

SUPREME HEADQUARTERS
ALLIED POWERS EUROPE
B-7010 SHAPE BELGIUM



GRAND QUARTIER GÉNÉRAL
DES PUISSANCES ALLIÉES
EN EUROPE
B-7010 SHAPE - BELGIQUE

ACO DIRECTIVE (AD) 80-25

TT 206383
14 May 2009

ACO FORCE PROTECTION

- REFERENCES:
- A. Allied Joint Doctrine for Force Protection AJP-3.14, dated 26 Nov 07.
 - B. NATO Crisis Response System Manual (NCRSM), Final, dated Sep 07.
 - C. ACO Guidelines for Operational Planning (GOP), Final Revision 1, dated 18 Jul 05.
 - D. ACO Forces Standards – AFS Vol VII – Combat Readiness Evaluation of Land HQs & Units (CREVAL), dated 01 Feb 09.
 - E. ACO Security Directive 70-1, dated 25 Mar 09.
 - F. Military Engineering Volume IX, Force Protection Engineering, Part I Fundamentals, Issue No 1.0, dated Jan 07.
 - G. Joint Forward Operations Base (JFOB) FP Handbook, dated Dec 06.
 - H. Bi-SC 85-1 Capability Package Directive (Interim), dated 11 Jun 07.
 - I. NATO Glossary of Abbreviations used in NATO Documents and Publications AAP-15 (2007).

1. **Status.** This directive represents a complete rewrite of ACO Directive 80-25 - ACO Force Protection dated 23 May 2006. It is effective immediately.

2. **Purpose.** This ACO directive is the operational / tactical complement to the strategic AJP-3.14 (Reference A). This directive provides the basis for Force Protection (FP) advice given by any JFC or subordinate command. This document is also an exercise in Knowledge Management, to record the hard-learned experience of many nations during operations.

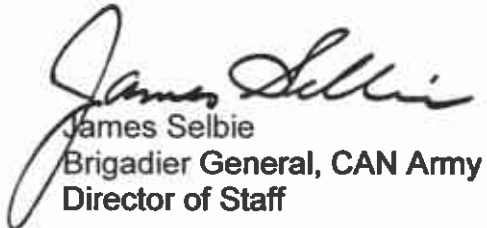
3. **Applicability.** This directive is applicable to all ACO headquarters/units and has been written to provide FP Direction & Guidance for operational-level planners, as well as practical examples for tactical-level units.

4. **Supplementation.** Supplementation is authorised. The proponent at SHAPE is to be provided with a copy of any such supplement.

5. **Publication Updates.** Updates are authorised when approved by the Director of Staff (DOS), SHAPE.

6. **Proponent.** The proponent for this direction is the Joint Operations Section in J3 Division – Joint Operations Support Branch, SHAPE.

FOR THE SUPREME ALLIED COMMANDER, EUROPE:



James Selbie
Brigadier General, CAN Army
Director of Staff

AD 80-25

TABLE OF CONTENTS

	Page	Paragraph
CHAPTER 1 – OUTLINE OF FP		
Scope	1-1	1-6
Definition	1-1	1-8
Responsibilities	1-2	1-10
The Need for FP	1-3	1-11
Principles	1-3	1-14
Capability Areas	1-5	1-15
Force Generation Process & Funding	1-8	1-17
CHAPTER 2 – THE FP PROCESS		
Initiation	2-1	2-2
Constraints	2-4	2-7
Environmental Factors	2-6	2-8
Opposing Forces and Threat Assessment	2-7	2-9
Alliance Forces	2-9	2-17
Focus Areas	2-11	2-19
CONOPs Development	2-15	2-20
Review	2-18	2-22
ANNEXES		
A	Relevant NATO FP Documentation	A-1
B	NATO FP Posts and Responsibilities	B-1
C	Common Principles of Incident Management	C-1
D	FP Planning Template	D-1
E	Threat-Capability Matrix	E-1
F	Crisis Response Operation Urgent Requirement (CUR) Process	F-1
G	C-IED Defeat Activities – With Utility for FP	G-1
H	FP Measures	H-1
I	Military Engineering Design Guidelines for Expeditionary Operations	I-1
J	Example Annex J for FP	J-1
K	Force Escalation	K-1
L	Tactical Landing Zones	L-1
M	Force Health Protection - Occupational Health & Safety and Fire Prevention	M-1
N	Counter Surface-Air-Missile Operations	N-1
O	Example Defence Plan Diagram	O-1

AD 80-25

		Page	Paragraph
P	FP Vulnerability Assessment	P-1	
Q	FP Minimum Standards and Essential Tasks for CRO	Q-1	
R	Identity Management for FP	R-1	
S,T	Not issued at this time		
U	Example Annex U – Operations in a CBRN Environment	U-1	

AD 80-25

CHAPTER 1

OUTLINE OF FORCE PROTECTION

1-1. This directive has been written to offer guidance on **how** to write and implement FP plans; whereas the strategic-level Direction & Guidance (D&G) contained in the AJP-3.14 defines **what** FP is. Best practice and guidance have been incorporated from operations, training, and the documents listed in the References.

1-2. Modern operations are marked by complexity. The multi-national nature of NATO operations adds a degree of complexity but more significantly, operations are likely to be distinguished by an inter-relationship between terrorism, insurgent activity, criminality, corruption and local power disputes. It has been shown that in complex situations like this, it is the force that able to adapt the quickest that succeeds.

1-3. Therefore, **a dynamic planning process is a prerequisite for successful operations**. Plans need to be made from the 'top down' to integrate with higher level master plans and synchronize the efforts of the many forces involved. This approach is required on every level because the sheer number and variety of Alliance forces and other agencies can lead to confusion.

1-4. This document focuses on FP but is structured in line with the Operational Planning Process (OPP) to achieve workable FP plans that make sense of the complex operational environment. Using the OPP, individuals can incorporate their detailed and specialist knowledge whilst following proven guidelines. The aim of producing this document is to help FP staff combine good sense with best practice in order to identify the most effective Tactics Techniques and Procedures (TTPs). This approach will ensure that commanders have the utility to protect their forces for all types of military operation against all types of threat.

1-5. One must not forget that plans take a great deal of effort to implement and keep them valid as the situation changes. This is operational art.

1-6. **Scope.** The structure has been designed to first present the theory and background information about FP (Chapter 1) followed by the FP planning process (Chapter 2). The annexes offer specific planning and implementation guidance.

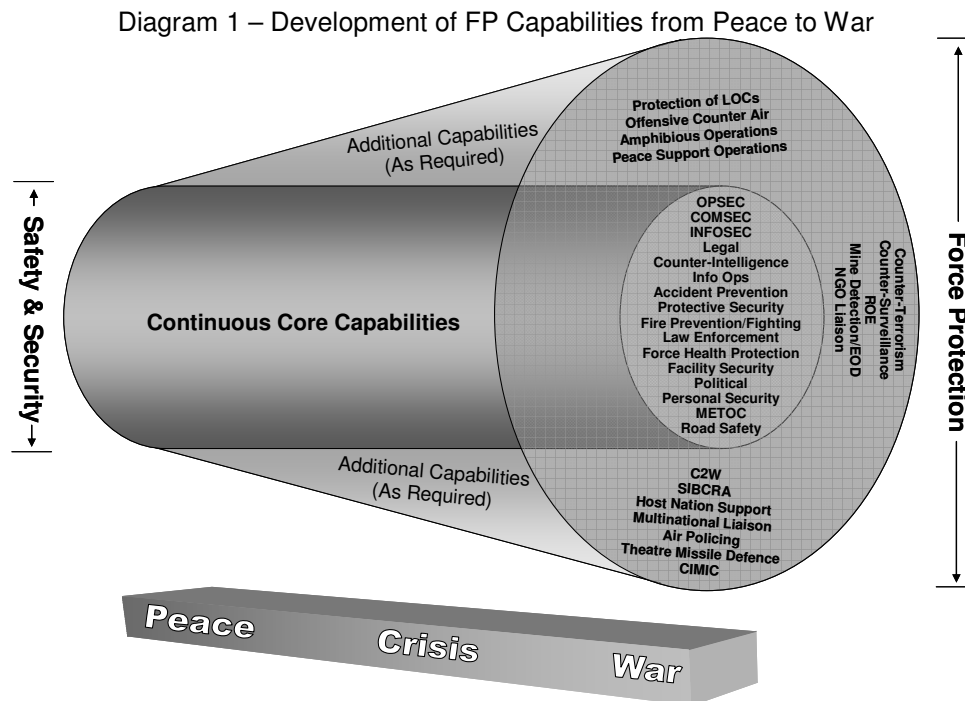
1-7. There is considerable scope during the planning process for overlap or duplication between the different topics; however, this ensures important concepts are definitely covered. The best technique is to **start hard – finish easy**, as all the information is processed in the early stages and leads naturally to clear requirements.

1-8. **Definition.** FP is defined as 'measures and means to minimize the vulnerability of personnel, facilities, materiel, operations and activities from threats

AD 80-25

and hazards in order to preserve Freedom of Movement (FOM)¹ and operational effectiveness thereby contributing to mission success².

1-9. FP is classified as an Essential Operating Capability³ (EOC) and can create a safer environment in which forces are able to focus on their main objectives. It is about bringing together many sub-capabilities under one control / coordinating element in order to counter the threats from an adversary, natural and human hazards including fratricide in order to ensure security and FOM. Because the scale of FP is entirely dependant on the situation and threat, not all sub-capabilities will be required all of the time. This is especially important given that, for political and military reasons, a deployed footprint should be kept as small as possible. The diagram below illustrates what FP sub-capabilities could be needed from peace to war.



1-10. Responsibilities

a. **FP is the Commanders' responsibility** and as such they must ensure FP is provided for all aspects of their assigned forces and facilities. Troop Contributing Nations (TCN) will be responsible for their own FP and for contributing to the wider protection of the force to which they are assigned. Host Nations (HN) may be responsible for the provision of FP depending on agreements reached with the HN. Legal constraints to physical FOM, and

¹ Movement refers to the physical ability to move around the Area of Responsibility (AOR) as well as the morale and political scope to implement plans within it.

² AJP-3.14

³ FP is defined as an Essential Operating Capability in Military Committee (MC) 161.

AD 80-25

powers of stop, search, arrest and detention should be detailed in relevant agreements such as a Military Technical Agreement or Status of Forces Agreement (SOFA), Rules of Engagement (ROE) or Operational Plans.

b. **NATO Staff.** The NATO Peacetime Establishment (PE) exists within the standing HQs throughout member nations. Each HQ has FP staff and they undertake specific roles as well as support to each other. Annex B has been included to clarify what the responsibilities are of NATO FP staff at the various levels of an operation.

1-11. **The Need for FP.** Current and foreseeable operations are very difficult to define and prepare for; operations are likely to range from peace-support to war-fighting at the same time in the same area, and are likely to involve deploying a Combined Joint force into a failed or failing state or even crisis zone. Any deployed force will need to preserve its fighting potential for the operations that matter and minimise losses against natural or human hazards.

1-12. However, the most likely scenario and the one that requires the most complete FP plan is protecting against persistent, low-intensity threats from complex, adaptable, and difficult-to-identify extremists. Action against a NATO deployed force will normally be to affect our physical and political FOM and is only limited by imagination; hence, there is a constant asymmetric threat designed to capitalise on surprise and to cause rapid escalation in an attempt to overload Alliance forces and the casualty or cost tolerance threshold within the TCNs. Opposing forces understand that small, carefully targeted tactical operations can have a strategic impact against the public opinions of TCNs.

1-13. Knowing the **intent** and **capability** of the threat is paramount to implementing effective FP and thereby provide Alliance forces the FOM needed to conduct their primary mission. Other dimensions that define the operating landscape are crime, ungoverned or ungovernable territory, and espionage threats from Foreign Intelligence Services (FIS), all of which can make FP planning a very intricate process. Following the process explained within Chapter 2 will ensure effective FP.

1-14. **Principles.** The following principles are essentially the main parts of the planning process, as detailed in the AJP-3.14. They have also been illustrated in the 'FP Model' on page 10⁴. The planning process is covered in detail in Chapter 2 and a thorough template is at Annex D⁵ with hard-learned guidance contained within it.

a. **Prioritisation.** Staff can prioritise how finite FP resources should be allocated by balancing mission imperatives against known vulnerabilities and the impact of losing them. When, rather than if, the situation changes, the FP C2 can quickly reallocate resources by pre-agreed priorities as based on the threat. This process is explained in the Threat-Capability Matrix at Annex E.

⁴ Although illustrated differently in the AJP-3.14, this FP model shows the same clear steps needed to apply the principles.

⁵ The template plan includes all significant detail for operational and tactical use.

AD 80-25

b. **Threat Assessment (TA).** Again, Annex E has been written to help make a TA, but the real support would come from specialist Intel staff. Understanding the various threats allows for sustainable and realistic counter measures to be implemented. The threat is coupled with the mission imperatives to establish the priorities for FP and ensure time, effort and money is rightly focused. In essence, the threat is viewed from 2 perspectives:

- (1) Opposing forces' **intent & capability**; and
- (2) The **vulnerability** of losing Alliance locations or operational capability.

c. All sources of intelligence need to be constantly reviewed in order to maintain Situational Awareness (SA) so an appraisal can be made of what is most at risk. Perhaps the COE points offer an easy target, perhaps equipment is vulnerable to Indirect Fire (IDF), and perhaps the supply of food, water or energy can be easily interdicted. Also intentional and naturally occurring environmental threats to force health may exist. Medical Intelligence will enhance ability to recognize these threats and produce a health risk assessment and recommendations. Each possible opposing force Course of Action (COA) needs assessing in terms of **likelihood** to help define FP priorities.

d. **Risk Management.** Risk must be minimized because it cannot be eliminated. Casualties and materiel damage are an implied risk in military operations, and an unrealistic expectation to avoid such effects may impact adversely on the accomplishment of the mission and, when casualties ensue, undermine political and military resolve. Balancing the financial and political costs / consequences between success and failure of certain FP measures can identify what the real risks are.

e. FP staff needs to prioritise and understand the TA before allocating finite resources. This means there will be capability gaps or weaknesses at best. Therefore, a Risk Mitigation Plan⁶ is required to document what risks exists, what will be done to resolve weaknesses, and what the impact will be if weaknesses are exploited. **The Risk Mitigation Plan would be signed by the commander whose responsibility it is to provide resources to solve capability gaps – this is Risk Transfer.** FP staff must advise the Commander so he can conduct a balanced risk mitigation assessment in order to accept / avoid risks based on the operational impact in relation with available resources.

f. **Interoperability.** Interoperability with all force components and civilian agencies can be achieved through **common communication systems,**

⁶ Also known as a Risk Register or Contingency Management Plan.

AD 80-25

synchronising patterns of work and standardising TTPs. Interoperability also includes understanding HN and other Alliance members' perceptions, concepts, policies and procedures. This can be achieved through common identity management and communications systems, and frequent face-to-face liaison. This can be developed during the analysis of Alliance forces during planning and can lead to **cohesive FP operations**.

g. **Flexibility.** FP forces must have the scope to adapt to and meet any threat as it arises, and at the same time be able to undertake Contingency Management (CM) after any accident / incident in order to restore efforts back to the primary mission. Flexibility derives from planning by the FP C2 element, and such plans must be rehearsed otherwise they will not work when the real emergency comes.

h. **Tactical Area of Responsibility (TAOR).** The TAOR, sometimes called a Ground Defence Area (GDA), is a vital part of establishing effective FP around a static location. Experience shows the advantages of a TAOR far outweigh the disadvantages. A TAOR allows unity of command for all FP assets on and around the location; it reduces the number of 'seams' that opposing forces could exploit. Additionally, seams between units provide scope for confusion and inefficiency. A TAOR ensures one FP C2 element has control over all layers of the location's defence and allows the C2 to coordinate the activity out to the limit of opposing forces' weapon range. External activity outside of the location's perimeter fence is not a stand-alone requirement and cannot be divorced from internal / perimeter measures. All efforts must be integrated to achieve early warning, unity of command, mutual support and depth.

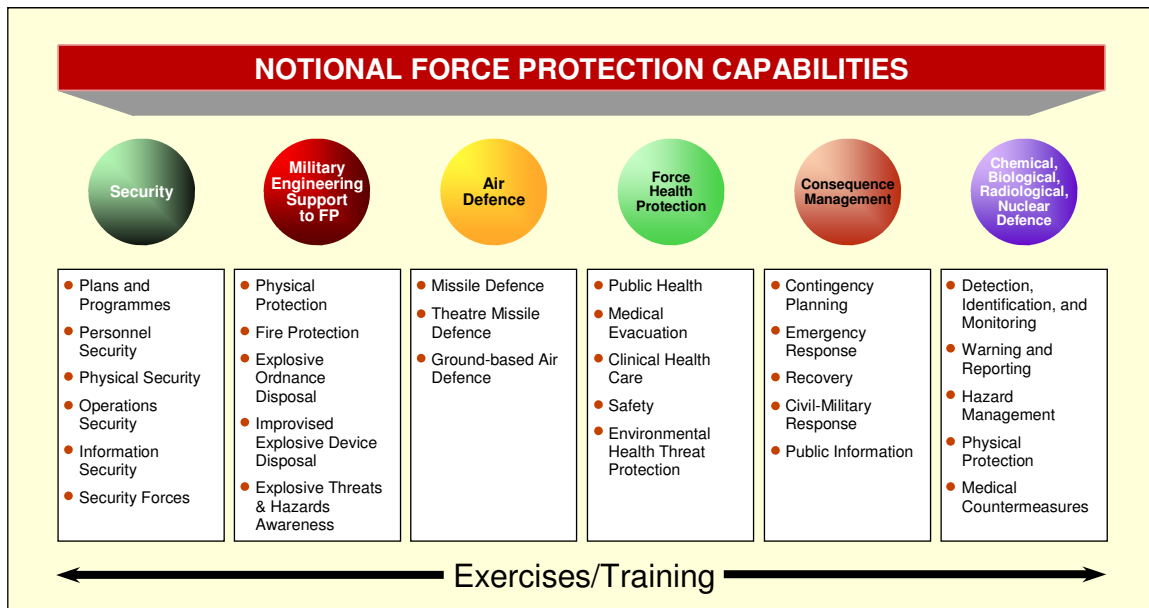
1-15. **Capability Areas.** Depending on individual perceptions, the requirements for FP can range from far-reaching to very limited. As a result dedicated FP C2 can sometimes be neglected and even if it exists the C2 may lack the authority to coordinate all the assets it needs to ensure **cohesive** operations.

1-16. FP must be a centrally controlled effort because the overall effect is greater than the sum of the individual parts. **Centralised control of FP is vital.** The capability areas given in the AJP-3.14 have been outlined below but C2 has been added due to its importance.

