mission analysis, see AJP-5, *Operations-level Planning*, or Allied Command Operations *Comprehensive Operations Planning Directive (COPD)*
[21] IAW AJP-2.1, *Intelligence Procedures*, the joint intelligence preparation of the batttlespace (JIPB) contributes to hazard and threat identification. The FP staff should participate in the JIPB process.

f. Maintain, reassess, and amend FP measures, tasks, and activities throughout the mission (**supervise and review**).

0304. **Mission Analysis**. Mission analysis is a logical process for extracting and deducing, from the OPORD and commander's guidance, the specified and implied tasks, and mission essential actions necessary to fulfil a mission. It is a dynamic process that continues as the situation and the mission are reviewed. Any of the tasks and actions identified through mission analysis that fall within the FP fundamental elements should be covered in detail in the FP annex to the operation plan or order. Additionally, the FP C2 element will need to coordinate and assign these as mission tasks to the appropriate FP assets. The mission analysis includes the determination of the higher command authority's intent; the analysis of Allied security and military direction, including short and long-term objectives to attain the end state; and pre-conditions for success.

0305. **Hazard and Threat Identification**

a. **Criticality Assessment**.[22] 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, the course of action (COA) selected in the OPP, and physical inspection. 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 results of the criticality assessment permit risk analysis to be conducted by considering the likelihood and impact of a threat exploiting a vulnerability of an asset that is critical to mission success.

b. **Threat Assessment**

(1) MC 161 is the basic intelligence guidance that provides the general TA framework.[23] Such assessments, complemented by current

[22] For more on criticality, threat, and vulnerability assessments, see Allied Command Operations Force Protection Directive 80-25, 14 May 2009.

[23] MC 161, *NATO Strategic Intelligence Estimate*, provides NATO-agreed intelligence on threats/risks faced by the Alliance. MC 161, together with MC 400/3, *MC Guidance for the military Implementation of NATO's Strategic Concept*, and MC 0590-2010, *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 CBRN hazards and incidents.

intelligence (to include CI and indications and warnings) and law enforcement assessments, allow commanders at all levels to assess any hostile intent within their respective operational areas and therefore focus the direction of a FP programme. NATO HQ, the Strategic Commands, and subordinate commands analyse and disseminate threat information and make local TAs available to all commands within their operational areas and areas of interest.

(2) 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 CIMIC staff, as one of the intelligence products provided in accordance with the OPP. Additional localized TAs will need to be conducted, particularly in CRO, that consider TESSOC, insider threats, cyber intrusion, environmental hazards, the ethnic or political affiliations of the population, and other cultural and historic concerns that may impact friendly operations.

(3) The TA identifies known threats along with their capabilities, most likely and most dangerous courses of action, and their overall intentions. The threat analysis includes assessments of:

(a) **Threat Capability**. The ability of potential threats to cause harm to NATO assets. Analysis of threat capability considers threat structure, leadership, professionalism, tactics, weaponry, targeting, and logistics.

(b) **Threat Intent**. The willingness of potential threats to target Allied assets. Analysis of intent considers threat ideology, objectives, strategy, likely intentions, and previous history.

(c) **Threat Likelihood of Exploiting a Vulnerability**. Analysis of likelihood includes threat history under similar circumstances, the adversary's overall campaign plan, currently implemented measures, tasks, and activities, the phase of the operation, and most probable threat COAs.

(4) The TA should address the full range of threats and attack possibilities and identify likely weapons and delivery tactics. The TA should also address environmental and occupational hazards that may have an impact on the mission.

(5) The ICP, which is based on the commander's critical information requirements[24] and priority intelligence requirements, 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 should consider the fusion of information and intelligence acquired from military, security, political, social, CI, and criminal intelligence sources and agencies.

c. **Vulnerability Assessment**

(1) 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 from threats or degradation due to hazards identified in the TA. Each VA is accomplished by multi-disciplinary subject matter experts who conduct operational analyses and assess the vulnerability of personnel, materiel, information, facilities, and other assets.

(2) 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.

0306. **Risk Assessment and Force Protection Task Analysis**. Armed with the results of the mission analysis and hazard and threat identification (criticality, threat, and vulnerability assessments), a FP task analysis and initial risk assessment will then be conducted. Specified FP tasks are those specifically identified as a result of the mission analysis. Other FP tasks will be derived from a detailed analysis of the hazards and threats from the previous step. The risk assessment will be completed to determine the potential adverse effects from

[24] For more information on commander's critical information requirements see AJP-2 and AJP-3.

those hazards and threats, the probability of occurrence, and the degree of exposure. Risks are then prioritized and FP measures, tasks, and activities identified. Pending the type of operation, any residual risk is accepted by the commander in close coordination with partner nations.

0307. **Develop and Implement Force Protection Measures, Tasks, and Activities**.

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

b. During this step, FP measures, tasks, and activities are developed and analysed as 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, tasks, and activities are implemented and can be integrated into SOPs, written and verbal orders, mission briefings, and staff estimates. This is usually achieved by converting FP controls into clear and simple execution orders, establishing proper authorities and accountabilities, and providing the necessary support to implement, whilst remaining fully aware of any residual risk.

c. FP measures, tasks, and activities generally fall into the categories described below. For more specifics on measures, tasks, and activities as they apply to the fundamental elements, see Annex A.

(1) **Procedural**. These involve operational or administrative procedures:

(a) Operational measures such as SOPs, boundaries, reporting, and ROE.

(b) Administrative measures such as written policies and instructions.

(c) Business processes.

(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.[25]

(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.

(3) **Materiel**

(a) Physical security measures, tasks, and activities to prevent unauthorized access such as security badges. Biometric[26] 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.

[25] Depending on the threat, specially trained bodyguards and protection personnel or teams may be provided for the protection of designated and targeted personnel.
[26] The collection, use (to include fusion with other intelligence), storage and dissemination of biometric data are controversial in many nations, and national legislation might limit individual TCNs from taking part in, or contribute to, this process. Information about national reservations is of importance in the planning of FP in operations.

(c) Engineering and technical measures to reduce risks such as select better or more appropriate materials, identify suitable substitute materials or equipment, and adapt new technologies to existing systems.

(d) Physical security measures to prevent unauthorised access to weapons or ammunition.

(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 stand-off distances. This includes the defence, protection, and safe management of own ammunition storage areas. Additionally, individual hardened sleeping cubicles will further protect sleeping personnel during indirect fire, missile, or air attacks.

(c) Collective physical protective measures such as theatre ballistic missile defence and surface based air defence provide protection against air threats, including aircraft, helicopters, remotely controlled systems, and missiles. Furthermore, air defence assets able to perform C-RAM defensive roles can enhance the required security to infrastructures, facilities, and personnel.

(5) **Information**

(a) The security of information is safeguarded by complementary procedural, personnel, physical, and information security (INFOSEC) measures. CIS security, INFOSEC, and cyber defence, include security measures to protect information processed, stored or transmitted in communication; to protect information and other electronic 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 electronic protective measures (a part of EW) and OPSEC.

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

0308. **Incident Response and Recovery**[27]

a. **Incident Response**. Incident response includes measures to neutralize, isolate, contain, and resolve a specific threat or act. 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 necessary measures in order to regain operational capability as soon as possible. Effective incident response may require the coordination of the activities of a number of disciplines including, but not limited to, security, safety, firefighting, search and rescue, PA, EOD, and CBRN. Response actions should follow process and procedures outlined in response plans. Incident response includes:

(1) Immediate action by first responders, such as quick reaction forces, security forces, fire departments, medical personnel, or hazardous material teams.

(2) Establishing an emergency operations centre.

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

(4) Implementing operational continuity and alert plans.

[27] For more on response and recovery operations, see *Allied Command Operations Force Protection Directive* 80-25, 14 May 2009.

(5) Implementing additional protective measures.

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

(7) Releasing internal and external information updates.

(8) 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.

(9) Implementing medical measures commensurate with the major incident medical management and support approach. This includes medical and casualty evacuation procedures.

b. **Recovery**. Recovery operations involve the coordination and implementation of measures intended to mitigate the damage, loss, hardship, and suffering caused by a natural, accidental, or deliberate threat event. Recovery operations include measures, tasks, and activities 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, decontamination, 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.

0309. **Supervise and Review**. Regardless of whether an incident has occurred, supervision and review is required to validate the effectiveness of the overall FP plan, 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, tasks, and activities in supporting the objectives and desired outcomes. While this is presented as the final step in the FP model, supervision 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.

CHAPTER 4

FORCE PROTECTION PLANNING CONSIDERATIONS

0401. **Planning Overview**. FP planning establishes requirements and identifies necessary measures and means to minimize assessed vulnerabilities to threats and hazards, 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 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 operation, the strategic level will provide FP guidance and direction 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, tasks, and activities to be taken under the various threat categories. Forces are normally particularly vulnerable to attack during deployment; reception, staging and onward movement; and redeployment.

a. FP planning is a cyclical process that assesses the mission criticality of all assets; assesses threats, hazards, vulnerabilities, and risks; and prescribes appropriate measures, tasks, and activities to reduce or mitigate identified vulnerabilities and risks.

b. As appropriate, FP specific orders, plans, directives, instructions, procedures, and other forms of direction must be developed as outputs of the OPP. For NATO OPLANs, FP is addressed in the coordinating instructions of the basic plan and Annex J, Force Protection.[28]

0402. **Plans and Procedures**. NATO-led forces should have specific and appropriate plans and procedures to manage the preparation and generation of FP measures, tasks, and activities, to include any anticipated enhancements to peacetime FP measures, tasks, and activities to meet escalating threats. These plans should establish the FP organization, C2 and CIS, appropriate operational areas and resources, and should allow for conducting sustained operations in all five possible threat environments (negligible, low, medium, high, and critical) with special regard to CBRN implications. These plans should also include, where necessary, the relevant FP aspects of the HN's plans. Additionally, during the conduct of certain operations, such as non-combatant evacuation operations, NATO-led forces will be required to provide FP for civilians, family members, and others.

[28] See Allied Command Operations *Comprehensive Operations Planning Directive* (COPD).

0403 **Developing Force Protection Procedures**. FP procedures specify when, where and under what circumstances FP measures, tasks, and activities 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 CBRN hazard management measures, or protective security, should be considered when developing FP plans. In developing FP procedures, commanders should be cognizant that some measures, tasks, and activities may affect the civilian population. These will be subject to appropriate and timely legal review and will need to incorporate the requirements of appropriate international and HN law, and any SOFAs.

0404. **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 Directive 80-25. Additionally, guidance for air operation FP planning is provided in ATP-3.3.6, *NATO Force Protection Doctrine for Air Operations*[29]. Details on FP planning for maritime forces and infrastructure in ports and anchorages can be found in ATP-74, *Allied Maritime Force Protection Against Asymmetric Threats in Harbour and Anchorage*.