Note: More detail on sub-capabilities has been added at Annex E, the 'Threat-Capability Matrix, which has been included as a tool to be used on real operations to help users make an objective assessment of the threats and to prioritise counter-measures.

AD 80-25

Diagram 2 – Possible FP Capabilities



a. **Command & Control.** A dedicated C2 is essential for effective FP; it may not have 'command' but more actual Direct Local Authority (DIRLAUTH) whereby the higher commander allows the FP C2 to coordinate the day-to-day activity of sub-capabilities in order to achieve **unity of command**. The FP C2 element should undertake the planning process and implement the most effective FP posture. As threats evolve the FP C2 element needs control of FP sub-capabilities in order to protect the commander's priorities. This occurs day-to-day and in emergencies, which is why the planning process needs to be familiar to the FP C2 staff so they can quickly work the decision making process.

b. **Security.** Security forces will be very diverse and may need to undertake internal or external patrolling, social policing functions, COE, and Point Defence. This area covers all aspects of personnel and physical security as well as INFOSEC and OPSEC. These measures are the constants within FP that will need attention during peace to any level of operation. Of strategic importance within this capability area is the threat from high yield explosives, for example suicide bombers and Improvised Explosive Devices (IED). Because of the strategic importance of Counter-IED (C-IED), this will normally be undertaken as a separate effort with major resources allocated to support it.

That said, integration with FP is important as IED attacks around locations of strategic or operational importance could have dire second order effects, e.g. the inability to provide battlefield mobility because the rotary wing assets have no or little fuel due to the destruction of the fuel transfer point at the airhead.

AD 80-25

c. **Military Engineering.** Military Engineering (MilEng) support to FP is of huge importance. Military Engineers, as well as professional fire-fighters, need to be involved from the design stage onwards to ensure protection against blast and fire is incorporated into COE points and accommodation, as well as many other mission essential locations without higher costs being incurred later in the operation.

Aspects of 'town planning' should also be included when bases are established to make sure the infrastructure is built to meet the right level of threat, as well as meet the needs for water, sewerage, messing and waste disposal. Experience from recent operations has proven that the failure to involve MilEng expertise at the beginning has led to very high costs and time delays later, not to mention the negative morale effects on the deployed troops or homeland political impact due to negative media coverage. Annex I gives further details on MilEng support and defines the Minimum Military Requirement (MMR) in generic terms for NATO expeditionary operations.

Explosive Ordnance Disposal (EOD) not only achieves their obvious primary duties but with proper integration through the FP C2, forensic exploitation is possible to support the C-IED effort. Annex G gives further details on the aspects of this.

d. **Air Defence.** Air Defence will be undertaken by specialists, but will need incorporating into FP at the C2 level to ensure integration into the Warning & Reporting systems (W&R). Given the potential threat of CBRN payloads in weapons and devices which can be delivered by all kinds of aerial platforms, a Chemical, Biological, Radiological or Nuclear (CBRN) hazard might occur (normally to impose a psychological and logistical burden on deployed troops) so Air Defence will need integrating with Chemical Biological Radiological Nuclear (CBRN) plans.

e. **Force Health Protection.** Force Health Protection is a critical and key supporting component of Force Protection. The reduction or elimination of threats to the health of force personnel from diseases and injuries is the primary objective of Force Health Protection and contributes significantly to the goal of maintaining operational and combat readiness/effectiveness. Force Health Protection includes a wide array of medical and health specialty areas including deployment health surveillance, food and water sanitation, disease vector control, occupational health and safety, health promotion, disease outbreak investigation, and CBRN agent exposure prevention issues. Force Protection officials must work in close association with Theatre Medical Advisors and Force Health Protection officers to ensure that FHP threats are included in the overall FP threat assessment.

f. **Consequence Management (CM).** This aspect of FP is about prior planning and preparation to prevent poor performance when real emergencies materialise. Plans should be clear, simple and follow common principles so

AD 80-25

troops who may be under extreme time pressure during incidents are able to remember what they need to do. Thought is required about Civil-Military Response and what agencies / pools of manpower can undertake specific roles. Everything needs rehearsing! Some principles of CM are laid out in Annex C.

g. **CBRN Defence.** The threat will drive the need to: deploy and activate CBRN W&R systems, plan for CBRN Reconnaissance, Surveillance and Sampling teams, prepare Decontamination assets and facilities, establish Collective Protection (COLPRO) shelters, issue orders for appropriate CBRN/TIM threat levels to include IPE (Individual Protective Equipment) dress states and so forth. Integration with the medical services will be needed to deal with CBRN casualties. In failed or failing states, industrial infrastructure may be decrepit. Risks from Toxic Industrial Materials (TIM) are therefore of concern. A theatre recce / sampling capability is invaluable in this situation to log all potential threat areas so further action can be taken. Additionally, there is obvious benefit to the HN when TIMs are removed.

h. **Identity Management.** Effective Force Protection can only be provided if the necessary controls are in place to distinguish Blue from RED and Grey forces. An integrated identity management infrastructure will be key in establishing this. This IDM needs to be provided with the necessary tools as to ascertain the authenticity of the identities over the mission lifecycle such NATO Public Key Infrastructure derived authenticity.

1-17. **Force Generation Process & Funding.** This section has been added to develop an understanding about how NATO generates manpower and funding for procurement. There are too many details to include everything here, but these are well explained in Reference H (Bi-SC 85-1).

a. **Force Generation**

(1) **Crisis Establishment (CE).** The CE is an authorised list of manpower and personnel requirements for a unit, formation or HQ under crisis conditions. The CE contains military and civilian posts. Nations are called upon to bid for CE positions in the ranks of OF-4 and below. Nations bid for the positions at the regular SHAPE Manpower Coordination Conference or when a requirement is identified. Posts for OF-5 and above are determined by the "Flags to Posts" (F2P) process that is owned and managed by SHAPE. SHAPE determines which nations are eligible to fill all OF-5 and above posts based on their Combined Joint Statement of Requirements (CJSOR) contribution.

(2) **Peacetime Establishment (PE).** The PE sets the authorised peacetime organisational structure and manpower requirement for a unit, formation or HQ.

AD 80-25

(3) **Combined Joint Statement Of Requirement (CJSOR).** The MMR for forces in a theatre of operations is defined in the CJSOR. The capabilities within it are delivered and paid for by the Troop Contributing Nation (TCN).

(4) **Theatre Capability Statement of Requirement (TCSOR).** The TCSOR is a table of required theatre capabilities deemed to be eligible for Common Funding. Resources under the TCSOR can be redeployed by the theatre commander from their originally designated role / location.

(5) **Voluntary National Contribution (VNC).** In addition to those posts that are designated by the CE, nations may also contribute personnel as VNCs in excess of the CE requirements. These are either on the basis of specialist knowledge, in support of other national functions that are not bound by CE, CJSOR or TCSOR constraints.

b. **Common Funding.** Common Funding is provided by NATO to provide money for personnel, services or resources. The process used to request funding is the Crisis Response Operation Urgent Requirement (CUR), which is detailed at Annex F, and in complete detail in Reference H⁷. Eligibility for an operation is defined by the Senior Resource Board (SRB) for funding through: NATO Security Investment Programme (NSIP); or Military Budget (MB).

NATO will only pay those costs that are not attributable to a specific nation and are deemed as critical theatre-level enabling capabilities (as defined in the OPLAN as part of a TCSOR). The technical solution must be in line with the duration of the operation and not exceed the MMR. More detail is given below:

(1) **NATO Security Investment Programme (NSIP).** Costs cannot be attributable to any single nation and for requirements that have not been identified in the Military Budget. Therefore, the NSIP consists of a programme of capital investments in military capabilities that exceed the national defence budget of individual nations. These funds would be used to pay for items such as fixed infrastructure, CIS equipment and deployable strategic equipment. This is where the MMR is used to define the need for the request (see Annex I), and if an MMR does not exist, then one could be suggested as the final design.

(2) **Military Budget.** This money is used to pay for manpower to fill CE, PE and emergency establishment positions, operating & maintenance (O&M) costs, mission operating expenses and capital expenditure of the network of NATO military HQs, programmes and agencies.

⁷ All new infrastructure requirements are to include FP measures into ALL CURs, as mandated in Annex D to Reference H (Bi-SC 85-1).

AD 80-25

c. **Theatre Financial Controller (FINCON).** The Theatre Financial Controller (FINCON) is responsible for the financial management and contracting of the common-funded resources in theatre (except of those under the direct responsibility of lead nations). The Theatre FINCON is authorised to approve commitments of funds, and via his Purchasing & Contracting officer, to enter in to legal obligations supported by the Military Budget approved for the operation. He is authorised to undertake obligations supported through NSIP funding as approved by the IC on a project-by-project basis. Unless otherwise specified, he is authorised to grant departures from procedures for MB-funded acquisitions up to NATO established financial limit (EFL) Level D for recurring requirements/follow-on support. Within means and capabilities, nations may use the services of the Theatre FINCON in the framework of the implementation of national projects in support of the operation. As a rule, this will require nations to provide full funding of the projects in advance. No pre-financing from NATO common-funded resources should be considered.

d. **National Funding Streams.** Nations can be refunded for pre-financing projects by passing a Type B Cost Estimate (TBCE) through the Infrastructure Committee (IC) (see Annex F).

e. **Cost Estimates**

(1) Type A (TACE) is used to describe requirements.

(2) Type B (TBCE) is used mainly in the CUR process to assess the overall cost or for refunding a nation for pre-financing a project.

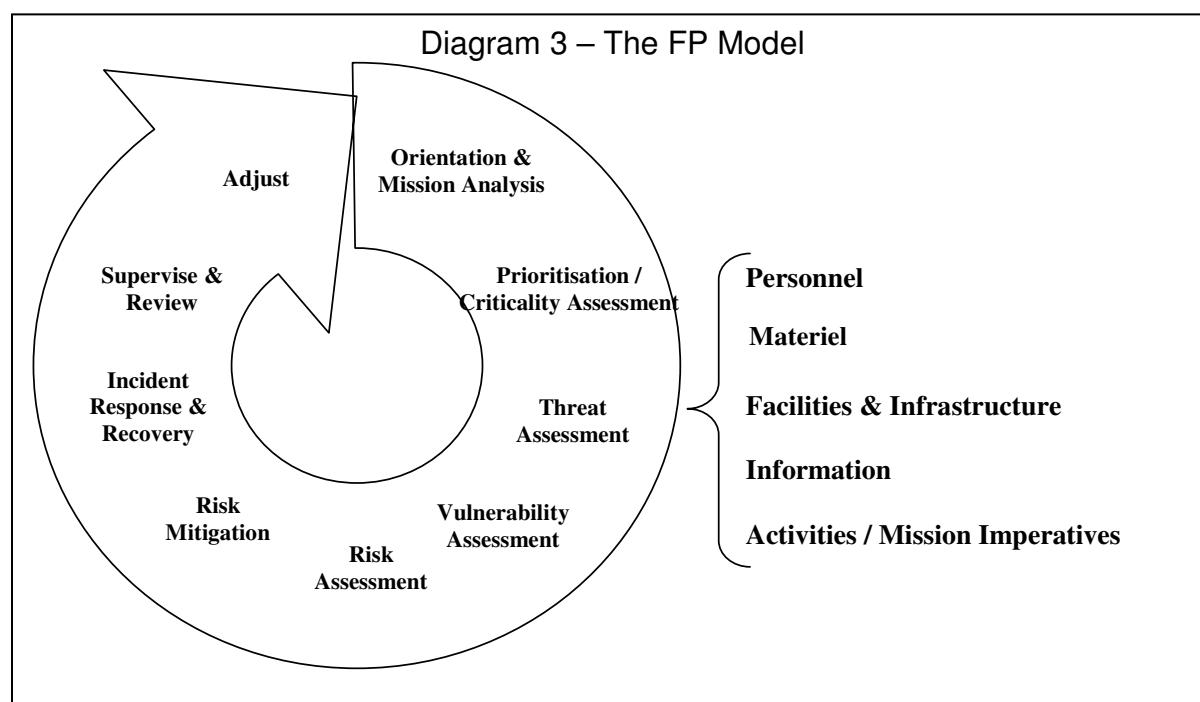
(3) Type C (TCCE) is used when cost over-runs are expected or have occurred.

AD 80-25

CHAPTER 2

THE FP PROCESS

2-1. This chapter has been structured in line with planning principles as it is an effective way of describing FP, containing the current FP knowledge, and enabling the user to produce effective FP plans. The FP planning process is effectively the same as the OPP, but a few aspects may appear slightly different because of some unique requirements. Additionally, for lower levels of command, planning may be simplified by just using the principles given in Chapter 1 and as represented in Diagram 3 below.



INITIATION

2-2. This phase of the planning ensures that the unit has considered their place in the higher commanders' (plural) overall plan. This means considering what the FP units can do to achieve their mission **and at the same time** help the commanders achieve their operational and / or strategic goals. This stage of planning ensures continuity between all levels of the operation. Some of the examples below are more for the theatre-level FP planners than for tactical units, but a broad understanding by all FP staff is useful.

2-3. Initiation should begin with gathering the mission statements, assigned military tasks, direction from senior staff, intents, specified tasks and implied tasks

AD 80-25

from all senior levels of command. By asking how each aspect is relevant to FP allows staff to clearly identify and analyse important roles. This may appear long-winded, but it pays dividends in terms of operational effectiveness in the long-run.

2-4. The point being made with the examples below is that a high-level view can identify priorities and justify certain COAs. Additionally, operations at all levels of command can be aligned. For long-term success, FP operations need to consider how the environment can be proactively shaped, i.e. winning the consent of the local population. Because of this, many of the ideas given in this document are about raising the priority of other operations around the location being defended that can contribute to the same aims.

2-5. It must be made clear that FP forces are not required to undertake the work of anyone else or even start tasks that are outside of their expectations; rather it is about assessing what needs to be done, justifying what units are required and perhaps help coordinate their activity.

a. **Higher-Level Assigned Military Tasks.** An example of a higher commander's assigned military task could be '*to protect energy or government infrastructure*'. This could impact on tactical FP because infrastructure may exist in the TAOR and would therefore require some effort to protect it. The destruction or maintenance of local electric sub-stations, gas pipes, schools, police offices, etc. would directly influence to local populations view on Alliance presence. In extreme cases, there may be an increase in attacks should their living conditions worsen and opposing forces gain sympathy from the local population. Alternatively, a broad, long-term view of FP may require security of energy and government infrastructure.

b. **Intent.** The Intent may be '*to deploy rapidly and visibly to protect High Value Assets (HVA) in order to ensure FOM for Alliance forces*'. **At this early stage of the planning process, many significant deductions can be made.** For example, an appreciation of this task during an estimate process would lead one to deduce that protection of the HVAs is a priority and requires a highly visible presence on the ground. Conclusions and resultant tasks that fall out from this line of thinking may include patrolling off-base and establishing relationships with the locals and understanding their patterns of normal daily life may be important. The follow-on deductions could be language barriers; the ability to interact with the local populace given that patrolling troops may be constrained by a nationally-mandated protective posture; the required range, duration, and frequency of patrolling; who the adjacent friendly units are and what boundaries / systems of liaison can be used.

c. **Specified & Implied Tasks.** The specified task/s may be as simple as '*provide FP of...*'. The definition of FP is a good place to start as is the Threat-Capability Matrix at Annex E, which highlights a list of realistic threats and

AD 80-25

possible capabilities needed to counter them. The list of implied tasks is limited only by imagination as to what needs undertaking to achieve the specified tasks. For example, *'providing vetting of all Locally Employed Civilians'* means using administration and intelligence personnel to collect, research and process information about individuals as well as establishing a system of identification.

d. **End State.** Understanding the commander's desired end state ensures there is a goal to work towards, and provides the guidance for FP staff to decide what their End State will be. For example *'establishing a stable environment in which peaceful and fair elections can be held'* means that much of the FP effort may have to be working with the populace in the TAOR to develop stable local conditions. A bunker mentality in this situation would be inappropriate.

e. **Main Effort.** The Main Effort allows commanders to prioritise work and resources, such as *'deny opposing forces FOM'*. When producing FP orders, one should decide what single task will form the bedrock of the FP work. For example the key task to enable all other tasks could be to *'establish C2 that has control over all FP sub-units'*. Such a task would involve having the higher commander's permission / Direct Local Authority (DIRLAUTH) to coordinate the efforts of important elements such as Fire Crash Rescue Service (FCRS), medical and dental teams, environmental health experts, CBRN Warning & Reporting cell, as well as influencing messing times to reduce population density in areas vulnerable to Indirect Fire (IDF).

f. **HN Liaison.** There may be a need to work along side the local security forces in order to promote wider cooperation, mutual support and depth of protective measures, as well as foster a valuable source of information. Additionally, higher commanders may wish to achieve mentoring or training of local forces with a view to transfer the lead for security responsibility. Again, to stabilise the area around locations of operational importance, it may be wise to raise the priority for such operations in the TAOR. Perhaps the local FP unit would be able to fulfil this function without the need to deploy additional manpower into theatre for this specific task.

g. **Information Operations (IO).** It may be possible for FP operations to take advantage of or contribute to the Information Operations (IO) campaign. Such examples include informing the HN population about Force Escalation (FE) procedures (see Annex K), i.e. how to react to military convoys and at check-points. Getting the correct messages out can help to increase compliance and good will.

h. **Consent Winning & Measurement.** FP units may prove an excellent tool for delivering or supporting initiatives that harmonise the interests of the local population with those of the Alliance. At the same time, it is highly likely

AD 80-25

that patrolling units can gather information of intelligence value from their limited TAOR. Greater stability can be brought to the area around the location by protecting the delivery of CIMIC and Veterinary and Medical Outreach (VMO) projects. Liaising with Non-Government Organisations (NGO) and / or International Organisations (IO) to support or prioritise work in the TAOR for refugees, food or health may help develop greater stability in the TAOR.

i. One way to measure consent in an area is to allow the same tactical commander into the same area who can then gauge the mood of the local populace. Over a period of time, trends can be observed and assessed against ongoing operations to see if Alliance forces are seen more or less favourably over time. This is an important feedback system to prevent wasting resources and effort.

j. With FP units being a constant feature in the TAOR and supporting the delivery of such projects could develop a greater degree of consent from the local population. Developing this thought further, and depending on the reader's point of view, such FP effort could be extended to support the intelligence gathering effort in building a picture of the local patterns of life.

k. Activity like this may promote social stability around mission critical locations and may even indirectly contribute to longer term mission success. And even though one or even 2 projects may not be obviously successful, a thorough and integrated approach would increase the chance of success and add another dimension to the defence plan.

l. **Embargos.** Maybe the FP unit could undertake a role in stopping or searching potential criminal activity or smuggling. It is important to consider unintended side-effects such as a resultant increase in attacks on Vehicle Check Points (VCPs). If a status quo of non-confrontation is maintained between Alliance and opposing forces, it is important to know that you are in control of such a decision.

2-6. With a dedicated FP C2 element, there are / would be sufficient staff to contribute towards higher-level, longer-term issues as covered above at the same time as undertaking their tactical mission.

CONSTRAINTS

2-7. Good planning should provide the justification to convince higher commanders to relax the limiting factors that may constrain or impede the success of the FP mission. Some examples are given below:

AD 80-25

- a. **Time.** There may be deadlines to prepare plans, complete training, deploy, and provide an Initial / Full Operational Capability (IOC / FOC). Training time is of huge importance and some preparations may have to be undertaken in theatre or the deployment date postponed.
- b. **Space.** There may be no authority to patrol off base, but higher commanders should at least be requested to challenge some caveats if they are impacting on the chances of mission success. However, some constraints are politically imposed and need to be observed for strategic reasons. A constraint such as not being able to dominate the TAOR would require an FP unit to coordinate with their adjacent forces in order to control the areas beyond their perimeter.
- c. **Physical versus Social Environment.** Static locations have very little choice other than to accept some constraining factors of time and space. The mission must be conducted at that time and the base infrastructure may be too complex to relocate. Moving the local population, if at all possible, would lose consent towards the Alliance. Static locations are difficult to defend so a proactive approach to engaging with the local population is needed. Rather than shaping the physical environment, the 'social' environment can be influenced.
- d. **Combat Service Support (CSS).** It is important to recognise the logistical footprint of FP operations. This can be in the form of consumable equipment to maintaining observation devices, weapons, vehicles, etc. There may be a higher maintenance demand on equipment due to the climate and terrain. Issues regarding specialists to operate and maintain loaned / donated equipment also need considering.
- e. **Personnel.** FP staff will have a good idea about the number of troops they need for a particular mission; however, it is worthwhile ensuring specialisations are accounted for such as infantry, Police, CI, Intelligence, etc. More or specialist / liaison positions can be requested at this early stage and revisions suggested to the Statement of Requirement (SOR).
- f. **Legal Aspects.** Understanding the Rules of Engagement (ROE) including Alliance forces' powers of stop, search, arrest and detention of opposing forces is vital. National caveats and legal restrictions may limit the ability of some national contingents to use force in defence of others or to protect property where there is no concurrent threat to life. Therefore, a detailed understanding of the impact of such national caveats or restrictions is particularly vital in Alliance operations. The relevant FP related provisions of agreements such as a SOFA must be understood, both by Alliance forces and HN personnel. It is worth taking the time to ensure that local HN police and security forces are aware of such provisions. Consider making time to meet

AD 80-25

local police, security forces, prosecutors and judiciary prior before you are forced to as a result of an incident occurring (see sub paragraph 37k).

g. **Cultural Implications.** There may well be issues regarding searching of people (are female searchers required?) or body-scanning by machines (do the displays need hiding so as not to offend those being scanned?). Efforts to reduce the offence felt by the HN will be directly translated into consent. Trading benefits against the threat is important at this stage to ensure optimum levels of Risk Management. Dismounted patrolling at times may be dangerous but the populace may perceive the troops more favourably and offer greater levels of consent for Alliance operations.

ENVIRONMENTAL FACTORS

2-8. **Ground Area Analysis.** Understanding the ground enables troops to dominate the TAOR by identifying and eliminate a whole range of threats.

a. **External.** Important factors include the size of the TAOR and how accessible the terrain is by vehicle and foot. Consideration is needed into likely areas where stand off attacks / observation can be conducted by hostile forces. The ground needs breaking up into different levels of priority from a friendly **and** hostile perspective. The possible infiltration routes need identifying, as well as routes used during the normal patterns of daily life. Breaking up the external TAOR will allow the FP unit to focus their efforts on the parts that matter. Lastly, having a variety of routes / access points and alternating them is one of the most effective ways to avoid attacks.

b. **Perimeter.** The quality and type of perimeter is of obvious importance. New infrastructure such as fencing and surveillance devices can be provided by nations or through common funding via the Crisis Response Operation Urgent Requirement (CUR). It is very important to understand this process so more detail is given at Annex F. The FP Engineering MMRs at Annex I provide further technical details on perimeter protection.

c. **Internal.** The area and facilities within the perimeter of the location should also be broken down according to priorities. This allows FP staff to identify mission essential or priority working areas that require additional security or protective measures. Dining Facilities (DFAC) may need hardening and meal times spread to reduce population density. Access control may be required at DFACs or sensitive working areas. Any areas that may be targeted because they offer tempting results for adversaries will need additional protective measures. Further details on the FP Engineering MMR for ECP and infrastructure are given at Annex I.

AD 80-25

d. **Geographic / Climatic.** Both geographic and climatic factors such as latitude, altitude, and seasonal climatic conditions, should be assessed in terms of their impact on the ability of forces to operate in regards to existing and potential health threats. These threats could range from the prevalence of heat or cold injuries and other geographic and climatic factors. Also the adverse effects of prolonged operations at high altitudes, and other health treats from dust inhalation, high humidity, etc. must be taken into account. Also the frequency and severity flooding / droughts and the subsequent effects on the local community, access routes, and infrastructure need thought in order to avoid being surprised by sudden constraints, e.g. areas from where IDF attacks are launched can no longer be patrolled due to flooded or boggy tracks; after wet weather will the boggy tracks / slow-go terrain create an ambush risk?

e. **Diseases.** The threat of parasitic, bacteriological and viral infectious and communicable diseases endemic to the operating area must also be assessed and included in the overall FP Threat Assessment process. Recommended prevention measures to health threats identified in the Threat analysis and assessment process, i.e., vaccinations, prophylactic medications, personal protective clothing, mosquito nets, use of insect repellent, etc; should be included in the overall FP Plan.

f. **Flora & Fauna.** Force Health Protection experts can advise on the specific risks posed by animal and plant life. Failure to recognize, identify and educate operating forces on risks from animals and plants may lead to illness, injury or death. This can not only compromise the operational and combat readiness but may lead to criticism in the press of a government's ability to support troops. It is important to consider the logistics of medical supply and resupply for vaccines and drugs as well as shelf life, refrigeration and cold storage requirements of certain medical supplies and reagents. Also re-supply lead time must be considered for perishable and short shelf life consumable medical items.

OPPOSING FORCES AND THREAT ASSESSMENT

2-9. **Threat Levels.** The threat posed by opposing forces is measured by **capability** and **intent**. A highly motivated group with views about using extreme violence to achieve their aims may lack the capability. The opposite may also be true. It is useful to ask '*what opposing forces want to achieve and why?*' A little thought about opposing forces' COA will help prioritise the **most likely, least likely** and **most dangerous threats**, in order to focus and justify the FP posture. This also helps explain to troops why they need to be aware of and adhere to dress categories, arming states, convoy procedures and so forth. There is an opportunity here to include education and training.

AD 80-25

2-10. A Threat-Capability Matrix has been included at Annex E to highlight some of the likely threats posed to Alliance forces. However, only current intelligence for specific operations will justify why some threats need higher priority than others. The 3 NATO-recognised levels of Threat Environment are given below for guidance:

a. **Low-Level Threat Environment.** This is the likely threat level during Peace Support and Crisis Response Operations (PSO / CRO). This level means that a general threat exists, but there is a greater likelihood of peacetime incidents (such as traffic accidents, fire, injuries, etc), civil disorder, espionage from FISs and even sabotage by non-state and / or state-sponsored terrorist organizations. Toxic Industrial Materials (TIM) are also a threat as experienced in states with poor domestic infrastructure. Industrial infrastructure will also be a tempting target to contaminate people or areas, for example destroying the oil processing plants in a sea port could trigger Environmental and Industrial Hazards (EIH) which effects might be comparable to releases of CBRN substances.

b. **Medium-Level Threat Environment.** The Medium-Level Threat Environment expands on the measures for low threat levels, but involves a more localised threat without defining the specific nature, target or time. A short duration engagement is likely as are coordinated attacks from tactical air, land or maritime forces as well as Special Operations Forces (SOF). A medium-level threat would indicate that terrorists have the capability and intent to attack. The use of nuclear weapons remains unlikely but Chemical, Biological, Radiological, Nuclear (CBRN) weapons and devices to include TIM (Toxic Industrial Materials) could be used to carry out asymmetric attacks.

c. **High-Level Threat Environment.** This level expands on lower threat-levels to include a specific threat or is adopted if an incident has occurred in the same vicinity. This threat level allows for possible attacks by a Major Opposition Force (MOF) following a period of warning and tension. The full range of attack possibilities would be likely.

2-11. **Conducting the Threat Assessment.** Assessing the quantity and quality of opposing forces is a very daunting task. However, this combined with earlier efforts of the planning process means that deploying forces will fully appreciate every aspect of their operating environment. This is exactly what opposing forces will be doing to deploying NATO force elements.

2-12. Intelligence officers are able to undertake the Threat Assessment (TA) at the same time that FP specialists work on the initial phases of the planning process. This is important as analysing the complex inter-relationships and history between conflicting parties needs concentration and time. Understanding the social-political background is laborious but important to ensure that simple procedures of dealing with local civilians and security forces can be managed with a reasonable

AD 80-25

expectation of what can be achieved, and how deploying forces can maintain credibility in the eyes of the HN.

2-13. Examples include active insurgent groups undermining the HN government by attacking the infrastructure. Insurgents may want to reduce the confidence people have in the government's ability to control in an attempt to promote an opposing political party. It is important to recognise this dimension in addition to the superficial level of IED and IDF attacks and place everything in context, because it may be better to improve cooperation with the HN security forces to achieve the long-term and mutually beneficial goals.

2-14. **Counter Intelligence (CI).** CI is a separate and distinct discipline that supports commanders and other operational intelligence activities. CI cannot be ignored until the onset of an operation since potential adversaries may seek to obtain information prior to escalation. Similarly terrorist organizations may seek to target military assets at any time, whether they are deployed on operations or not. CI also helps to determine the ability and willingness of the HN to protect NATO forces, thus ensuring that the FP capabilities are fully integrated. To be fully effective, CI activities must be closely co-ordinated with, and complement, operational intelligence activities conducted by other CJ2 staff, and be included early in the planning phases for all training, exercises and operations. CI activities must also be closely linked to the civil authorities for co-ordination and information-sharing.

2-15. **Quantifying Risk.** There is a system to objectively assess risk during the TA phase by using a Balanced Scoreboard. Details have been included in the Threat-Capability Matrix (Annex E) to demonstrate this objective process in more detail and what 'scores' could be used. It is surprising how using such a system at this stage of planning can help prioritise FP measures and assess where weaknesses exist. This work directly benefits the writing of the CONOPs later in the planning stage.

2-16. The final point to be made in this part is the ability to have a Major Incident Plan (MIP) to meet the need for CM. More detail on CM is given later, but really understanding the threat allows a MIP / CM to be established so as to regain control after any situation, whether an emergency has arisen due to an adversary, nature or accident. Some CM principles have been given at Annex C.

ALLIANCE FORCES

2-17. By this stage of the planning, COAs will become more obvious as most of the information regarding the operating environment has been assessed. The final information requirement is what and how Alliance forces can undertake FP operations. This can be thought of in 3 ways: firstly, what specific FP forces will be available; secondly, what other forces can support; and thirdly, what other forces can be supported. The diagram below illustrates the many FP assets that require coordinating at an operational or tactical level.

AD 80-25



2-18. Operational Considerations

- a. **Theatre FP Officer.** The role of the theatre FP staff is to ensure facilities / installations have the necessary capabilities in terms of manning, resources and authority needed to undertake their commitments. This will involve conducting Vulnerability Assessments (covered in more detail later) to help identify and resolve capability gaps. Another serious consideration of this staff will be to ensure effective W&R or the flow of information between units / regions in order to balance collective needs and the developing operational situation.
- b. **FP C2.** International operations mean there will be a variety of perceptions about who should and should not control certain assets. Assessing a unit's MIP is the best way to demonstrate the importance of having a C2 element to ensure cohesion of FP assets. Establishing FP C2, no matter how complex the unit, ensures the commander can focus on their primary mission safe in the knowledge that incidents will either be prevented or dealt with effectively and efficiently.
- c. **Integration.** Being familiar with the other assets in theatre allows FP staff to be proactive in integrating themselves into the wider operation. For example, movement around theatre can be solved by having an existing working relationship with the right people in the Air Operations Planning Group. ISTAR assets can be requested, or better working relationships made with air casualty evacuation units. Additionally, good integration with the intelligence community can be established. FP staff should not wait until the real emergency comes before they discover how they can obtain additional support.
Good FP requires prior planning and tactical working relationships.

AD 80-25

2-18. **Tactical Considerations.** On the tactical level, FP staff should try to achieve centralised control over specialist-FP sub-units. The Threat-Capability Matrix at Annex E covers what forces could be used for certain roles. More detail on tactical FP operations is given in CONOPs development.

FOCUS AREAS

2-19. It is not possible to categorize conflict as it constantly evolves; therefore, blindly following criteria can hinder free thinking and initiative. That said, some descriptions are offered below to stimulate thought and encourage a 'mix-and-match' use. A quick scan of the following will assist in identifying the detail of defence that opposing forces seek to exploit. A full list of references of each category is at Annex A.

- a. **Emerging Military Engineering Technologies.** Standing HQs should be responsible for continually monitoring evolving MilEng technology to ensure the optimal level of protection to NATO infrastructure is delivered with value for money. This aspect is vital as a significant element of FP is about passive protection measures and resisting the evolving asymmetric attacks.
- b. **C-IED.** C-IED is defined as the collective efforts at all levels to defeat the IED system in order to reduce or eliminate the effects of all forms of IEDs used against friendly forces and non-combatants. Successful C-IED operations prevent the adversary from using one of his most potent weapon systems and thus allow freedom of action and manoeuvre for the NATO force and facilitate achievement of the operational or campaign objectives. It must not be planned or executed in isolation; C-IED activities are cross-functional and must be an integrated part of overall operations and remain a key consideration in respect to FP. A useful list of C-IED defeat activities that has utility for FP has been included at Annex G while more comprehensive explanations can be found in the C-IED doctrine (AJP 3.15) and training standards STANAG 2253.
- c. **FP Measures.** The AD 70-1 (Directive for Security) contains all security requirements and is very useful. Applying the measures stipulated in the 70-1 is the role of experienced police staff; this also allows the FP commander to concentrate on planning and integrating other FP capabilities. The AD 70-1 also contains pre-agreed definitions for Alert States, Dress Codes, Weapons Codes, CBRN Threat Levels, and Vehicle Movement Codes. However an example of these has been included at Annex H.
- d. **Entry Control Points (ECP).** An ECP can be a soft target as they are choke points for all civilian and military traffic and can be heavily manned. Without good ECP procedures (reliance must be on procedures not just equipment), or if one is destroyed, supply limitations can affect primary operations and ultimately Alliance FOM. Annex I defines the layout and FP

AD 80-25

Engineering considerations for ECPs, giving broad technical details for construction and operation.

e. **Force Escalation.** As well as ECPs, Alliance Check Points (CP) and convoys also present vulnerable targets. But there is more to consider. Recent operational statistics show that preventable deaths occur due to unclear Force Escalation (FE) procedures at these points and on convoys. This is a serious impediment to mission success as opposing forces can easily capitalise from accidental deaths with propaganda. Annex K contains some FE and CP ideas.

f. **Tactical Landing Zones (TLZ).** Air Transport (AT) is an essential capability and force multiplier in large theatres of operations. AT offers FOM and the ability to react to threats by redeploying assets as required, thereby reducing the overall demand for troops. Therefore, maintaining the integrity of TLZs is an operational-level requirement. Proven TLZ advice can be found at Annex L.

g. **Counter Surface-to-Air Missile (SAM) Operations.** Annex N has been included to show the principles of FP and highlight the essential considerations needed to protect air assets from this Surface to Air Fire (SAFIRE). The importance of AT and TLZs has already been covered, but considering most Alliance permanent operating areas will have some form of airstrip, SAFIRE operations should be seen as a natural extension to other FP operations.

h. **Force Health Protection - Health & Safety (H&S).** It is not unusual for more casualties to result from injuries and illnesses due to unhealthy or unsafe working environments than from active operations. Numerous occupational health and safety risks are present in the operating environment such as exposure to hazardous levels of noise, chemical vapour/fume inhalation, excessive dust inhalation, eye impact injuries, and other unsafe working environment risks. Simple but effective Force Health Protection H & S guidelines are given at Annex M.

i. **Fire Prevention.** While Fire Safety in regards to Burn injury prevention does fall under the auspices of FHP-Occupational Health and Safety, prevention of fire does not. When it comes to fire prevention equal concern regarding this effort is also directed towards the protection of valuable property, supplies, and other material assets.

j. **COIN.** Counter Insurgency (COIN) includes those military, paramilitary, political, economic, psychological and civic actions taken by the government to defeat an insurgency. COIN involves an offensive approach and makes use of all elements of national power, and it can take place across the range of operations and spectrum of conflict. COIN operations include:

AD 80-25

- (1) Strategic and operational planning, and FP needs to be involved as FP troops tend to be concentrated in and around the operational and strategic centres of Alliance activity, and these are often in very close proximity to important centres of the civilian population.
- (2) Intelligence development and analysis. FP should already be deeply integrated into the intelligence infrastructure given the value of the locations often defended.
- (3) Training and advice. Low-level cooperation is possible through liaison between HN security forces and the FP troops. This would also form part of the military-civil liaison to add a layer of defence and eventual transition of lead security responsibility (as required).
- (4) Materiel, technical and organizational assistance.
- (5) Infrastructure development. To ensure this is properly focused, the understanding of the TAOR by the FP patrols can help support the higher-level picture driving tactical projects such as CIMIC, PHSYOPS, etc.

k. **Coordination with Host Nation Civil & Military Authorities.**

Sovereignty issues are very thorny and can demand a great deal of the commander's time in order to resolve them. However, they form the bedrock of what is and is not achievable. Such issues may also be used against Alliance forces to gain political capital when they are not observed. Some examples of sovereignty issues include:

- (1) Collecting and sharing information. This means when, who, where and how information is exchange and plans of action agreed upon.
- (2) Basing and access routes. This is of particular note when considering the ground immediately outside bases when modifications are required and patrolling conducted.
- (3) Over-flight rights.
- (4) Use of airports, harbours and the rail network.
- (5) Border crossings.
- (6) Force Protection – as covered in detail throughout this entire publication!