0405. **Host Nation Force Protection Support Planning**. Depending on circumstances, it may be necessary to develop supporting plans to the main plan in order to address all aspects of operations at the appropriate level of detail. The advance planning process identifies HNS requirements for many FP-related functions. However, NATO and TCN plans should address the potential for FP deficiencies in such support, particularly if the HNS relies heavily upon reserve force mobilization or civilian work forces. Similarly, where HN FP is envisioned, plans should include any necessary separation of responsibilities for specific FP functions and the C2, transfer of command authority requirements, and national capabilities and restrictions for protecting property and civilians. 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). Unfortunately, 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 / counterintelligence, law enforcement, and security personnel support. NATO-led forces may have differing relationships with each HN for FP within each region. Commanders are responsible for developing plans

[29] ATP-3.3.6 is currently a study draft and not an official NATO document.

to cover local civil and military authority involvement, since local FP will likely be shared between their command and the HN. However, the JFC should be aware that IOs and NGOs may not follow NATO FP guidance.

0406. **Incident Response Planning**. Plans for initial response to an attack by opposing forces must include the possibility that the primary or additional goal is to inflict casualties among first responders. Military and civil responders may present themselves as easy targets to an enemy that knows these personnel will gather in a single location at a known time. A loss of or threat to fire departments, paramedics, or CBRN specialised teams can cripple on-going and future recovery efforts. Planning must incorporate training and procedures to increase FP capability during incident response under hostile conditions.

0407. **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.

0408. **Force Manning Planning**. Manning plans for NATO C2 entities have to consider maintaining the safety and protection of their organizations/HQ and the potential need to increase manpower to achieve the organizational strength necessary to meet increasing threats and hazards. All identified manpower should be trained to the appropriate operational performance standards within the required readiness state. Local FP commanders may not have all needed assets to conduct all FP missions as discussed above. Discussions with other unit commanders within the FP commander's area of responsibility are required upon deployment to mitigate these issues.

0409. **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 Adviser and Public Affairs Officer, should ensure the chain of command is informed in advance of any FP change.

0410. **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 any error in the risk management process which is inherent in FP. 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.

0411. **Civil-Military Cooperation and Force Protection**. 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, warnings on current threats, etc.[30]

0412. **International and Non-Governmental Organizations**. NATO-led forces conduct operations as a contribution to a wider comprehensive approach[31] that requires coordination and cooperation with national governmental organizations, IOs, NGOs, and private actors. In such complex multi-organization 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, as appropriate, to offering FP 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 organisations operating in the area of operations, through the Provost Marshal Office, are required.

[30] For more on CIMIC, see AJP-3.19, *Civil Military Cooperation*.
[31] For more on a comprehensive approach, see AJP-01, *Allied Joint Doctrine,* or AJP-3, *Allied Joint Doctrine for the Conduct of Operations*.

0413. **NATO International Civilians, Civilian Contractors, and Staffs**

a. The NATO policy on contractor support to operations states that a distinction must be made in reference to several types of civilians and the related responsibility of the military/NATO for their security in the JOA.[32]

(1) NATO civilians (consult legal status in respect to the Geneva Conventions when applicable).

(2) Personal service contractors (military/NATO act as the employer of the individual).

(3) Personnel employed by a company which in turn works under a military/NATO commercial service contract (the military/NATO is not the employer of the individual).

(4) Local employees (under a different legal status because they fall under the jurisdiction of local authorities).

(5) Other civilians who are present in the JOA on invitation or with permission of the NATO commander.

b. Civilian 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.

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 deployed in direct support of NATO operations.

(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 civilians and civilian contractors employed directly by NATO/ Nations resides with the NATO/national commander, the responsibility for civilian

[32] C-M(2007)0004, *NATO Policy for Contractors Support to Operations*.

contractors employed by a company operating under a NATO or national contract needs to be clarified in the contract.

0414. **Fratricide and Mutual Interference Prevention**.

a. 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 process of combining SA, target identification, and specific TTPs with effective battlespace management. Additionally, with increasing competition for use of the electromagnetic spectrum, the need to minimise mutual interference through the effective management of the operational environment and electromagnetic spectrum becomes an essential part of both maintaining combat effectiveness and minimising fratricide. 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. Moreover, the 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.

b. Prevention of mutual interference involves measures to minimize the interference between friendly forces and units, up to and including fratricide. Interference can be physical (collision, weapon hit) or occur in the electromagnetic and acoustic spectres. Mutual interference can be prevented by separating activities either in space, in time or in (electromagnetic or acoustic) frequency.

(1) **Airspace Control**.[33] The implementation and coordination of the procedures governing airspace planning and organization to minimise 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.[34].

[33] 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 (AAP-6)

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

(2) **Waterspace Management**. A system of procedures for the control of antisubmarine weapons to prevent inadvertent engagement of friendly submarines.[35]

(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.[36]

(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.

0415. **Use of Non-Lethal Capabilities in Force Protection**. Non-lethal and lethal use of force 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, the principles of distinction, military necessity, proportionality and humanity. Non-lethal capabilities 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 and aid in the discrimination of hostile from non-hostile individuals. Proper training in the use of non-lethal capabilities is a primary consideration prior to their employment.

0416. **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 enemy activity. Furthermore, proactive operations and a clear presence of weapon systems will have a deterrent effect on a possible enemy. Use of weapons systems that can operate from NATO bases in the operational area provides a flexible capability without deploying to forward locations, thus reducing the forward footprint, which in turn decreases the demands on FP means.

[35] See ATP-18, *Allied Manual of Submarine Operations*.
[36] See ATP-1 Volume 1, A*llied Maritime Tactical Instructions and Procedures*.

0417. **Use of Stability Policing Assets in Force Protection**. Stability policing is a set of police-related activities which contributes to the restoration or upholding of public order and security, rule of law, and the protection of human rights to enable the development of a sustainable peace, through supporting and temporary substitution (if necessary) of the indigenous police. 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 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.