AD 80-25

- (7) Jurisdiction of NATO members (by HN and by other NATO members e.g. by International Military Police).
- (8) ROE, powers to stop, search, arrest, detain and hand over of civilians & captured opposing forces to the civilian powers.
- (9) Operations / jurisdiction within and outside of territorial waters.

l. **Anti- & Counter-Terrorism.** Anti-terrorism is the use of defensive measures to reduce the vulnerability of forces, individuals and property to terrorism, to include the limited response and containment by military forces and civilian agencies.

There may be risks to the general safety of personnel, exposed parts / nodes of mission essential services (logistics, gas, electric, water, communications, etc), destruction of infrastructure / property, attacks against forces actually executing the mission, attempts to disrupt physical FOM (e.g. IEDs) or political FOM (e.g. hostile Information Operations), as well as attempts to divert or degrade the effort of the deployed force by forcing them to increase their security posture.

There is no substitute for common sense. Attacks can be by any means, but of particular note are asymmetric methods such as IEDs, IDF and CBRN weapons/devices including TIM (Toxic Industrial Materials). **The only way to truly counter any threat is to dominate the TAOR and ensure all defensive measures are centrally controlled in order to establish unity of command, mutual support, depth and ultimately economy of scale.** Relegating FP to an afterthought is risking strategic consequences due to the vulnerability of some deployed sites and the sensitivity of TCNs to loss of life.

m. **Lessons Identified.** Learning the lessons from history allows us the avoid making the same mistakes as before. Lessons are not learnt until they have been actively incorporated into the new plan; until that point they are only identified. Lessons Identified provide a ready-made 'Capability Gap Analysis' for new staff.

n. **Long-term / Strategic Plan.** FP planning should be made with time in mind. The duration of the mission will then drive the need to enhance FP measures, especially costly engineering projects, installing sensors and fusing data to an Operations Centre which all involve contractors, time and money. Taking a long-term view will ensure any adaptations will all contribute the long-term benefit and eventually reduce the overall costs.

o. **Continuity.** Maintaining a detailed file of contact information, background information and decision making will ensure that on unit hand-over, information

AD 80-25

– or more importantly ‘knowledge’ – will not be lost. Building a well structured file of information during the mission analysis and reconnaissance phases ensures better transition of authority when units undertake their rotations.

p. **Command Relationships.** Building a ‘Continuity of Operations Information File’ as described above ensures that before, during and after deployment, units are able to develop relationships with others who can enhance or support the FP mission. Units should have a ‘who’s who’ list of involved forces and influential members of the local populace.

q. **Training.** The mission will drive the training, and necessary training objectives can be developed from currently deployed units of on a pre-deployment reconnaissance mission.

r. **Reconnaissance.** Time spent on reconnaissance is never wasted. Visiting the actual deployment location ensures theories are developed into realistic TTPs. Nothing should be left to chance or assumed.

s. **Evolution of the Battle-space.** Opposing forces will evolve their TTPs and so must Alliance units. A system for reviewing TTPs must be established in the planning stage. This can be achieved by identifying individuals to monitor the effectiveness of Alliance versus opposing forces’ TTPs, secure regular periods for in-theatre or on-the-job-training, and maintain Knowledge Management systems (even if this is only a database of Lessons Identified).

CONOPs DEVELOPMENT

2-20. At this stage, all information regarding the operating environment, opposing forces and Alliance forces should be well understood. Deductions and tasks should have been made about relevant aspects of the operations and these effectively form the CONOPs. Therefore, this final stage of planning means pulling together the ideas and work highlighted earlier. Following the principles below will ensure the resultant CONOPs / FP plan and Layered Defence Plan (examples are at Annexes J and O respectively) are meaningful and focused. Some ideas to help develop the CONOPs are given below:

a. **Effects Based Thinking.** Sometimes, there are no right or wrong ways of doing business; rather what matters is achieving the desired effects. For FP it is about clarifying the desired effects. Perhaps this will be to deter activity by an adversary, in which case FP operations will be about high visibility, Information Operations and cooperation with HN security forces.

b. Controlling access into or around the location may be one desired effect. This then leads onto the need for controlling or recognising possible threats moving outside a perimeter area, and of course COE onto the location itself.

AD 80-25

This leads onto searching and vetting issues not to mention engineering and ergonomic aspects about gate designs, which all require a lot of work to implement effectively. Essentially, effects based thinking is about identifying **Ends, Ways and Means** – or what is to be achieved, how it may be achieved and with which resources.

c. For example, a desired effect may be to prevent attacks or mitigate the effects of an attack (ends). There may be little stand-off distance between working areas and possible attack locations, so effective methods could be cooperation with HN security forces to deter and disrupt opposing forces' operations or construct suitable barriers (ways). These requirements would necessitate a need for patrolling, HN integration and / or construction (means).

d. **Prioritisation & Risk Mitigation.** The possible threats and how they could manifest themselves needs prioritising and listing in a risk register of sorts, such as the Threat-Capability Matrix at Annex E. Each identifiable threat needs a mitigating solution including in the register along with the required enabling tasks / resources / manpower. It then becomes possible to prioritise the tasks and allocate the available manpower or resources. Any threats with little or no available mitigating resources can be identified as a **capability gap**. The commander whose responsibility it is to provide such resources should sign off these risks as 'accepted', whilst plans to solve the shortfalls are developed. This is risk transfer.

e. **Consequence Management (CM).** While it is not realistic to prevent all threats all of the time, CM plans may be the only way to mitigate the less likely or resource hungry threats. CM plans would state how resources would be re-allocated in the face of emerging or changing threats. The risk register can be helpful in this situation by clarifying the priorities for FP and where finite resources / manpower are already focused. There will always be a chance of a rapid and serious escalation focused on low priority vulnerabilities that have few mitigating measures, but this is **risk management**.

f. **Centres of Gravity.** Attention must be given to political, military and economic Centres of Gravity (COG) and Lines of Communication (LOC). These may be viewed as **tangible** as well as other examples like HQs, concentration areas and logistics / CIS nodes, Main Supply Routes (MRS). **Intangible** aspects include Alliance cohesion and political will as influenced by public opinion. Similarly, potential targets of media or political significance to terrorists must also be considered.

g. **Mutual Support.** Mutual Support means establishing how one capability / unit / location is able to support another. This is achieved through C2 from which an overview can be formed about overlaps or seams in capability, the

AD 80-25

total capacity for each capability and what the priorities are. Working smart in this respect can help reduce numbers of deployed manpower and provide a much more integrated protective posture.

h. **Depth.** Providing a layered defence, see Annex O for an example, means coordinating the efforts of different capabilities to ensure any attempt to affect Alliance forces has to negotiate several obstacles. In essence, depth provides a filtering concept. An adversary should have to outwit patrolling units in the TAOR, surveillance devices, perimeter guards and fence-lines, and access control on classified working areas. Health can be protected by depth of measures such as education in limiting the spread of disease, healthy lifestyle, water and food security (including the vetting of sources), as well as medical professionals. Depth can drain the energy from an adversary's attack and increase the likelihood of stopping potential infiltration or being influenced by a problem.

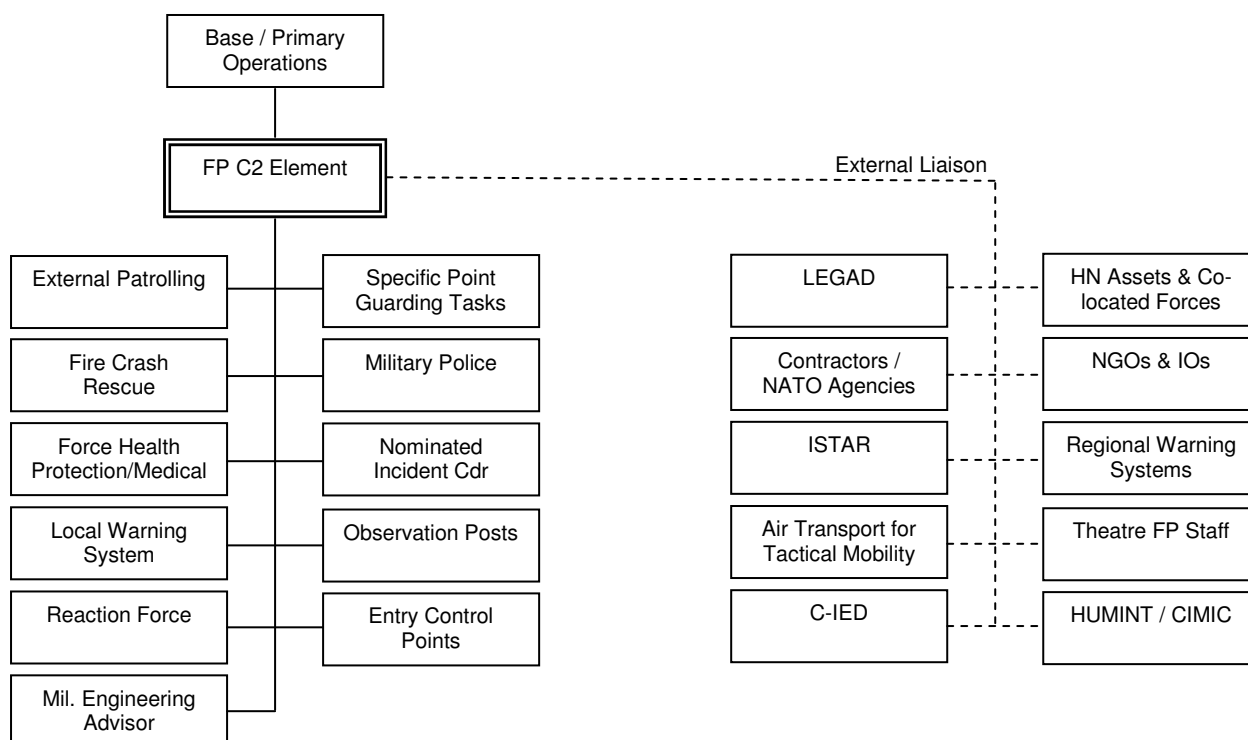
i. **Flexibility.** Understanding the individual and combined capacity of the different capability areas allows FP staff to meet changes in demand as they arise. A location's tactical Reaction Force (RF) may also be used as a rest period for troops. The RF may also be used to provide the Incident Commander (IC) during an emergency. Point defence guards deployed to protect only national assets could be re-mustered as a more complete security force that could have mutual benefits.

j. **Reserve.** Reserve goes hand-in-hand with **flexibility** as they achieve similar effects. Knowing where extra resources or troops will be mustered from in case of an emergency is a pre-requisite to successful CM. Some examples of the considerations needed include: how big the RF is, where the operational-level Quick Reaction Force (QRF) is located and how easy or long it takes to deploy them, and whether or not base personnel can be mustered into useful groups, for example for Post Attack Recovery (PAR). Making assumptions about this information is dangerous.

k. **Command and Control.** FP cannot function without complete C2 of its related assets. Authority is needed from the local, higher commander for FP to establish CIS and cohesion of FP functions. A tactical FP C2 example is given below:

AD 80-25

Diagram 4 – Example FP C2 Structure



2-21. **Example Annexes J & U.** A theatre-wide FP plan will obviously be different from that of a single base, but the planning process and headings are the same. The content of this document may seem very doctrinal, but it has been tested and proven to work in practice. Ultimately, the FP process leads to effective and complete FP Plans or the theatre-level plan known as Annex J, and Annex U for CBRN. Examples of these documents are at Annex J and U respectively.

REVIEW

2-22. **Assessment.** A great deal of effort is required in the planning phase, and more so when implementing plans; however, it is not possible to complete such work because the situation always changes. During recent Alliance operations, opposing forces have adapted their TTPs to exploit weaknesses. The planning process should be reviewed regularly.

AD 80-25

2-23. **Quality Control.** There are several methods within NATO for quality control and oversight.

- a. **Vulnerability Assessments (VAs).** SHAPE-directed VAs must be conducted to ensure that deployed units have plans that are relevant to the current situation. Annex P has been written to provide some helpful advice for conducting VAs. Annex P outlines some considerations for VAs, and Annexes D and E provide good templates for assessing current FP dispositions.
- b. **FP Advisory Team (FPAT).** Deployed operational-level teams can be formed from across Standing HQs in order to gain situational awareness on specific issues and ongoing projects. These are necessary to ensure long-term continuity, adjustments to ongoing projects and integration with higher-level plans.
- c. **Coordination.** A set rhythm is needed to coordinate the activity in-theatre FP elements and Standing HQs. FP activities should focus on creating **deliverables** and **decisions** that are aligned with operational / regional commanders and Standing HQ timelines. The latter would be driven mainly by procurement, force generation and budgeting processes.
- d. **Video Tele-Conference (VTC).** VTCs enable real-time coordination between the different levels of command / control. Issues can be identified and assigned to an Office of Primary Responsibility (OPR) without the impact of travelling time.

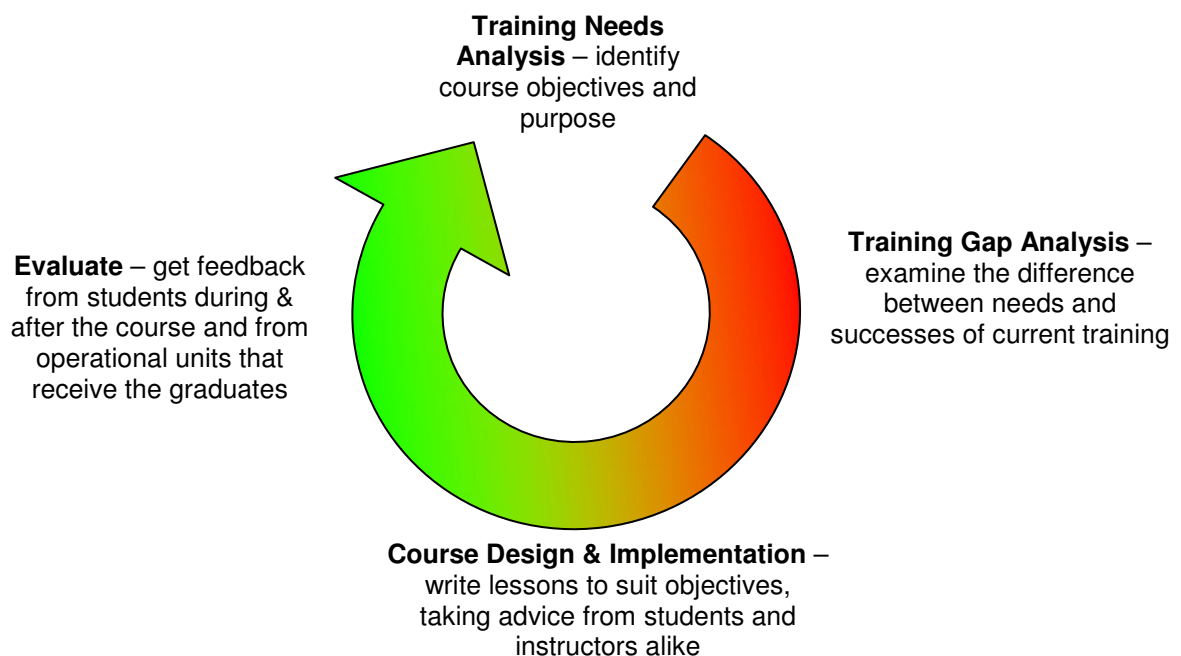
2-24. **Knowledge Management.** It is necessary for deployed units to maintain a journal of Lessons Identified for incoming units and for NATO HQs so past successes can be build upon. Failure to do this, in whatever format, means deployed units can waste almost half their time learning the same lessons rather than making progress.

2-25. **Training.** The quality of training is proportional to quality on operations. It is vital for the longevity of a military organisation to have a training system that can evolve. By building in a 'feedback loop' into the training system allows the effects of TTPs and doctrine to be re-invested in individuals undergoing initial, continuation or specialist training. A simple training system is described below in Diagram 9.

AD 80-25

2-26. Training standards have been produced and included at Annex Q.

Diagram 9 – Systems Approach to Training



NATO RESTRICTED
Releasable to PfP

AD 80-25

ANNEX A TO
AD 80-25
DATED 14 MAY 09

RELEVANT NATO FP DOCUMENTATION

Sub-Capability	Document
General	
Strategic NATO FP Doctrine	AJP-3.14
Logistics Support	MC 319-1 AJP-4
Command & Control	
Battlespace Management	AFP 1 STANAG 2029
Information Operations	MCs 348, 368, MC 422/1/1 CM (2002)49
Intelligence	MCs 128, 161, MC 165, MC 166 AJP 2-1
METOC	AWP 1-5 AJP3.11 ATP32(C)
Security	
Electronic Warfare	MC 64-8
Counter-Intelligence	MCs 161, MC 165, MC 166 AJP 2-2 AD 65-3
General / Operational / Physical / Personnel / Information Security	CM (2002)49 AD 70-1 MC 362/1 NATO Rules of Engagement
Terrorism Defence	MC 472 AD 65-2 (Bi-SC Military Concept for the Defence Against Terrorism) CM (2002)50 AD 70-1
Anti-Torpedo Defence	ATP-1(D) ATP-18(D) ATP-28
Maritime	ATP-1(D) ATP-6(C) Vol I ATP-6(B) Vol II ATP-24(C) Vols I & II
Military Engineering	
Military Engineering	MC 0560 "MC Policy for Military Engineering" AJP 3.12(A) "Allied Joint Doctrine For Engineer Support To Joint Operations" ATP-52 (B) Land Force Combat Engineer Doctrine
Deception, Security and Protection	ATP-52(A) STANAG 2280
Airfield Damage Repair	AD 80-15 ATP-52 (A) STANAG 2929
Health Protection	
Environmental Health	AJP 4.10
Casualty Care	MC 326 AD 85-5 Hague Convention – 1907 Geneva Convention -1949 STANAGs 2037, 2461, 2462, 2463, 2475, 2476, 2477,

A-1

Releasable to PfP
NATO RESTRICTED

NATO RESTRICTED
Releasable to PfP

AD 80-25

Sub-Capability	Document
	2478, 2874, 2479, 2480, 2500, 2908, 2910, 7141, 2122, 2126, 2127, 2132, 2342, 2347, 2358, 2871, 2873, 2879, 2917, 2931, 2954.
Consequence Management	
Fire-Fighting	STANAG 3929
Explosive Ordnance Recce / Disposal	STANAGs 2143, 2221, 2370, 2377, 2389, 2929, 2897 AJP 3.12 (A) (STANAG 2238) ATP 52(B) (STANAG 2394) ATP 72 (STANAG 2282)
Counter-IED	
Air Defence	
TMD	MCM-039-097 STANAG 6432
Ground-Based Air Defence	MC 5417 (Rev)
Fighter Air Defence	MC 54-1 (Rev)
Maritime Air Defence	ATP-1(D) TASMO Guide, AJP 3.3.3
CBRN	
Individual & Collective Protection NBC Reconnaissance/Survey Decontamination Warning & Reporting	ATP-59 AJP-3.8 ATP45-C AEPs 4, 7, 10, 14, 18, 19, 20, 21, 22, 25, 41, 49, 57 STANAGs 2150, 2352, 2871, 2954, 4145, 4192, 4328, 4359, 4447, 4510, 4511, 4521, 4524, 4548, 4571, 4590, 4475
Funding & Force Generation	
CRO Urgent Requirements (CUR)	Bi-SC 85-1 Capability Package Directive Bi-SC 60-70 Procurement Directive Revised Funding Policy For Non-Article 5 NATO-Led Operations, PO(2005)098 Revised Funding Arrangements for ISAF, dated 25 Jul 06 Guidance on NSIP Funded Infrastructure and CIS Projects on CRO, 06 Feb 03 COFS SHAPE Letters on Parallel Staffing (DEC 06), Establishment of Capability Management Directorate (CMD, Apr and May 07)

NATO FP POSTS AND RESPONSIBILITIES

The cooperation between NATO FP Officer (FPO) and deployed units can help reduce the tension created from different priorities, perceptions, expectations and tempo. A table of NATO FP positions and their respective responsibilities is given below. FP in NATO is led by the FPO at SHAPE. In turn, FPOs and their teams from the Standing HQs¹ such as Joint Force Commands (JFC) as well as from the Component Commands (CC) and many other HQs work together, as much as is practicable, as a community. Some posts may be gapped at one level and well supported at another, so it is vital the community work together to routinely support operations, exercises, and NATO School (Oberammergau) courses. Additionally, FPOs can serve in a consultancy role to member nations as requested. The FPOs can also help establish contact with Subject Matter Experts (SMEs) from other capabilities areas within their HQs such as CBRN, Fire Fighting, C-IED, medical, Environmental Health, etc., depending on the individual HQ's PE structure.

Contacting any FPO within NATO before deploying on operations will give the unit a real advantage in solving manning or equipment problems that may arise or be ongoing.

¹ These HQs are manned with a Peacetime Establishment and are located throughout member nations.

NATO RESTRICTED
Releasable to PfP

AD 80-25

STRATEGIC ----->OPERATIONAL----->TACTICAL----->					
	SHAPE	JFC	CCs	Theatre/Regional Commander	APOD/DOB/FSB/PRT
Force Generation (personnel, materiel, facilities)	Standardize FP across all operational theatres and align procedures with strategic guidance.	Standardize theatre FP requirements and align them with future operational requirements	Support, evaluation, and training	Apply requirements in theatre as required	Identify and submit requirements
	Crisis Management Resource Board (CMRB) for approving CRO Urgent Requirements (CUR)	Crisis Requirements Coordination Board (CRCB) for CUR		Initial Operational Requirements Review Board (IORRB) for CUR	Generate CUR
	CE/CJSOR Final Approval	Review CE/CJSOR and submit changes to SHAPE	Provide assistance to operations such as deployable CAOCs / fill CE posts	Ensure changes are realistic and reflect CONOPs, then direct forces to fill requirement or submit request for more forces	Generate CE/CJSOR requests
	Approve and forward Minimum Military Requirements (MMR) to NATO HQ	Develop and submit MMRs to SHAPE	Recommend MMRs based from operational experience	Advise on MMRs	Request MMRs
Training	Coordinate with SACT	Steadfast Joist Series of Exercises	Expeditionary Training Exercises	Theatre training plans	Exercise SOPs & Plans
	Arrange FP Situational Awareness training for Key Leaders	Develop staff training such as NATO FP Courses and pre-deployment seminars	Provide operational FP specific training for Troop Contributing Nations (TCN)	In-theatre FP WG	Attend FP WG
	Conduct ACO Force Protection WG with JFCs		Conduct assessments		
Doctrine	OPR and final approval for AD80-25	Develop and coordinate suggested changes to ACOs and AJPs		Produce theatre OPLAN, CONOPs & SOPs iaw higher D&G	Produce local SOPs, FP Plan, CONOPs iaw higher D&G
	Forward AJP change recommendations to SACT	Adjust OPLAN	Identify doctrine shortfalls	Link requirements to AJP/AD	Promulgate effective TTPs, SOPs, procedures, etc.
Organization	Integrate with subordinate HQs	Integrate with SHAPE, CCs, and own staff	Coordinate with JFC and in-theater staff	Integrate with JFC and CC FP Staff	Integrate with Theatre FP and JFC FP
	Ensure unity of effort for FP staff work across subordinate HQs	Delegate authority for tasks and missions such as VAs & OPR-ship	Undertake tasks set by higher HQ	Establish and practice clear C2 and communications	Practice communications with Theatre FP
	Produce OPLANS	Produce OPORDs and Op Directives		EXORD/FRAGO	Provide feedback on EXORD/FRAGO

NATO RESTRICTED
Releasable to PfP

AD 80-25

B-3
Releasable to PfP
NATO RESTRICTED

COMMON PRINCIPLES OF INCIDENT MANAGEMENT

1. The ability for any unit to recover from an attack or incident needs to be described in a plan, and the plan must be rehearsed so that it is familiar in peoples' minds as well proven to work. Emergency management plans must be easy to remember when under pressure and therefore they should follow basic principles. This also allows for the flexibility to adapt depending on the scale of the incident.
2. Once a plan has been written, it must be run through as a table-top exercise, refined, then rehearsed to ensure it is workable. In locations with a high turn over of personnel, plans may well need rehearsing regularly otherwise in the event of a 'spectacular' terrorist attack or large scale incident there would be a needless loss of life due to delayed decision making and confusion when allocating resources or manpower. This message is the result of experience!
3. **Command.** Command has 2 levels:
 - a. An **Incident Commander (IC)** should be someone who fills an on-shift post so they can be immediately deployed to the scene of the incident in order to confirm what has occurred, gather information for the Operations Centre and establish local control. At the onset of any disaster / incident, there will be confusion and many unknowns so the IC must travel to the scene very quickly and clarifying the situation. This is vital to enable effective decision making. The IC should not be someone who will be drawn into hands-on treatment of personnel or equipment such as a fire or medical personnel – the IC must be able to focus on the larger picture.
 - b. The **Operations Commander (OC)** is someone who has control of base operations and can divert or mobilise extra / specialist personnel and resources to deal with the incident as required, which would be based on the information and direction from the IC. They should be located at the Operations Centre and allow the IC to deal with the minute-to-minute detail.
4. **The 4 Cs**
 - a. **Confirm.** The IC can confirm to the Operations Centre what has occurred by talking with personnel from the incident location. Confirmation of the incident will allow the Operations Centre to mobilise the right numbers / type of personnel and resources to manage the emergency.
 - b. **Clear.** The IC should use personnel in their vicinity to clear the area so as to limit further risks to personnel. It helps greatly to have a set procedure to clear working areas on hearing alarms signals. Using fire evacuation procedures is a good method of establishing one, clear procedure for any incident - all personnel will evacuate and be accounted for. Additionally,

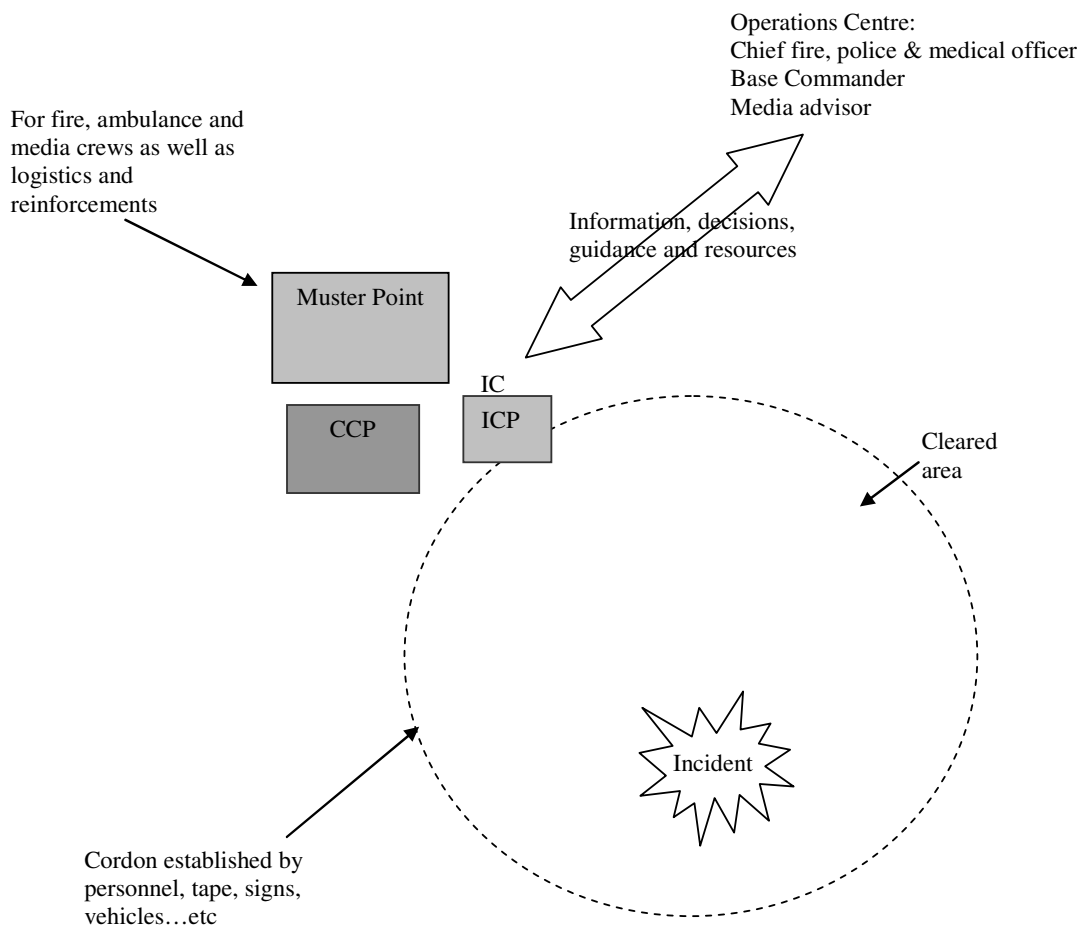
AD 80-25

knowing where personnel will meet allows the IC to access pools of manpower almost instantly for cordon or first responder duties. On deployed, austere bases, a warning, reporting and alarm system is very important, and if it does not exist, the CUR process should be used to obtain one. One way of improvising would be to use air horns or loud hailers – effective systems were developed during World War II without the reliance on technology to provide a system.

c. **Cordon.** The IC will need evacuated personnel to establish a cordon in order to keep an area clear. Equipment such as high-visibility signs / vests, tape and radios are highly recommended in order to maintain the cordon boundary and keep information flowing between cordon personnel and the IC. On aircraft crashes, cordons may remain in place for days, so food / water and protection from the weather are worthy considerations.

d. **Control.** The flow of information needs maintaining between cordon personnel, the IC and the Operations Centre. Additionally, the IC must establish an **Incident Control Point (ICP)** where all personnel and support (fire teams, medical teams, reinforcements, logistics support, etc.) can report to ensure all effort is centrally coordinated. All casualties should be brought to this point to form the **Casualty Collection Point (CCP)**, ensuring rapid prioritisation, treatment and evacuation of personnel.

Diagram 5 – Major Incident Control



C-2

FP PLANNING TEMPLATE

1 - Over type with relevant information

2 - Fill out the deductions

3 - Group deductions at end to give CONOPs

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
1	<p>INITIATION & MISSION ANALYSIS</p> <p>Orientation</p> <p>Mission</p> <p>Intent, End State & Main Effort</p> <p>Specified Tasks</p> <p>Implied Tasks</p>	<p>- The information required below can be obtained from SHAPE's OPLAN or JFC's OPORD.</p> <p>- What are the local political and social situations? In what ways will these situations positively and/or negatively influence the unit's ability to achieve its mission?</p> <p>- What are the implications of the Status of Forces Agreement (SOFA), and Memorandum of Understanding (MOU)?</p> <p>- What is the latest information from CJ2?</p> <p>- What is the mission statement and what deductions about the tasks and objectives can be made from it?</p> <p>- What is the superior commander's desired End State and Main Effort? What measures can support this? What shortfalls are there between the specified tasks and the required capability?</p> <p>- What are the specified tasks and what are the reasons behind them? What effects need to be achieved and how can they be reached?</p> <p>- What supporting tasks will enable the specified tasks and mission, and what are the effects of these? What will that mean to your Main Effort/Centre of Gravity (COG) – in other words</p>	

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
		what single factor will enable or halt their operations?	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
2	<p>CONSTRAINTS</p> <p>Time</p> <p>Space</p> <p>CSS</p> <p>Personnel</p> <p>Legal</p>	<p>- What are the deployment times? - What are the selected/necessary decision points that will trigger the deployment of local or higher-echelon Reaction Forces/Quick Reaction Forces (RF/QRF)? How long does it take to generate the RF/QRF and how long does it take for them to move to areas in the Tactical Area of Responsibility (TAOR)? - What is the commander's battle rhythm?</p> <p>- Where are you able/not able to operate? What geographical controls can be imposed in the TAOR? - What are the Friendly Forces vs. OPFOR weapon ranges? - Where are the probably stand-off attack launch sites? - What ability does the unit have to dominate the ground?</p> <p>- How reliable is the supply/logistics element? - What transportation is there? - What engineering/armoury support is there (including contractual support to specialist systems such as CCTV/sensors, etc)? - Are there weapons and ammunition storage locations? - What standard is the accommodation and food?</p> <p>- How many personnel are there and can all tasks be undertaken? What capability gaps are there as result?</p> <p>- What are the ROE/arrest, stop, search & detention procedures? - What differences exist between the Contributing Nations' (CNs) ROEs? - What are force escalation principles and training procedures?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
3	<p>NATURAL ENVIRONMENT</p> <p>Ground/terrain</p> <p>Climate</p> <p>Flora/Fauna</p> <p>Discipline</p>	<p>- What are the effects of the terrain, including: radio dead-spots, dead-ground, easy going terrain, flood plains, weapons launch sites (for MANPADS, mortars, rifles, rockets), good observation points?</p> <p>- What should be identified as Vital Ground, Key Terrain, Vulnerable Points and Key Points?</p> <p>- What are the reaction times to each?</p> <p>- How can the defence be structured around priority ground / assets?</p> <p>- What are the effects of the climate on: work rates, heat stress/cold injuries?</p> <p>- Is water or treatment readily available for casualties?</p> <p>- What is the disease prevalence?</p> <p>- What type of wild-life is there that may prove directly hazardous to people, and what animal may serve as vectors for disease? What can be done to mitigate these effects?</p> <p>- What measures can be put in place to reduce the probability that a road accident, disease or injury can occur from undisciplined behaviour?</p> <p>- What can be done to ensure the Health & Safety / Occupational Health plans are followed?</p> <p>- What are the risks to mission success by poor discipline?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
4	<p>NON-COALITION</p> <p>Composition</p> <p>Objectives</p> <p>Tactics & Equipment</p> <p>Ends, Ways & Means</p> <p>Intent & Capability</p> <p>Strengths</p> <p>Likely COAs</p> <p>Most Dangerous COA</p>	<p>- Who fights for OPFOR and who might support them? What is their training and experience?</p> <p>- What are the OPFOR objectives, What is the effect they want to achieve on coalition forces? What is their overall aim?</p> <p>- What are the OPFOR tactics and equipment and how experienced are they in using them? - What training do they receive? - How committed are they to achieving their aims and employing extraordinary methods?</p> <p>- What has the unit established as the ends / results that non-coalition forces want to achieve at tactical, operational and strategic levels? - What has the unit considered as the ways / techniques that non-coalition forces can employ in order to influence operations on the tactical, operational and strategic levels? - What has the unit identified as the available means / resources with which they can achieve their objectives?</p> <p>- What capabilities do non-coalition forces have, and what is the intent to use them based on historical data / statistics? - What is the probability of certain events occurring or the impact on the mission success?</p> <p>- What advantages can non-coalition forces exploit? - What are the coalition weaknesses?</p> <p>- What tactics are non-coalition forces likely to use and what equipment / manpower / intent do they have to employ them in a strategy against coalition forces?</p> <p>What is the most dangerous COA that coalition forces could pursue that would have the most significant effect on coalition operations and ultimately on mission?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
5	<p>COALITION</p> <p>Composition</p> <p>Tactics</p> <p>Strengths</p> <p>Training</p> <p>Equipment</p>	<p>- What units are nearby and what roles are they undertaking? How can they support, and integrate into the FP unit's operations in order to achieve the superior commander's mission?</p> <p>- How has the unit aimed to support or benefit from local infantry units, HUMINT teams, Information Operations teams, CIMIC teams, OMLT, ISR, AT, CASEVAC assets?</p> <p>- What tactics and equipment do the unit and the nearby units employ? How experienced are they in using them? What training do they receive?</p> <p>- What advantages can non-coalition forces exploit?</p> <p>- What are the unit's weaknesses?</p> <p>- Is it possible to rehearse and train all FP Plans involving all FP sub-units?</p> <p>- Can the base population, military and civilian, undergo rehearsals for emergency procedures? What can be implemented in terms of a theatre induction training package for new arrivals?</p> <p>- Can personnel be taught about the local civil environment such as culture, history, and customs? Where/how can the results & feedback be collected to improve the training?</p> <p>- What assets can support / enhance the FP mission?</p> <p>- What capability gaps are there and what assets can fill these gaps? What plans need writing to fill capability gaps and at what level do they need agreeing to make them effective?</p> <p>- What are the political constraints involving cooperation between nation's equipment?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
6	<p>COMMAND, CONTROL, INTELLIGENCE & INTEGRATION</p> <p>Authority</p> <p>Command Post</p> <p>Interoperability</p> <p>Intelligence</p> <p>Warning & Reporting (W&R)</p>	<p>- What are the command relationships between the FP sub-units? At what level does permission need agreeing for DIRLAUTH / TACON over FP assets such as Med, EOD, Police, Infantry & Fire Crash Rescue Services?</p> <p>- What local arrangements are required to ensure the control needed over FP units?</p> <p>- What can be done in order to liaise with sub-units to ensure effective unity of effort and trust?</p> <p>- What can be designed to ensure an ergonomically friendly command Post (CP) that allows control of emergency response units and focuses the liaison between units that contribute to FP?</p> <p>- What liaison mechanisms can be put in place between the FP unit and adjacent coalition forces, Non Government Organizations (NGO), International Organizations (IO), higher echelon, adjacent units and Host Nation (HN)?</p> <p>- What is the plan to coordinate the CONOPs, concepts, doctrine and procedures of other relevant units?</p> <p>- How can the unit integrate into the base's operation centre in order to make decisions that affect the overall mission?</p> <p>- How can intelligence be gathered and disseminated within the unit and within higher echelon/adjacent units? Who can gather intelligence from other sources and integrate this into the unit's FP plan? Who can conduct Counter Intelligence?</p> <p>- What W&R systems can be used?</p> <p>- How will messages be passed to higher command / adjacent units?</p> <p>- What local-level alarms will there be, how will they be initiated and linked to the FP C2?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
	Fratricide	<ul style="list-style-type: none">- What can be done to limit the risk of fratricide?- What can be done in terms of identification plans or weapons tight areas?	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
7	<p>SECURITY</p> <p>Plans and Programs</p> <p>Personnel Security</p> <p>Physical Security</p> <p>Operations Security</p> <p>Information Security</p> <p>Security Forces</p> <p>Camouflage, Concealment, Dispersal & Deception</p> <p>Civil Interference</p>	<p>- What unit security plans are required to ensure all security force and other personnel are fully aware of what their roles and responsibilities are?</p> <p>- How can access control be managed onto the base and into mission essential areas? - How can locally employed civilians be cleared and controlled?</p> <p>- How can mission essential areas of the base be protected with the correct levels of access control e.g. locks, combinations, card-readers or guards on doors? - Where will classified documents be stored and can access to them be controlled?</p> <p>- How well can the flow of classified information be controlled? - How effective are the normal procedures for safeguarding classified information? - What measures can be put in place to control the use of unclassified / unregistered personal electronic systems or mobile phones? - Is it possible to designate working areas for classified work?</p> <p>- What measures can be taken ensure mission sensitive and personal information is controlled, from maps to electronic data?</p> <p>- What security forces are needed? - Who will be responsible for prisoner handling, and how will prisoners dealt with?</p> <p>- How will camouflage, concealment, dispersal and deception be employed?</p> <p>- What measures can be put in place to deal with civil disturbances, riots, blockades, refugees, etc?</p>	