0418. **Insider Threat Considerations**. Non-traditional threats, such as the insider threat, can undermine JFC FP plans as well as the cohesion of the 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 between the HN and NATO-led forces can affect military capability. Minimizing 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 organizations the Alliance is trying to protect. Adversaries may view attacks against NATO forces as a particularly effective tactic, especially when using co-opted coalition or host nation forces to conduct these attacks. While these types of insider or "green on blue" attacks have been context-specific to a particular theatre, JFCs should nevertheless ensure that their FP plans take into account the potential for these types of attacks and plan appropriate CMs as the situation dictates.[37]

0419. **Use of Remotely Controlled Systems in Force Protection**. Remotely controlled systems such as aircraft and maritime surface or subsurface vehicles can be used in a 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.

[37] To counter the insider threats, NATO-led forces increase intelligence and counterintelligence efforts aimed at stopping attacks before they occur, improve the vetting process for HN security forces, analyse attacks that do occur, and implement the Guardian Angel programme. The programme requires that a NATO service member, dubbed a "guardian angel," observe any gathering of NATO and HN troops to identify anyone who could potentially be involved in attacks on NATO-led forces.

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.

0420. **Force Protection Training**

a. **General**. NATO training, exercise, and evaluation policy is prescribed in MC 0458/2, *NATO Education, Training, Exercise, and Evaluation Policy*. The focus of NATO training, including exercises and evaluations, as well as national training programmes, 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 necessary 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 that includes likely response measures, basic health and safety skills, such as first-aid, sanitation, fire and light rescue, and, when appropriate, assigned weapon proficiency. The scope, type, methodology, length, frequency, and execution of FP training are conducted in accordance with the relevant NATO Standardisation Agreement or command authority. In the absence of such direction, it should be conducted at the discretion of the appropriate NATO commander.

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. 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**.[38] In the context of expeditionary operations, advance preparations through pre-deployment training (PDT) are vital to

[38] Pre-deployment training has more recently included issues related to insider threats and the associated Guardian Angel programme. The Guardian Angel programme was started in March 2012 after a spike in "green on blue" attacks on NATO forces. The programme will require J1 and J4 coordination and

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.[39] Deploying forces are highly encouraged to undergo cultural awareness training as part of the deployment training process. Insider threat is a major FP concern for future Allied operations; therefore, pre-deployment FP training should include insider threat advanced training.

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 OE or refresher training as well as collective training. Commanders should plan for and provide the needed resources for such training, especially for extended deployments.

planning (significant increase in personnel with associated training, equipping, and support planning considerations).

[39] As a minimum, this should include individual common core skills.

ANNEX A

Force Protection Fundamental Elements

A001. **General**. NATO 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 civil environment. In a low-threat level environment, security and health protection may be the only FP fundamental elements required. As threat levels increase in level, additional measures may be required such as air defence, EOD, and CBRN defence. However, hybrid threats may exist at any level of intensity, and therefore, require the application of protection measures, tasks, and activities across the entire spectrum. The key to FP planning includes not only recognising the appropriate threat level but also having a comprehensive understanding of the OE. Below is a discussion of the measures, tasks, and activities 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, tasks, and activities in only one particular area. The intent of this annex is to describe the fundamental elements all together, provide the types of measures, tasks, and activities involved, and explain how they can contribute to the overall FP plan.

A002. **Tactical Area of Responsibility Control**

a. **Introduction**. The threat of an attack against a deployed location necessitates the establishment of an area of operations around and inside a base, facility or deployable camp known as the tactical area of responsibility (TAOR).[40] 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.

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.

[40] A ground defence area (GDA) may be included within a TAOR. For more on GDA see ATP-3.3.6.

(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.[41]

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

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

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

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

(9) 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.

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

[41] For more on C-IED, see AJP-3.15, *Allied Joint Doctrine for Countering-Improvised Explosive Devices*.-

(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, naval mines, and underwater IEDs. Conducted in coordination with port security measures, tasks, and activities.

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

A003. **Air Defence**.[42] 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 HN air defence systems, and the exchange of information necessary to support civil defence activities. Air defence measures, tasks, and activities are both active and passive. Active air defence involves any direct defensive action taken to destroy, nullify, or reduce the effectiveness of enemy air and missile attack against friendly forces and critical elements. Passive air defence includes all other measures taken to minimize 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.

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

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

c. **Maritime Air Defence**. Anti-air warfare (AAW) is the defence of maritime forces against attack from the air, including surface-to-surface and air-to-surface missiles, cruise missiles, rockets and bombs. Maritime AAW is part of the joint defensive counter air and can provide air defence for friendly forces ashore.

d. **Airborne Air Defence**. Defence from the air against air attacks.

e. **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.

[42] For more on air defence, see AJP-3.3, *Allied Joint Doctrine for Air and Space Operations*.

f. **All Arms Air Defence**. The low-level air defence of a unit using small arms (i.e. individual and unit-level weapons of a calibre less than 20 mm); fire control is essential to prevent fratricide and fall of shot must be considered.