NATO RESTRICTED
 Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
	<p>Piracy & Banditry</p> <p>Kidnapping / Hijacking</p> <p>Sy Clearance</p>	<p>- What measures can be taken to mitigate the effects of crime, especially from piracy and banditry?</p> <p>- What can be done to avoid, transfer or mitigate against the risk to kidnapping or hijacking?</p> <p>- Will personnel, civilian and military, who require access to information classified CONFIDENTIAL or above vetted and briefed on their responsibilities?</p> <p>- Will there be systems in place to control personnel such as messengers, visitors and cleaning staff whose duties give inadvertent access to classified information?</p> <p>- How will records be held of these systems, checks and training?</p> <p>- What systems will there be to report incidents, associations or habits that are likely to have a bearing on the security reliability, or vulnerability, of personnel?</p> <p>- How can classified material be protected in an emergency situation, for example, in an evacuation?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
8	<p>FP Engineering</p> <p>Physical Protection</p> <p>Fire Protection</p> <p>EOD</p> <p>IED Disposal</p> <p>Explosive Threats & Hazards Awareness</p> <p>Damage Control & Repair / Airfield Damage Repair (ADR)</p>	<p>- What are the high-risk locations for attack? What will be done in terms of hardening existing buildings / facilities against the threat?</p> <p>- What is available in terms of blast protection?</p> <p>- Have the stand-off distances for the likely threat been calculated and adhered to?</p> <p>- Who will write the SOPs for Fire Prevention, Health & Safety, Environmental Health, and Hazardous Materials?</p> <p>- What is the EOD capability and what can be done to mitigate capability gaps, if they exist?</p> <p>- What is the IED Disposal capability and what can be done to mitigate capability gaps, if they exist? How can the IEDs be exploited for intelligence?</p> <p>- What measures can be taken to mitigate the risks associated with explosive hazards?</p> <p>- What capability will there be to undertake damage control and restore essential services?</p> <p>- What plans will be made to improve the restoration of services after an attack / incident?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
9	<p>HEALTH PROTECTION</p> <p>Environmental Health</p> <p>Medical</p> <p>Evacuation</p> <p>Safety</p> <p>Meteorological Protection</p>	<p>- What can be done on the camp in respect of preventative medicine, and to limit the effects of pollution, poor sanitation and climatic extremes (snow/ice, floods, hurricanes, tornados, forest fires, strong sun, dust and sand storms, etc)?</p> <p>- What are the risks from a tsunami or earthquake?</p> <p>- What acclimatization and vaccination programs against disease and biological weapons are needed?</p> <p>- Is there a need for a health education program as part of the unit induction training package?</p> <p>- What is the medical capacity and limitations thereof? How does this relate to the threat?</p> <p>- What measures are required to evacuate medical emergencies to better facilities, or when the base's medical capacity has been reached?</p> <p>- What will be in place to provide a Casualty Collection Point and will it be equipped / prepared for service?</p> <p>- What will be the hazards from industry and poor working conditions? What measures are in place to limit the risk of traffic accidents?</p> <p>- Who will write the SOPs for Fire Prevention, Health & Safety, Environmental Health, and Hazardous Materials?</p> <p>- How will the threat from the climate be published? What support / education is required to protect people against the effects of climate?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
10	<p>EMERGENCY MANAGEMENT</p> <p>Contingency Planning</p> <p>Emergency Response</p> <p>Recovery</p> <p>Civil-Military Response</p> <p>Public Information</p>	<p>- What are the identified gaps in the defensive measures / capability and what possible solutions can be implemented from other units?</p> <p>- What are the requirements of the Major Incident Plan?</p> <p>- How will these plans be written, tested, communicated and rehearsed?</p> <p>- Who will lead the emergency response to an incident? Where will be controlled from?</p> <p>- What has been identified and prioritized as essential services for recovery (electricity, fuel, water, gas, sewerage, data communication, telephone, cleaning, refuse, Aircraft Operating Surfaces, etc)?</p> <p>- What teams have been identified to undertake the restoration of such services?</p> <p>- How can medical, fire crash rescue services, EOD, decontamination, transportation, logistics, security and comms be integrated into the recovery operation?</p> <p>- What can be done to establish and test the coordinated response between the military and civilian powers?</p> <p>- Who can coordinate with Information Operations and Psychological Operations (PSYOPS)?</p>	

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
11	AIR DEFENCE Missile Defence Theatre Missile Defence (TMD) Ground-Based Air Defence (GBAD)	- Who is planning the AD and how can the AD plans be integrated in the FP measures? - At what level can AD W&R be integrated in FP alarm systems?	

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
12	<p>CBRN</p> <p>Sampling, Detection, Identification & Monitoring</p> <p>Warning & Reporting (W&R)</p> <p>Hazard Management</p> <p>METOC</p>	<p>- What capability will be in place to manage these tasks? - How will this task be coordinated and conducted?</p> <p>- What will be the theatre and localised CBRN W&R structure? - What capabilities / units will form this structure, and how will it be tested?</p> <p>- What capability will be employed to identify, sample and log potential hazards? - Who will manage this capability?</p> <p>- What integration can there be between CBRN and METOC?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
13	<p>LOGISTICS</p> <p>Fuel</p> <p>Food & Water</p> <p>Transport</p> <p>Equipment</p> <p>Weapons & Ammunition</p> <p>Sensors, ECM and Specialist Equipment</p>	<p>- Where will be the fuel points, Bulk Fuel Installations (BFI), fuel transfer points, fuel distribution systems (vehicles or pipes)? - What are the assessed vulnerabilities and how can they be protected?</p> <p>- How will the food and cooks / kitchen staff be inspected for hygiene/disease? - What are the risks to the food / water being deliberately contaminated? - How secure are the food / water convoys into the base? How are they inspected? - How will the food & water distribution points / sources / warehouses be inspected? - What capability will be in place for water purification?</p> <p>- What are the considerations surrounding FP unit transport? What are the effects of patrolling? What is the physical FoM given the threat, climate and terrain? Will there be a higher maintenance bill on the vehicles? Is there a need for extra training?</p> <p>- What effects are there from equipment limitations? Is there a need to re-supply essential equipment / spare parts, and if so, what is done to protect the supply chain?</p> <p>- Will weapons and ammunition storage locations be adequately defended against lightning, weather, and attack?</p> <p>- How will specialist systems such as ECM and sensors be maintained and supported? Who has responsibility to ensure they are functioning correctly?</p>	

NATO RESTRICTED
Releasable to PfP

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
14	<p>CONCEPT DEVELOPMENT</p> <p>Desired Effects</p> <p>Targeted Areas of Interest</p> <p>Named Areas of Interest</p> <p>Communication</p> <p>Defence Planning</p> <p>Prioritization</p>	<p>- What effects are required and why? How can these effects be achieved and with what resources?</p> <p>- What are the likely non-coalition / criminal infiltration routes and likely stand-off attack launch sites for MANPADS, rockets, mortars, snipers, IEDs, suicide attacks?</p> <p>- What controls exist over the local work force, critical working areas, access & control of food, water and fuel, flight-line sy, aircraft operating surfaces, and BFIs?</p> <p>- What are the priorities from the Targeted Areas of Interest to become the Named Areas of Interest?</p> <p>- What will be priority for defence and control? For example: FP C2 and CJ2 integration, population awareness & local political developments to drive the response and escalation of defence, COE, fuel/water/food security, security of HVAs. What assets/methods can be allocated?</p> <p>- What are the CIRs and where is the comms network diagram? Do they indicate who FP needs to liaise with on a regular basis, within and outside of their command?</p> <p>- Are there links into the CBRN W&R network, AOPG for requests for AT and ISR, other land units / LCC, Reaction Forces, local / HN security forces, CJ2, TBM Cell, COE points, medical, FCRS, PAR teams and shelters?</p> <p>- What are the priorities for telephone, data and radio links between units depending on time-critical information requirements e.g. between ATC and TESSERAL patrols.</p> <p>- Are there clear concentric layers of defence and are they centred on the COG / VPs? Who controls each layer? How are the different layers integrated into a coherent plan? How can mutual support be provided? How do units contribute in ways other than their core role to provide the flexibility needed to meet alternative or new threats?</p> <p>- How are Threat Assessments integrated to drive the prioritize vulnerabilities? How is</p>	

AD 80-25

SER.	QUESTION/ FACTOR	CONSIDERATION	CONSTRAINT / DEDUCTION / CRITICAL INFORMATION REQUIREMENT
	Risk Management	Situational Awareness (SA) maintained i.e. what sources of intelligence are used in order to help the commander re-assess their priorities? - How can the unit manage the risks posed by the various threats against the success of the overall mission? With all risks, what can be done to identify how to avoid, transfer, mitigate or accept them? - How can the risks be prioritized and what contingencies are in place to meet shortfalls?	

THREAT-CAPABILITY MATRIX

The FP Risk Matrix has been designed to put the threat first as this drives the FP process and to allow staff to view a near-complete list of possible mitigating factors for each threat. The Matrix combines several objectives into one table and forces staff to think deeply about the threat and possible / current mitigating measures. A lot of thought should go into the numbers selected, and ideas have been provided in the threat chapter in the main document. This tool enables FP staff to record what measures exist and apply scores against their individual effectiveness. This will vary with time and so should be updated regularly. **This process creates a list that can both enable an objective prioritisation of the various threats and identify shortfalls in mitigation measures.**

HOW TO USE (practice makes perfect!)

1. **Likelihood** is the probability that an event will occur – Table I.
2. **Impact** is the effect/s of an incident – Table II.
3. **Risk** is the Likelihood multiplied by the Impact.
4. **Likelihood Mitigation** comes from measures that prevent an incident from occurring – Table III.
5. **Impact Mitigation** comes from measures that lessen the impact of an incident - Table III.
6. *(Note that the effectiveness of a mitigating factor may change against different threats)*
7. **Overall Likelihood** is the **Likelihood** minus the average score for **Likelihood Mitigation**.
8. **Overall Impact** is the **Impact** minus the average score for **Impact Mitigation**.
9. The **Residual Risk** identifies the level of risk *after* mitigating measures have been applied, and is a % calculated by: the **Overall Likelihood** multiplied by the **Overall Impact** to give the **Overall Risk**, this figure is then divided by the **Risk**.

AD 80-25

The first row has been completed overleaf as an example! Practice!

Table I - Likelihood	
Severe	10
High	9
Significant	8
Medium	7
Low	6
Negligible	5

Table II - Impact	
Possible Mission Compromise	10
High Loss of Life / HVAs	9
Moderate Loss of Life / HVAs	8
Some Loss of Life / HVAs	7
Low Loss of Life / HVAs	6
Injuries / Repairable Damage	5

Table III - Effectiveness	
Extremely. There is an unlikely chance of successful hostile attack or error / failure, and main operations would be restored within the hour.	5
Very. Only a determined adversary or rare incidents are likely to affect operations, which would be fully restored within 2 hours.	4
Reasonable. Determined adversaries or common incidents could disrupt operations for several hours, and a limited recovery effort would restore essential services / operations within 3 hours.	3
Some. Opportunists could attack and disrupt operations and common incidents are likely to occur. Limited operations and some essential services may take up to 4 hours to restore.	2
Limited. Opportunity attacks would be difficult to prevent or respond to. Common incidents are likely affect operations, and any recovery effort would detract from main operations.	1
Negligible. Adversaries could easily attack operationally necessary equipment or personnel. The scope for incidents or accidents is very high and there are no measures or plans to direct a recovery effort.	0

NATO RESTRICTED
Releasable to PfP

AD 80-25

Threat / Hazard	Likelihood	Impact	Risk	Likelihood Mitigation	Effectiveness	Impact Mitigation	Effectiveness	Overall Likelihood	Overall Impact	% Residual Risk
Indirect Fire (IDF)	7	7	49	Dominate AOR Counter-Battery Systems Early Warning from HUMINT / CI Effect of Geographical Location ISTAR Integration Light Discipline	2 0 1 2 0 0 Ave=0.8	Incident Control / Command & Control Sense & Warn Accommodation Construction Shelters Personal TTPs (First Aid) IPE CASEVAC EOD	2 0 2 3 3 2 1 1 Ave=1.8	6.2	5.2	66 %
IED against ECP				Dominate Perimeter / Deterrence Observe Perimeter / Deterrence ECM ECP Procedures Stand-off Explosive Detection Dogs Searching outside ECP Searching Inside ECP Early Warning from HUMINT / CI		Incident Control / Command & Control ECP Construction Personal TTPs (First Aid) IPE CASEVAC EOD				

NATO RESTRICTED
Releasable to PfP

AD 80-25

Threat / Hazard	Likelihood	Impact	Risk	Likelihood Mitigation	Effectiveness	Impact Mitigation	Effectiveness	Overall Likelihood	Overall Impact	% Residual Risk
IED against Perimeter				Dominate Perimeter / Deterrence Observe Perimeter / Deterrence ECM Stand-off Early Warning from HUMINT / CI		Incident Control / Command & Control Engineering – Perimeter Engineering – Internal Bldg Personal TTPs (First Aid) IPE CASEVAC EOD				
IED or Sabotage on Base				Internal Patrols / Support by Base Personnel Early Warning from HUMINT / CI Dispersal of Accommodation		Incident Control / Command & Control Accommodation Protection Personal TTPs (First Aid) IPE CASEVAC EOD				
IED against Vehicle Patrol				Armoured Vehicles C-IED TTPs Vary routes / exits ECM Route Clearance Early Warning from HUMINT / CI ISTAR Integration		Incident Control / Command & Control QRF Personal TTPs (First Aid) IPE CASEVAC EOD				

NATO RESTRICTED
Releasable to PfP

AD 80-25

Threat / Hazard	Likelihood	Impact	Risk	Likelihood Mitigation	Effectiveness	Impact Mitigation	Effectiveness	Overall Likelihood	Overall Impact	% Residual Risk
IED / Mine against Foot Patrol				C-IED / Counter Mine TTPs Vary routes ECM Route Clearance Early Warning from HUMINT / CI ISTAR Integration		Incident Control / Command & Control QRF Personal TTPs (First Aid) IPE CASEVAC EOD				
Direct Fire (DF) / Close-Quarter Attack				Armoured Vehicles TTPs in Vehicles or when Dismounted Vary routes / exits Early Warning from HUMINT / CI		Incident Control / Command & Control QRF Personal TTPs (First Aid) IPE CASEVAC				
Surface-to-Air Fire (SAFIRE)				Dominate AOR / Anti-SAFIRE Ground Ops Observation / Over-watch ECM on Aircraft Flight Path Variation / Tactics Early Warning from HUMINT / CI		Incident Control / Command & Control IPE QRF CASEVAC EOD Specialist Fire Crash Rescue				
Kidnap				Armoured Vehicles TTPs in Vehicles or when Dismounted Vary routes / exits Early Warning from HUMINT / CI		Incident Control / Command & Control QRF Personal TTPs (Conduct After Capture) Personnel Recovery				

NATO RESTRICTED
Releasable to PfP

AD 80-25

Threat / Hazard	Likelihood	Impact	Risk	Likelihood Mitigation	Effectiveness	Impact Mitigation	Effectiveness	Overall Likelihood	Overall Impact	% Residual Risk
Subversion or Foreign Intelligence Services (FIS)				Access Control to Secure Working Areas Security Training & Education Security Furniture Early Warning from HUMINT / CI Communication Information Systems (CIS) COMSEC		CI / Police Investigation				
Crime & Policing Issues				CI / Policing		CI / Police Investigation				
Infiltration				Dominant Perimeter / Deterrence Observe Perimeter / Deterrence ECP / Control of Entry Procedures Pass System & Vetting by CI		Alert by Base Population / Patrol QRF / Incident Control				
Energy Security and preservation				Avtur / Diesel / Gas Delivery Protection Avtur / Diesel / Gas Storage Protection Generator Protection Distribution Protection		Back-up Supplies Back-up Generation / Redundancy				
Food & Water Security and preservation				Vetting of Sources Storage Protection Preparation Quality Control / Treatment Training & Education of Base Personnel		Medical Treatment & CASEVAC				

NATO RESTRICTED
Releasable to PfP

AD 80-25

Threat / Hazard	Likelihood	Impact	Risk	Likelihood Mitigation	Effectiveness	Impact Mitigation	Effectiveness	Overall Likelihood	Overall Impact	% Residual Risk
Health Protection				Training & Education of Base Personnel Ablution Maintenance Refuse Collection Laundry Pest & Vector Control Prophylaxis		Medical Treatment & CASEVAC				
Environ. and Industrial Hazards (EIH)				Training & Education of Base Personnel Survey Possible Threats		Medical Treatment & CASEVAC				
Unexploded Ordnance				C-IED / Mine TTPs Mine & C-IED Maps		Incident Control QRF EOD				
Civil Unrest				Early Warning from CI / HUMINT		Riot Training and Equipment				
CBRN & TIM				Reconnaissance of Possible Threats Early Warning & Tracking		Alarms CBRN TTPs IPE CBRN COLRPO				

NATO RESTRICTED
 Releasable to PfP

AD 80-25

Threat / Hazard	Likelihood	Impact	Risk	Likelihood Mitigation	Effectiveness	Impact Mitigation	Effectiveness	Overall Likelihood	Overall Impact	% Residual Risk
Hostile Influence of Tactical Cohesion				Command & Control Consequence Management Legal / ROE Higher HQ Integration ANSF Integration CI / CIMIC / HUMINT Integration ISTAR Integration IO Integration		CI Investigation Analysis of Procedures				

CRISIS RESPONSE OPERATION URGENT REQUIREMENT (CUR) PROCESS

1. The following information has been added to provide CUR originators with advice on how to avoid common mistakes that delay the staffing process.
2. **Justifications.** It is necessary to provide clear message to the Standing HQs on new and emerging requirements. Critical information needed includes how the budget and Force Generation process can provide a capability that would not be possible to implement by any other means.
3. **Linkages.** NATO will support requirements that are clearly bourn from officially recognized documents and processes. The types of documents that are highly effective include OPLANs, OPOrDs, MMRs and doctrine. Demonstrating that mitigating measures are clearly based on the FP Process, which includes a Mission Analysis and thorough Threat, Vulnerability and Risk Assessments.
4. **CUR Contents.** The following list describes the sections of the CUR:
 - a. Originator.
 - b. Title of Project.
 - c. Capability Owner.
 - d. Requirement Definition Owner.
 - e. Detailed Requirements.
 - f. Military Justification.
 - g. Lines of Development.
 - h. Cost Estimate.
 - i. Operation and Maintenance Cost.
 - j. Rationale for NATO funding.
 - k. Implementation.
 - l. Time frame.
 - m. Impact of Failure.

AD 80-25

- n. Prioritization.

5. **ISAF Requirements and Ownership.** The following list details which JFCBS departments have ownership of certain capability areas, so when following up or preparing CURs, time can be saved by approaching the relevant staff.

- a. Infrastructure (JENG)
- b. Finance (J8)
- c. CIS (J6)
- d. Personnel (J1)
- e. Training (J7)
- f. Security (J2/J6)
- g. Force Protection (J3)
- h. Air ops (J3)
- i. Logistics (J4)
- j. CIED (J3)
- k. Intelligence dissemination and archiving (J2)

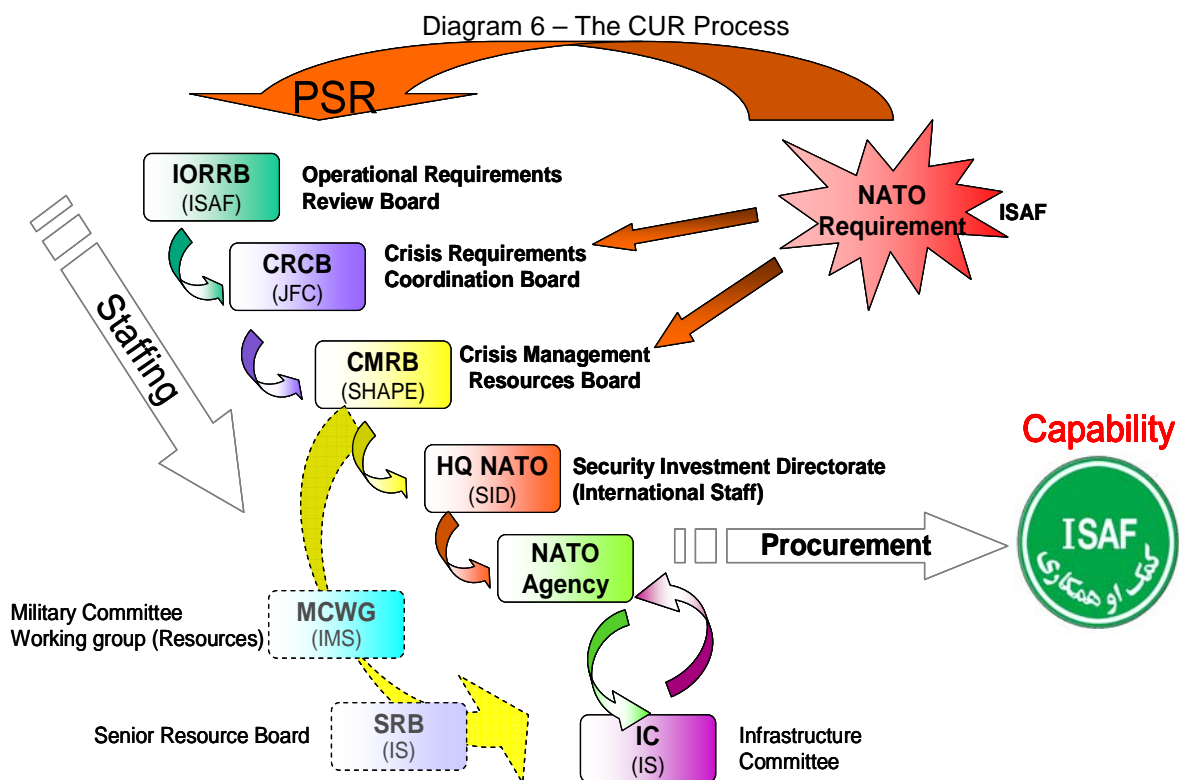
6. **ISAF Operational Requirements Players.** The following lists the agencies involved in the CUR process and their broad roles:

- a. NATO HQ:
 - (1) NATO Atlantic Council (NAC)
 - (2) Senior Resource Board (SRB)
 - (3) Infrastructure Committee (IC)
 - (4) International Staff (IS)
- b. SHAPE
 - (1) Capability Management Directorate (CMD)
 - (2) Crisis Management Resource Board (CMRB)

AD 80-25

- c. JFC HQ
 - (1) Crisis Resource Co-ordination Board (CRCB)
- d. Theatre
 - (1) ISAF Operational Requirements Review Board (IORRB)
 - (2) Originator
- e. Host Nations (NAMSA, NC3A, SHAPE, lead nation)

7. The whole CUR process can be represented by the following diagram:



C-IED DEFEAT ACTIVITIES – WITH UTILITY FOR FP

Strategic level C-IED involves the isolation of the adversary's in-theatre IED system from outside influences, finance and supplies. At the operational and tactical levels, the focus switches to the systematic application of the Key Operational Activities against the full depth of the adversary's IED system.

1. Predict

- a. Identify hostile patterns of activity by observing local routine.
- b. Establish patterns of normal daily life so changes are easy to spot.
- c. Identify emerging threats by contributing to and benefiting from good relationships with the intelligence community.
- d. Predict future likely hostile actions / targets by being objective and realistic about your weaknesses and strengths.
- e. Prioritize ISR missions by integrating with Air Operations Planning Group (AOPG) to include your requirements and maintain your priority in the mind air planning staff (you will be defending an installation of operational- and probably strategic-level importance!).
- f. Identify possible leaders, planners, bomb-makers and emplacers in your TAOR. This is entirely possible given external patrolling duties and the need to perform 'consent winning' work within the TAOR that has been proven to draw information from the local populace.
- g. Exploit forensics by using local Weapons Intelligence and EOD teams to collect material for forensic examination.

2. Prevent

- a. Disrupt hostile operations and their support structure through Information Operations and consent winning tactics in the TAOR. Hostile individuals will sometimes be from outside of the TAOR or be pressured into conducting operations and an intelligent approach by FP units can build trust and consent for coalition presence.
- b. Deny IED equipment / supplies by dominating the TAOR.

AD 80-25

- c. Educate coalition forces in hostile IED TTPs so indications of an attack can be spotted early. Good quality training has been proven as the most effective countermeasure!
- d. Reward the local populace for their cooperation, which comes back to consent winning operations. This can also discourage local people from developing loyalty to hostile forces. Such activities would all be part of the higher, if highest, commanders plans in any case.
- e. Avoid setting patterns which can be exploited by an adversary – be unpredictable.
- f. Effective TTPs particularly at halts and VP crossings saves lives.

3. **Detect**

- a. The detection of IED or CBRN materiel and their related components is possible through both physical and technical means. Recording when and where the systems or troops detect possible threats can help build a picture of attack patterns.
- b. Recognising suicide bombers is possible by having control over the TAOR so anyone trying to conduct an attack becomes conspicuous against the background of routine and normal daily life. Forensic teams can track those whom have been in contact with IED parts.
- c. Force manoeuvre elements need to be able to detect IEDs at a suitable range, in sufficient time, and with enough accuracy to allow the joint force to take action to prevent the attack from occurring.
- d. The FP operations may be tailored to suit the Priority Intelligence Requirements (PIR) that can support C-IED operations and relevant Named Areas of Interest (NAI). This may be done by increasing the contact between troops in the TAOR and populace or concentrating on a particular area (more troops or maybe no troops and covert surveillance).
- e. FP planners must consider the use of both explosives detection and counter radio controlled IED equipment at ingress and egress points as well as other vulnerable points.

4. **Neutralize.** There are materiel solutions such as ECM as well as TTPs to avoid triggering an IED. Neutralising also includes the rendering safe of IEDs, caches and captures enemy ammunition.

AD 80-25

5. **Mitigate**

- a. Again materiel solutions and TTPs can be used to limit the effects of a detonation such as using the right vehicles, personal protection and route selection. FP engineering is essential to ensuring facilities can withstand or minimise the blast and fragmentation effects of an IED.
- b. Control over the TAOR and the activities therein allow FP troops to dictate the possible distance between IEDs and their intended targets.
- c. Reducing the time likely targets are exposed is a method controlled under TTPs.
- d. By practicing the reaction to an attack such as evacuation and reinforcing guard / medical positions can ensure FP troops have a refined plan to contain the after-effects of an attack as well as regain control over the TAOR.
- e. Information Operations can alter the tide of public opinion in the favour of coalition forces to prevent non-coalition forces legitimizing their actions.
- f. Effective convoy drills, particularly at halts and VP crossing, can substantially reduce the risk of casualties.

FP MEASURES

1. **Introduction.** The overall aim of FP is to adopt appropriate protective measures relevant to the threat. By constantly referring to the Threat Assessments (TA), realistic measures can be implemented that do not degrade the primary mission nor allow personnel to become complacent. A fine balance is needed. Additionally, FP measures are not meant to portray the image of an occupation force; rather, the population should perceive ISAF FP Measures as being undertaken by a professional, disciplined, well-trained and confident force.
2. The Alert States and any changes would normally be decided upon by the theatre commander, and subordinate commanders / local FP officers are at liberty to impose more restrictive measures as the situation dictates, but may not relax the alert states. Theatre headquarters must be informed of any changes made by subordinate commanders as this offers valuable intelligence / information that may need distributing to others.
3. **Definition.** All measures taken to minimize the vulnerability of personnel, facilities, equipment and operations to any threat and in all situations, so as to preserve the freedom of action and operational effectiveness of a force are to be considered as FP Measures. The abbreviation CBRN is used for Chemical, Biological, Radiological and Nuclear protection, and includes protection from Toxic Industrial Materials (TIM), Releases Other Than Attack (ROTA) and associated hazards resulting from accidents or incidents leading to environmental damage or disaster.
4. **Theatre FP Measures.** Theatre FP measures are divided into 3 categories, and each category has related counter-measures associated with them:
 - a. **Alert States (Alpha, Bravo, Charlie and Delta)** which drive specific counter-measures. Each Security Alert State has a list of specific counter-measures attached to it, and the minimum standards for these are given in the ACO Security Directive 70-1. An example of what could be implemented has been included at Appendix 1. When a Security Alert State is declared, all related counter-measures must be implemented, as do additional specific measures if they are relevant to a specific risk or hazard.
 - b. **FP Colour Codes (Green, Yellow, Red)** which in turn drive the Dress State, Weapon State, and Vehicle Movement Constraints. An example of Colour Codes and associated constraints is at Appendix 2.
 - c. **CBRN / TIM Threat Level (Nil, Very Low, Low, Medium, High, Very High, and Actual)** which in turn drives the CBRN Dress State (0, 1, 2, 3 or 4). An example of the Dress Codes is at Appendix 3.

AD 80-25

5. **Route Restrictions.** In addition to the vehicle movement constraints, it may be necessary to open, close or restrict access along certain routes. This not only helps vehicles avoid choke points, and therefore become opportunity targets, but also forces a more varied use of routes. This latter point is essential to avoid pattern setting, which is one of the main precursors to attacks. An example is given at Appendix 2.
6. **Code Words.** Code words are an identification tool to permit all units to verify the authenticity of a distress call or unfamiliar visitor.
7. **Walking Out Policy.** This must be dependent on the Alert State but sensible enough to maintain morale and encourage a cultural interaction between troops and HN.
8. **Information Dissemination.** A system is required whereby theatre FP personnel can rapidly seek permission from the theatre commander to alter the alert states and pass this information down the chain of command to units. The information must work 2 ways if a subordinate unit moves to a higher alert state, everyone else needs to be aware that the threat has changed unexpectedly.

APPENDICES:

1. Alert State Definitions & Counter-Measures
2. Colour Codes, Weapon Codes, Vehicle Movement Constraints
3. CBRN / TIM Threat Levels

ALERT STATE DEFINITIONS & COUNTER-MEASURES

Alert States	Description
ALPHA	Issued as a general warning of possible terrorist activity, the nature and extent of which are unpredictable, and when circumstances do not justify the full implementation of the measures contained in a higher alert state. The measures in this Alert State must be capable of being maintained indefinitely.
BRAVO	Issued when there is an increased and more predictable threat of terrorist activity although no particular target has been identified. It must be possible to maintain this state for a period of weeks without causing undue hardship and without affecting operational capability.
CHARLIE	Issued when an incident occurs, or when intelligence is received which indicates that some form of terrorist action is an imminent possibility. The implementation of this Alert State for more than a short period will probably cause hardship.
DELTA	Issued in the immediate area when a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally this alert stage is used as localized warning.

NATO RESTRICTED
Releasable to PfP

AD 80-25

Counter Measure	FORCE PROTECTION MEASURES
ALPHA	
1	<p>Normal Framework Operations</p> <ul style="list-style-type: none"> a. All personnel to be reminded at regular intervals to be suspicious of strangers (particularly if carrying parcels or containers) and of unidentified vehicles or abandoned vehicles in the vicinity of ISAF buildings or facilities. b. Plans are to be in place for the evacuation of buildings and for sealing areas where an explosion or attack is most likely to occur – these are to be reviewed at regular intervals. c. Key security personnel are to be on call. d. Buildings, rooms and any areas where IEDs or personnel could be hidden and not in regular use are to be locked and checked. e.
2	<p>Walking Out Policy</p> <p>Granted in accordance with the regulations stated in Annex E to SOP 331.</p>
3	<p>Access to Installations</p> <ul style="list-style-type: none"> a. ISAF / GCTF / Diplomatic Corps / VIPs from ISAF Troop Contributing Nations (Generals / Heads of Mission): <ul style="list-style-type: none"> i. VIP Control Card must be displayed. ii. The ID of one passenger / driver will be checked (normally from the first vehicle). b. Others: <ul style="list-style-type: none"> i. Thoroughly check ID of all passengers / drivers (i.e. picture against person checked). ii. Visual vehicle search. c. Goods purchased outside of NATO or GCTF compounds to be checked. d.
4	<p>Preparation for Higher Alert States</p> <p>Review plans for implementation of a higher Alert State.</p>
BRAVO	
5	<p>Implement all measures for Alert State ALPHA</p>

NATO RESTRICTED
Releasable to PfP

AD 80-25

Counter Measure	FORCE PROTECTION MEASURES
6	Counter-IED a. The use of Electronic Counter Measures (ECM) where possible on Entry Control Points (ECP), vehicle moves and foot patrols. b. The inside and outside of buildings are to be inspected regularly for suspicious packages, especially at the start and end of the working period (before and after the location is opened for more people to enter). c. Where ever possible, all mail is to be positively examined for signs of letter / parcel bombs. d. All deliveries of goods / supplies are to be physically checked for signs of explosives / intruders. e. Random search of visitors' suitcases, parcels and containers for weapons and explosives.
7	Patrolling Routine patrolling within compound, especially around sensitive buildings and areas inside the camps
8	Access to Installations As per Counter Measure 3, but a partial search of all civilian vehicles or full search of random civilian vehicles is required.
9	Outgoing Traffic a. For ISAF traffic, check convoy card and compliance with ordered dress state, vehicle movement constraints, weapons state and CBRN dress state. Personnel carrying Force Exemption Cards or the like may be subject to local arrangements. b. For other traffic, conduct random body and vehicle searches. c.
10	Local Hires / Civilian Contractors Increased monitoring and continuous escorting (depending on the level of security clearance) of local civilian hires and contractors are required.
11	Reinforcement Preparations All RCs to identify forces to reinforce their pre-identified vulnerable sites.

NATO RESTRICTED
Releasable to PfP

AD 80-25

Counter Measure	FORCE PROTECTION MEASURES
12	<p>ID Checks</p> <p>Random check of ID cards on military personnel, local hires / civilian contractors and vehicles...etc.</p>
13	<p>Preparation for Higher Alert States</p> <p>Review plans for implementation of a higher Alert State.</p>
14	<p>Contingency Plans</p> <ul style="list-style-type: none"> a. Confirm plans for loss of essential services such as power, supplies, water...etc as is relevant to the installation. b. Identify manpower that may be used at higher Alert States to reinforce guard posts and check points as required.
CHARLIE	
15	<p>Implement all measures for Alert State BRAVO</p>
16	<p>Walking Out Policy</p> <p>Walking out by military personnel through and to non-secure areas to be halted.</p>
17	<p>C-IED</p> <ul style="list-style-type: none"> a. Where possible, cars and objects such as crates, dustbins...etc are to be moved 25m away from buildings of a high occupancy, sensitive or prestigious nature. b. Enforce centralised parking at least 25m away from likely target locations / buildings where possible. c. Restrict access to contactors' & vendors' vehicles.
18	<p>Patrolling</p> <ul style="list-style-type: none"> a. Surge patrolling of MANPADS footprint during landings / take-offs at all ISAF-used airfields is required. b. Increase patrolling activity in the vicinity of GIRoA and ISAF facilities is required.