A004. **Chemical Biological, Radiological, and Nuclear Defence**.[43] The aim of 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 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 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 include detecting and characterizing CBRN incidents, identifying the agents and hazards, delineating areas of contamination, and monitoring the changes.

b. **CBRN Information Management**. CBRN information management concerns the management of all forms of CBRN defence related information. It enables the rapid collection, evaluation, and dissemination of information concerning CBRN incidents; detection; assessment of threats and risks; prediction of hazard areas, W&R; and management of hazards. In-theatre, CBRN W&R systems for incidents and the resulting hazards prediction must be in place in accordance with STANAG 2103 so that the risk to NATO-led forces is minimised. This system needs to provide accurate and timely information about the CBRN situation to allow commanders and staffs at all levels to take appropriate mitigating CMs. CBRN reporting links should, in principle, be established vertically and horizontally to ensure effective warning to adjacent units. Procedures for sharing of W&R with other organizations and HN authorities should be established and disseminated.[44]

c. **Physical Protection**. Individual and collective protection enable personnel to survive CBRN incidents and to continue to operate in a

[43] For more on CBRN defence, see AJP-3.8, *Allied Joint Doctrine for CBRN Defence*
[44] For more on CBRN W&R, see ATP-45, *Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological, and Nuclear Incidents (Operators Manual)*.

CBRN environment. Measures, tasks, and activities to protect facilities, aircraft, ships, vehicles, and equipment, such as through original design or hardening, are included.

d. **Hazard Management**. Hazard management measures, tasks, and activities limit the operational impact of CBRN incidents and are based on the principles of pre-hazard precautions and hazard control through avoidance, control of spread, exposure control, and decontamination. TIHs 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.

e. **Medical Countermeasures**. Medical CMs are designed to diminish the susceptibility of personnel to the lethal and damaging effects of CBRN hazards and to treat and evacuate casualties arising from exposure to such hazards. The treatment and evacuation of casualties in a CBRN environment, whether contaminated or not, must be considered. The medical staff advises the commander on medical countermeasures and support.

A005. **Resilience**. Measures, tasks, and activities to increase friendly forces' ability to continue to operate despite adversary action or other hazards.

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

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

c. **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.

d. **Physical Protection**. Achievement of protection against weapon or hazard effects by physical means.

e. All military personnel irrespective of rank should be capable of contributing to the FP of the force. Their knowledge should include base sectorisation and sector C2, own asset/workplace protection and contribution to FP of

the base (including the role of commanders), sector/workplace control of entry, guards and sentries (including guard commanders), responses to alarms, warnings and information, post-attack-reconnaissance, UXO detection and marking, CBRN recce and marking, cordons, reporting, FP C2, incident C2, combined incident teams, and the rules / process for the inclusion of contractors and locally employed civilians.

A006. **Military Engineering Support to Force Protection**. MILENG support to FP is one of the eight defined FP fundamental elements; however military engineers also provide support in many other joint functional areas as part of engineering tasks.[45] 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 disposal, restoration of essential services and facilities, and fire safety. MILENG support to FP is divided into eight sub categories.

a. **Protective Infrastructure**. This includes all the infrastructure related measures, tasks, and activities that contribute to FP as well as planning, design, construction, and maintenance of all infrastructure and facilities to include appropriate blast and ballistic protection. It also includes consideration of appropriate safety distances within a camp layout (e.g. obstacles, fences) and hardening of individual sleeping areas.

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 program within a camp, which may also include training, as well as fire response capabilities in coordination with other logistics capabilities and FP fundamental elements.[46]

c. **Support to Explosive Ordnance Disposal.** Specially trained military engineers can be employed to assist EOD elements with the disposal of large quantities of munitions in order to reduce the significant threat to friendly forces and the local civilian population. The affiliation of EOD to MILENG varies within NATO nations; therefore the command status of all EOD forces participating in an operation will be clearly defined both in operations orders and within national and international directives. Military engineers are also responsible for the provision of awareness training to all force personnel on mines and other explosive hazards in support of EOD forces. The policy for the conduct and content of any such training will be a

[45] For more on Military Engineering, see AJP-3.12, *Allied Joint Doctrine for Military Engineering*.
[46] Firefighting is primarily a consequence management function. See paragraph A007 d. below.

a JFC issue. Overall, EOD contributes to the FP fundamental element of consequence management. See A007 b below.

d. **Support to C-IED activities**. Military engineers, due to their training in military search, or in specialist roles such as EOD and geospatial engineering, can support C-IED operations to defeat the device.

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

f. **Military Search**. Military search is an essential element of FP – both protecting coalition bases and enabling freedom of action and movement. Military search provides assurance of potential "high level" targets during pre-planned events and is employed to safeguard disparate friendly or neutral factions in the area of operation.[47]

g. **Route and Area Clearance**. Route clearance is a mobility task, under the MILENG support to joint function 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. Route and area clearance include the detection and, if found, the identification, marking and neutralization, destruction, or removal of mines, improvised explosive devices, booby traps, or other explosive ordnance threatening a defined route/area to allow a military operation to continue with reduced risk. Neutralization focus is both on UXO and obstacles. Route and area clearance leave residual risk.

A007. **Consequence Management**.[48] Consequence management 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**. EOD and support to C-IED activities are often required to contribute to incident response and recovery activities. EOD involves the detection, identification, on-site evaluation, rendering

[47] ATP-73 Volume I, *Military Search*.
[48] For more on consequence management, see (NSA(JOINT)0478(2009)1/CBRN dated 27 April 2009), AJP-3.8, *Allied Joint Doctrine for Chemical, Biological, Radiological, and Nuclear Defence*, AJP-4.10, *Allied Joint Medical Support Doctrine*, and MC 472, *NATO Military Concept for Defence against Terrorism*.

safe, recovery, and final disposal of UXO. EOD forces dispose of UXO that threaten friendly forces and, with their capabilities, contribute to protection of personnel and assets. This may include explosives which have become hazardous by damage or deterioration. EOD also contributes to resilience since it involves measures taken to prevent and minimise the effects of mines, IED, and UXO.

c. **Restoration of Essential Services and Facilities**.[49] 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 HQ. 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 case they must be linked to FP arrangements. Fire services may include the ability to deal with toxic industrial hazards.

e. **Personnel Recovery**. Personnel recovery (PR) is the sum of military, diplomatic, and civil efforts to affect the recovery and reintegration of isolated personnel. PR encompasses a variety of recovery options and categories/capabilities. Joint PR is controlled at the Joint Force level. It is likely that the forces available will only have a limited PR capability, but they must be able to undertake any PR execution task, within means and capabilities.[50]

A008. **Medical Force Protection and Force Health Protection**. 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 environment, occupational

[49] MILENG also contributes to this consequence management area, specifically damage control and repair and airfield damage repair.
[50] See Bi-SC Joint Operational Guidelines 11/01, *Joint Personnel Recovery*.

health risks, Environmental Industrial Hazards, disease, and selected special weapon systems through preventive measures for personnel, systems, and operational formations. Elements of medical activity contribute directly to FP; therefore, medical and FP staffs should work together in order to minimise preventable casualties and to ensure that, where casualties do occur, appropriate resources are available to manage them. There are two aspects to medical support to FP: medical force protection and force health protection (FHP).

a. **Medical Force Protection**.[51] Medical FP is the responsibility of the medical director's staff. Normally, a medical force protection cell will be established to properly incorporate medical aspects in the overall FP planning process. Medical FP includes:

(1) Medical FP assessment

(2) Pre-Deployment medical readiness preparation and baseline assessment.

(3) Deployment medical readiness support functions.

(4) Post-Deployment medical status monitoring.

(5) Preventive medicine measures and requirements.

(6) Morbidity surveillance and casualty reporting.

(7) Civil labour health support.

(8) Mass casualty and incident response planning.[52]

(9) Support to consequence management activities.

b. **Force Health Protection**.[53] FHP is the sum of all efforts to reduce or eliminate the incidence of disease and non-battle injuries to enhance

[51] For more on medical force protection, see AJP-4.10, *Allied Joint Doctrine for Medical Support*.
[52] A major incident situation occurs when troops, workers, or local civilians, are victims of a natural disaster or hostile act, which causes a complex emergency situation. A mass casualty situation occurs when there is an excessive disparity between the number of casualties resulting from an incident and the locally available medical capability to deal with the casualties. FP planning requires rapid and efficient response to major incident situations. Therefore, under such circumstances, all necessary actions required to cope with casualty peaks within the force have to be taken.
[53] For more on force health protection, see AJMedP-4, *Allied Joint Medical Force Health Protection Doctrine.*

operational health readiness and combat effectiveness. FHP measures, tasks, and activities fall into six main areas:

(1) Health and disease surveillance.

(2) Preventive medicine and disease control.

(3) Occupational, environmental, and industrial health hazards.

(4) CBRN health threats.

(5) Field sanitation, food and water hygiene, and veterinary services in the context of food and water borne diseases.

(6) Health promotion and health readiness.

A009. **Security**. 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 minimise attacks on personnel, information, equipment and installations through the application of physical, procedural and technical measures. Security in NATO encompasses entry control, OPSEC, counterintelligence, information, cyber/computer, physical, personnel, and air transportation security. Such security programmes interact with related programmes 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 an integral part of FP.

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

b. **Counterintelligence**. Activities concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in TESSOC.

c. **Computer Security/Cyber Defence**. 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 the cyber environment.

d. **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 unauthorized 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.

(3) **Information Security**. That part of security concerned with measures designed to safeguard relevant data of every description which may be used in the production of intelligence. It includes measures required to preserve confidentiality, integrity, and availability of information.

(4) **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.

e. **Air Transport Security**. That part of security concerned with measures designed to safeguard air transport operations, to prevent sabotage, damage, and theft. Air transport security describes the measures undertaken to screen passengers and cargo before and during transportation on NATO or NATO-chartered aircraft. Because of the legal and procedural requirements involved, it is a specialist task normally conducted by military police or FP personnel. Air transport security involves prevention of adversary and criminal actions against air transport operations, but also prevention of carriage or loading by friendly and neutral personnel of dangerous and prohibited goods on air transport aircraft.

f. **Port Security**. That part of security concerned with measures designed to safeguard maritime operations, to prevent sabotage, damage and theft. Port security not only involves prevention of adversary and criminal actions against port operations, ships in port, and ships at anchorages, but also screening of passengers and cargo. Port security measures for NATO or NATO-chartered ships will be based on the civilian port security measures that are coordinated through the International Ship and Port Security Code.

g. **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.

h. **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.

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

j. **Road Safety**. 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, ignorance, 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.

ANNEX B

Risk Management

B01. **Risk Management**. Risk management consists of choosing the appropriate response to a risk, by selecting one or a combination of the following possibilities: avoidance, transference, mitigation, or acceptance. It should be based on minimizing risk wherever possible, and not risk elimination. Risk management integrates the risk response evaluation and selection processes by assessing the value of assets, threats, hazards, and vulnerabilities, and weighs the risk of compromise or loss against the cost of implementing controls and measures and the impact on mission success. Following risk assessment, the implementation of appropriate controls and measures will reduce the likelihood or severity of the various risks and hazards involved. Risk management is a process of identifying, evaluating, selecting, and implementing mitigating controls and measures to reduce identifiable risks, commensurate with mission success, accepting residual risk, and then supervising and evaluating. Mitigating controls and measures to reduce identifiable risks may prevent, deter, detect, isolate, delay, deny, defend against, defeat, or destroy an attack or hazard.

B02. The risk management process, shown in figure B.1, consists of five phases: identify hazards, assess hazards to determine risk, develop controls and measures, implement controls and measures, and supervise and evaluate.[54]

[54] For more on this process, see ATP-3.8.1, *Volume* 1, *CBRN Defence on Operations*.

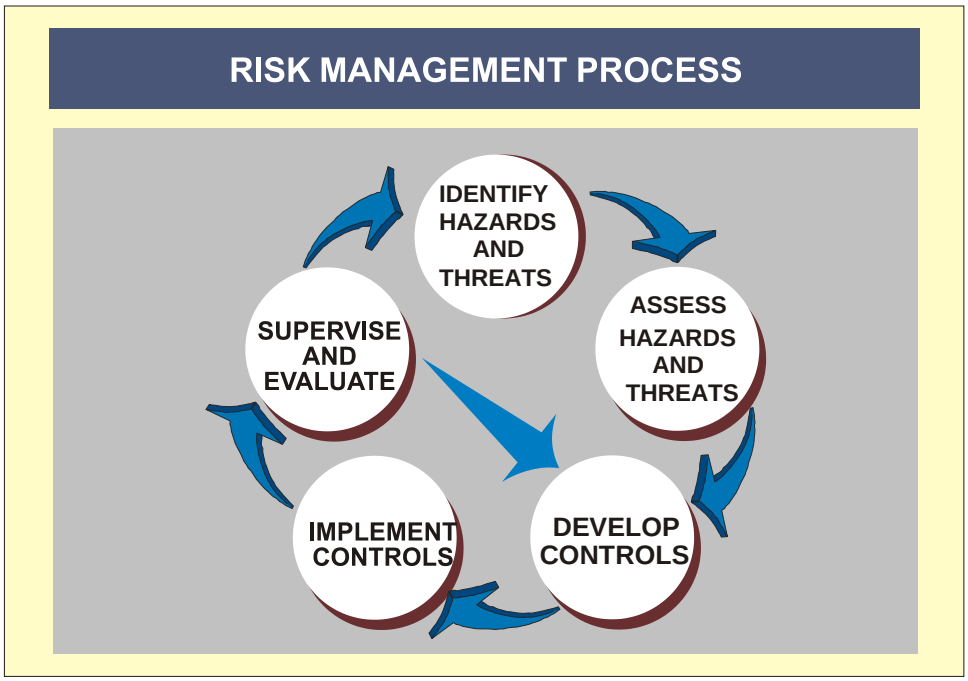


Figure B.1 - Risk Management Process

a. **Identify Hazards and Threats**. This phase attempts to answer the question "What can possibly go wrong?" Hazards and threats may arise from any number of areas and can be associated with enemy activity, accident potential, environmental conditions, health, sanitation, materiel, and equipment among others. This phase includes an analysis of the mission, listing of hazards and threats, and identification of underlying causes. It is the first step in completing a risk assessment.

b. **Assess Hazards (Risk Assessment)**. Risk is a function of the value of the asset and is compared to the potential impact of the exploitation of vulnerabilities by threats and hazards. This phase answers the question "What are the odds (probability) of something going wrong and what is the effect or impact (severity)?" The effect could be mission failure, injury, or loss due to a threat exploiting vulnerabilities or a hazard. It considers the risk or likelihood of an event or incident adversely impacting mission, capabilities, people, equipment, or property, and completes the risk assessment by systematically presenting a methodology to obtain a standardized level of risk. Risks must be identified by checking the cause, the event, and the effect of the risk. The risk assessment considers four points and should include a prioritisation of the risks to support the decision-making process:

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

(2) Probability or likelihood that a specific vulnerability will be exploited.

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

(4) The proximity of the risk.

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

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

e. **Supervise and Evaluate**. Is your plan working? Are changes or updates required? The purpose of phase five of the risk management process is to ensure that risk controls are implemented and enforced to standard and that a feedback mechanism is in place. As with the rest of the risk management process, supervision and evaluation must occur throughout all phases of an operation or activity.

INTENTIONALLY BLANK

LEXICON

PART I – ACRONYMS AND ABBREVIATIONS

AJP	Allied joint publication
AAW	anti-air warfare
C2	command and control
C4I	command, control, communication, coordination, and integration
CBRN	chemical, biological, radiological and nuclear
CI	counterintelligence
C-IED	countering improvised explosive devices
CIMIC	civil-military cooperation
CIS	communication and information systems
CM	countermeasure
CND	computer network defence
COA	course of action
C-RAM	counter-rockets, artillery, and mortars
CRO	crisis response operations
EOD	explosive ordnance disposal
EW	electronic warfare
FHP	force health protection
FP	force protection
GDA	ground defence area
HN	host nation
HNS	host-nation support
HQ	headquarters
ICP	intelligence collection plan
IED	improvised explosive device
Info Ops	information operations
INFOSEC	information security
IO	international organization
JFC	joint force commander
JOA	joint operations area
LOC	lines of communications

MC	Military Committee
MCM	mine countermeasure
MILENG	military engineering
NATO	North Atlantic Treaty Organization
NGO	non-governmental organization
OE	operational environment
OPORD	operations order
OPSEC	operations security
OPLAN	operation plan
OPP	operations planning process
PA	public affairs
PDT	pre-deployment training
PM	provost marshal
PR	personnel recovery
ROE	rules of engagement
SA	situational awareness
SC	strategic commander
SOFA	Status of Forces Agreement
SOP	standing operating procedures
StratCom	strategic communications
TA	threat assessment
TAOR	tactical area of responsibility
TCN	troop-contributing nation
TESSOC	terrorism, espionage, subversion, sabotage, and organized crime
TIH	toxic industrial hazard
TIM	toxic industrial material
TTP	tactics, techniques and procedures
UXO	unexploded explosive ordnance
W&R	warning and reporting

PART II – 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. (AAP-06)

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. (AAP-06)

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

consequence management
Actions taken to maintain or restore essential services and to lessen the effects of natural or man-made disasters. (AAP-06)

countering improvised explosive devices
The collective efforts to defeat an improvised explosive device system by attacking networks, defeating devices, and preparing a force. (NTMS-NATO Agreed)

counterintelligence
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. (AAP-06)

electronic countermeasures
That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum through the use of electromagnetic energy. There are three subdivisions of electronic countermeasures: electronic jamming, electronic deception and electronic neutralization. (AAP-06)

electronic warfare
Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects. (AAP-06)

explosive ordnance disposal
The detection, identification, on-site evaluation, rendering safe, recovery and final disposal of unexploded explosive ordnance. (AAP-06)

force protection
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. [This definition will be submitted as a change to AAP-6 upon promulgation of this AJP.]

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. (AAP-06)

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 which are located on, operating on/from, or in transit through the host nation's territory. (AAP-06)

incident response
Measures taken to neutralize, isolate, contain, or resolve a specific threat or act to minimize its effects on mission success, individuals, units, and facilities. [This definition will be submitted as an addition to AAP-06 upon promulgation of this AJP.]

military engineering
Engineer activity, comprising both force support engineering and combat support engineering, undertaken regardless of component or service, to shape the physical operating environment. (AAP-06)

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. (AAP-06)

organizational strength
The number of trained personnel, facilities, and the amount of materiel required to perform a unit's assigned mission. Note: The organizational strength of a unit may change in response to changing situations and mission requirements. (AAP-06)

physical security
That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. (AAP-06)

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 use within this publication only.)

risk
The probability and severity of a potential loss linked to hazards and threats. (Definition for use within 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 use within 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. (AAP-06)

rules of engagement
Directives issued by competent military authority which specify the circumstances and limitations under which forces will initiate and/or continue combat engagement with other forces encountered. (AAP-06)

security alert states
Normal security arrangements for the protection of sites, units and bases (including official residences, clubs, messes and domestic areas i.e. non-classified areas) established in accordance with local standing orders. The introduction of the minimum measures outlined in the Alert States will reflect a higher state of security protection required to counter an increase of terrorist threat. Additional measures for each standard alert state may be specified by the responsible authorities. (AJP 2.2)

INTENTIONALLY BLANK

REFERENCE PUBLICATIONS

C-M(2002)49, Security within NATO
C-M(2002)50, Protection Measures for NATO Civil and Military Bodies, Deployed NATO Forces, and Installations against Terrorist Threats
CM 2007/0004, *NATO Policy on Contractors Support to Operations*

MC 133/4, *NATO's Operations Planning*
MC 161, *NATO Strategic Intelligence Estimate*
MC 324/3, *The NATO Military Command Structure*
MC 400/3, *MC Guidance for the Military Implementation of NATO's Strategic Concept*
MC 411/1, *NATO Civil-Military Cooperation Policy*
MC 422/3, *Information Operations Policy*
MC 458/2, *NATO Education, Training, Exercise, and Evaluation Policy*
MC 472, *NATO Military Concept for Defence Against Terrorism*
MC 0603 *NATO Comprehensive CBRN Defence Concept*
MC XX, *Policy for Force Protection*

AAP-6, *NATO Glossary of Terms and Definitions*
AAP-15, *NATO Glossary of Abbreviations Used in NATO Documents and Publications*
AJP-01, *Allied Joint Doctrine*
AJP-2, *Allied Joint Doctrine for Intelligence, Counterintelligence, and Security*
AJP-2.2, *Counter-Intelligence and Security Procedures*
AJP-3, *Allied Joint Doctrine for the Conduct of Operations*
AJP-3.2.3.3, *Allied Joint Doctrine for Military Police*
AJP-3.3, Allied Joint Doctrine For Air and Space Operations
AJP-3.4.9, *Allied Joint Doctrine for Civil-Military Cooperation*
AJP-3.6, *Allied Joint Electronic Warfare Doctrine*
AJP-3.8, *Allied Joint Doctrine for Chemical, Biological, Radiological, and Nuclear Defence*.
AJP-3.10, *Allied Joint Doctrine for Information Operations*
AJP 3.12, *Allied Doctrine for Military Engineer Support to Joint Operations*
AJP-3.15, *Allied Joint Doctrine for Countering-Improvised Explosive Devices*
AJP-4, *Allied Joint Logistics Doctrine*
AJP-4.5, *Allied Joint Doctrine for Host Nation Support*
AJP-4.10, *Allied Joint Doctrine for Medical Support*
AJP-5, *Allied Joint Doctrine for Operational-Level Planning*

ATP-3.3.6, *NATO Force Protection Doctrine for Air Operations*
AJMedP-7, *Allied Joint Medical Doctrine for Support to Chemical, Biological, Radiological, and Nuclear (CBRN) Defensive Operations*.
Bi-SC Functional Planning Guide, Force Protection

ACO Comprehensive Operations Planning Directive

AC/237-D (2012)0001 NATO Crisis Response System Manual (NCRSM)
AC/336-D (2011)0033 final NATO Air and Missile Defence Policy (AMD)
AD 65-11, ACO Standing Policy and Procedures for Intelligence Production Management, 12 July 2010
AD 70-1, ACO Security Directive, 25 March 2009
AD 80-25, ACO Force Protection Directive, 14 May 2009

INTENTIONALLY BLANK

AJP-3.14(A)(1)