NATO RESTRICTED
Releasable to PfP

AD 80-25

Counter Measure	FORCE PROTECTION MEASURES
19	Outgoing Traffic a. 100% ID check of as many personnel as the traffic flow allows (i.e. picture against person checked). b. As per 9 but a full search of all non-ISAF vehicles is necessary (including storage areas, under body, engine compartment etc).
20	Movement Control Maximum use is to be made of armoured vehicles for transporting personnel.
21	Local Hires / Civilian Contractors a. All Local Hires / Civilians entering the facility are to be searched.
22	Reinforcements a. All RCs are to identify forces to reinforce airfields critical to their operations. b. All airfields, Main Operating Bases, Forward Mounting Bases, and Provincial reconstruction Teams are to confirm communications with their respective RCs.
23	Guard Posts a. All guard posts and checkpoints to be fully manned. b. All designated Vulnerable Points (VPs) are to be adequately protected with special attention given to facilities that are not within military establishment boundaries.
24	Contingency Plans a. Confirm and rehearse Incident Response procedures as per Special Operating Instructions (SOI). b. Establish communications between RC to ISAF facilities and to ANSF / GIRoA operations centres. c. Prepare to implement Non-Combatant Evacuation Operation (NEO). d. Consider recalling, based on the specific threat, ETTs, OMLTs to ISAF facilities.

NATO RESTRICTED
Releasable to PfP

AD 80-25

Counter Measure	FORCE PROTECTION MEASURES
25	Preparation for Higher Alert States Review plans for implementation of a higher Alert State.
DELTA	
26	Implement all measures for Alert State CHARLIE
27	Counter-IED a. Make frequent and thorough checks of building exteriors, especially areas that may be prove an attractive target. b. Centralise parking of vehicles at a suitable distance from key buildings and accommodation. c. All vehicles already in the installation are to be positively identified. d. Search all visitors' bags for weapons or explosives.
27	Patrolling a. Use personnel not on essential duty to increase patrolling activity, particularly on areas of threatened installations and on main roads. b. Depending on specific threat, active domination of MANPADS footprint during landings/take-offs becomes main effort. c. Request more ANSF cooperation with external patrolling and C2 liaison.
28	Outgoing Traffic As per 19 but with additional body searches of all non-ISAF personnel (in accordance with HN customs as required).
29	Movement Control a. Prepare to occupy precautionary critical chokepoints after an attack in order to cordon & control the area. b. Implement plans with the local authorities to close public and military roads which might make the site more vulnerable to an attack. c. Deploying additional traffic control measures (barriers and obstacles) external to ISAF installation. d. Only mission essential external road movement permitted.

AD 80-25

Counter Measure	FORCE PROTECTION MEASURES
30	Local Hires / Civilian Contractors Only mission essential visiting by civilians, local hires / civilian contractors.
31	Reinforcement Depending on specific threat, EOD Team and CBRN Team located routinely at HQ ISAF.
32	Sustainability of Security Measures Supervisors make constant checks (personnel, equipment, procedures, etc) in order to safely and effectively operate at this threat level.

AD 80-25

NATO RESTRICTED
Releasable to PfP

(INTENTIONALLY BLANK)

H-1-8
Releasable to PfP
NATO RESTRICTED

COLOUR CODES & VEHICLE MOVEMENT CONSTRAINTS

STATES INSIDE CAMP		STATES OUTSIDE CAMP		
DRESS STATE	WEAPON STATE	DRESS STATE	WEAPON STATE	VEHICLE MOV
CBA and helmet available	WU Weapon Unloaded	CBA and helmet available	WL Weapon Loaded	One vehicle with 2 armed personnel
WL: Only for camp security and specifically detailed personnel while on duty		Vehicle equipped with communications		
DRESS STATE	WEAPON STATE	DRESS STATE	WEAPON STATE	VEHICLE MOV
CBA and helmet available	WU Weapon Unloaded	CBA on , helmet available . CBA may be removed if personnel are protected by other means, and if approved by on-site commander	WL Weapon Loaded	Minimum of 2 vehicles and 4 armed personnel
WL: Only for camp security personnel while on duty, and other personnel as directed by the responsible commander, and iaw ROE		At least one vehicle equipped with communications		

NATO RESTRICTED
Releasable to PfP

AD 80-25

DRESS STATE	WEAPON STATE	DRESS STATE	WEAPON STATE	VEHICLE MOV
CBA and helmet on . CBA and helmet may be removed if personnel are protected by other means and approved by on site commander	WU Weapon Unloaded	CBA and helmet on CBA may be removed if personnel are protected by other means, and if approved by on-site commander	WL Weapon Loaded (Top cover or dismounted troops may be Wpn Ready (WR) if ordered)	Minimum of 2 vehicles, 4 armed personnel and mission-critical movement only
WL: Only for camp security personnel while on duty, and other personnel as directed by the responsible commander, and iaw ROE		At least one vehicle equipped with communications Depending on threat, all vehicle movements may be suspended COMISAF retains the right to limit to the use of only armored or hardened vehicles		

EXPLANATION OF WEAPON STATES	
Weapon unloaded (WU)	NO magazine on the weapon, NO round in the chamber, magazines readily available.
Weapon loaded (WL)	Magazine on the weapon, NO round in the chamber.
Weapon ready (WR)	Magazine on the weapon, round in the chamber, weapon on safe

ROUTE RESTRICTIONS	
OPEN	No restrictions on a specified route
RESTRICTED	Used to remove traffic from a particular section of a specified route (e.g. route PURPLE restricted between point 3 and point 4) Vehicles already using the route must (in order of priority) (1) move immediately onto an alternative route (2) move directly to the shelter of the nearest military compound on that section of route or (3) continue along that section of route and exit it as quickly as possible. Vehicles not on that section of route must plan an alternative route around it.





NATO RESTRICTED
Releasable to PfP





AD 80-25

CLOSED	Used to remove traffic from the complete length of a specified route (e.g. route PURPLE closed) Vehicles already using the route must (in order of priority) (1) move immediately onto an alternative route (2) move directly to the shelter of the nearest military compound if no alternative route is available Vehicles that have not yet left a military compound along a closed route must stay in position unless an alternative route is available
---------------	--

Note: Route restrictions will normally be considered in conjunction with the vehicle movement constraints driven by the FP Colour Code.

CBRN / TIM THREAT LEVELS

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

CBRN TIM - THREAT LEVELS¹			
Threat Level	Code	Threat Assessment	Description
LOW		Unlikely	Although TIM release is possible, industrial infrastructure ² and security levels are robust.
MEDIUM		Credible	There is an increasing risk of TIM release due to a decay of industrial infrastructure and/or a degradation of the security of industrial infrastructure.
SIGNIFICANT		Probable	Release of TIM may occur with little additional warning due to weakness of industrial infrastructure and/or insufficient security of industrial infrastructure.
HIGH		Highly Likely	There is an immediate risk of TIM release, without warning, due to damage to industrial infrastructure and/or a lack of security of industrial infrastructure.

¹ The likelihood of release is based on an assessment of accidental, collateral or intentional release.

² e.g. Installations, storage sites, transportation networks, pipelines.

AD 80-25

CBRN DRESS STATES				
	Respirator/Mask	Suit	Boots	Glove
NBC 0	Issued and carried	First set ready, second set deployed	First set ready, second set deployed	First set ready, second set deployed
NBC 1	Carried	Issued and carried	Issued and carried	Issued and carried
NBC 2	Carried	Worn	Carried	Carried
NBC 3	Carried	Worn	Worn	Carried
NBC 4	Carried	Worn	Worn	Worn

Notes:

1. Commanders may order the level of protection to be:
 - a. **Reduced** if warranted by special conditions e.g. if personnel are inside COLPRO or it is judged that the risk of casualties is outweighed by the need to pursue the mission unencumbered by the use of some or all items of IPE.
 - b. **Increased** if local conditions demand a higher degree of protection.
2. The additional description 'Mask' or 'Respirator' may be added to any of the Dress States: this may denote any nationally recognised form of respiratory protection.
3. Dependent on the operational situation and the tasks being carried out, to take full advantage of risk management commanders may add the suffix 'Jacket / Suit' open to any of the Dress States 2, 3 or 4.

NATO RESTRICTED
Releasable to PfP

AD 80-25

(INTENTIONALLY BLANK)

H-3-4
Releasable to PfP
NATO RESTRICTED

MILITARY ENGINEERING DESIGN GUIDELINES FOR EXPEDITIONARY OPERATIONS

References:

- A. AJP-3.14 Allied Joint Doctrine for Force Protection.
- B. Bi-SC 85-1 Capability Package Directive.
- C. NATO STANAG 2280 – Design Threat Levels and Handover Procedures for Temporary Structures.
- D. JFOB Handbook – US Force Protection Handbook for Joint Operational Bases, issued Dec 06.
- E. ME Vol. IX Pt 1 – UK Military Engineering Pamphlet – Force Protection Engineering, issued Nov 07.
- F. MC 0560 – MC Policy for Military Engineering.
- G. AJP 3.12(A) – Allied Joint Doctrine for Engineer Support to Joint Operations.

INTRODUCTION

1. Military Engineering support to force protection (FP) is only one element of the broader military engineering field; however, in the interest of brevity, the term Military Engineering (MilEng) is used within this document to specifically refer to MilEng support to FP. MilEng represents an essential element of the suite of FP measures available to a NATO expeditionary force to secure itself once deployed. They often represent the last line of defence in a layered approach of FP components including intelligence, early warning and detection systems and procedures which together combine to make NATO facilities secure. MilEng comprises:

- a. Blast & Ballistics Protection (***considered in this Annex***).
- b. Fire Safety and Fire Engineering (covered in Annex M).
- c. Public Health, including Utilities and Services infrastructure (covered in Annex M).
- d. Town Planning¹ (no further detail given in this document).
- e. EOD, IEDD, C-IED and Mines Awareness (covered in Annex G).

MilEng is, in short, an essential component of the integrated FP effect. Reference A gives further guidelines on NATO's integrated capability approach to FP.

2. The Delivery of MilEng measures on NATO Crisis Response Operations (CROs) remains a TCN responsibility; APOD/SPODs are eligible for common

¹ Including infrastructure / services de-confliction and dispersion.

AD 80-25

funding as well as those elements of HQs and FOBs/FSBs where strategic assets exist and where NATO has a common interest in funding them. The remaining fixed base infrastructure and MilEng shall be a national responsibility delivered by the nominated lead nation. All enabling infrastructure capability required for NATO CROs - and eligible for NATO common funding - is delivered as set out in Reference B. This process is initiated by the production in theatre of a CRO Urgent Requirement (CUR). As clearly directed in Annex D to Reference B, for all new infrastructures, consideration must be made in the submission of all CURs of integrating FP measures into the requirement at the front end. This consideration in itself does not mean that MilEng measures will be included in the end-product; however they do ensure that a process of analysis has been followed to ensure the infrastructure delivered is built in such a way as to make it optimally protectable through the lifetime of a CRO. (A simple example is the provision of tented accommodation; in the early stages of an operation time and resource availability may preclude the construction of blast protection; however, the tents can be laid out with such spacing that it can easily be provided if the threat increases. The spacing itself represents a MilEng measure in that it disperses personnel and therefore reduces the impact should a threat event occur.)

AIM

3. The aim of this Annex is to define the FP Minimum Military Requirement (MMR) for 'common funded' infrastructure on NATO led CROs. The material in the Annex is coherent with, and directly in support of, existing NATO doctrine on FP (References A and C). It further draws upon the wide and detailed national doctrine of the member nations, notably References D and E. The Annex gives commanders and military engineers in the Theatre of Operations the tools necessary to implement the optimal level of physical FP measures for infrastructure on the NATO fixed operating bases. The Annex describes, in generic terms, the minimum baseline of physical force protection needed in the Low Threat Environment (as defined in Reference A), from which additional enhancements can be added as, and if, the threat level increases. It is not overly technical in the specifications directed, thereby giving flexibility to the commander and engineers on the ground to deliver the optimal solution from the suite of national expertise and technical solutions that presently exist.

RISK AND RESILIANCE

4. As highlighted in the main document, all expeditionary forces have vulnerabilities. It is the responsibility of commanders at every level to conduct the necessary Threat Assessment, assess these vulnerabilities and mitigate the likelihood and consequences of them being exploited by enemy action. This effectively enhances NATO's ability to withstand single or multiple attacks on its fixed facilities on expeditionary operations. Fixed Infrastructure on APODs/SPODs/FOB/FSBs is one such critical vulnerability, identified by Vulnerability Assessments and mitigated by MilEng measures. The diagrams below illustrate the process of Risk Management, which must be gone through by the FP staff to determine the optimum FP measures (including MilEng) that should be put in

AD 80-25

place. MilEng provides a key passive measure that can be employed to reduce the residual risk to an acceptable level. It is important therefore that, throughout this FP planning process, Engineers are involved to ensure the optimum level of MilEng measures are put in place.

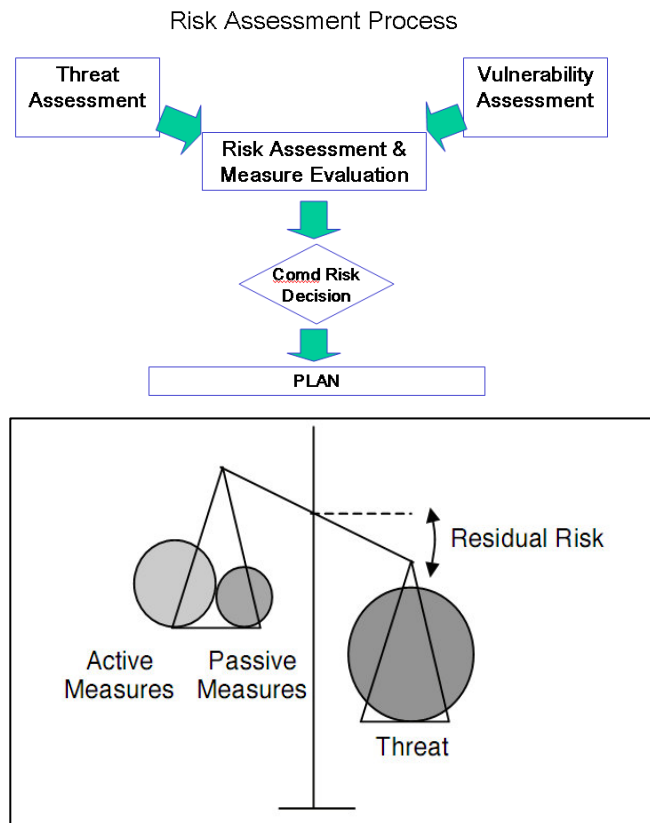


Figure 1 – FP Planning, balancing the threat with the optimum level of mitigation measures.

MILENG GUIDING PRINCIPLES

5. MilEng measures available to minimize blast and ballistic threats² include:
 - a. Standoff
 - b. Physical barriers (including compartmentalization)
 - c. Protective Structures
 - d. Access control (incl. ECPs)
 - e. Hardened fighting positions / towers / overwatch

² And secondary weapon effects, including hazards from structural material / debris and progressive structural collapse.

AD 80-25

- f. Security lighting
- g. Intrusion detection and surveillance systems (IDS / CCTV)

6. As a guiding principle, each MilEng measure must not be looked at in isolation but in an integrated approach; for instance the use of a combination of blast walls and standoff can achieve a protective effect that outweighs the use of either in isolation. MilEng methodology will evolve as an operation matures. In the early stages of a CRO the principles at Appendix 1 set out the recommended design guidelines that apply in the delivery of timely MilEng measures. Thereafter, as opposed to contributing nations' military engineer delivered options, a more deliberate approach can be taken utilising more permanent structures constructed by NATO Agencies.

7. The methodology behind each of the MilEng measures is:

- a. **Standoff.** For every doubling of the standoff distance from the threat, the fragmentation hazard is reduced by a factor of 4 (one quarter) and the blast effect is reduced by a factor of 8 (one eighth). The diagram illustrates the reduced effect of blast with standoff.

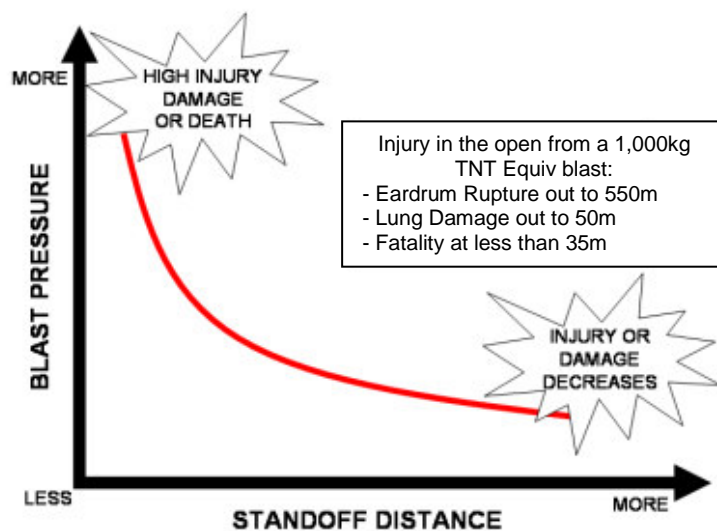


Figure 2 – Effect of Standoff

The best technique to reduce the risks and effects of an enemy attack, especially one involving explosives (VBIED, IDFs), is to keep the attack as far away from the facility and inhabited structures as possible (see Figure 2 above). Ideally, maximum standoff should be a primary consideration when personnel are deciding where to locate a facility. If distance is not possible, the next best solution is to maximize standoff for individual, inhabited structures. Regardless, even with adequate space, standoff must be coupled with appropriate operational security procedures in order to be effective. Allowances for standoff distance should also provide opportunities to upgrade

AD 80-25

structures in the future to meet increased threats or to accommodate higher levels of protection.

b. **Physical barriers**{ TC "PHYSICAL BARRIERS" \F H \L "9" }.

Physical barriers can serve to prevent the passage of both enemy personnel and equipment as well as weapon projectiles and effects. Two major types of physical barriers should be considered:

- (1) Natural (mountains, swamps, thick vegetation, rivers, bays, cliffs, etc).
- (2) Man-made (fences, walls, gates, vehicle barriers, etc).

Barriers form an integral part of the perimeter security system and serve to facilitate control of pedestrian and vehicle ingress and egress. Physical barriers are used at the facility perimeter to perform several functions:

- (1) Define the perimeter of the facility.
- (2) Establish a physical and psychological deterrent to attackers and individuals from attempting unlawful or unauthorized entry.
- (3) Optimize use of security forces.
- (4) Enhance detection and apprehension opportunities by security forces.
- (5) Channel the flow of personnel and vehicles through designated entry control points (ECP) in a manner which permits efficient operation of the personnel and vehicle identification and control system.

Barriers also provide protection from projectile, blast and fragmentation effects. Barriers must be designed to a level that fragmentation effects from the design threat cannot pass around them and blast effects cannot travel around them. A great deal of data on the protective properties of various materials against various threats exists in References D and E and other similar publications. This data should be referred to when developing MilEng designs. Note also that blast protection barriers must not in themselves create secondary fragmentation hazards and should therefore be of a durable nature. Barriers which can be relocated offer an attractive option as they can enable cost effective reconfiguration of physical force protection as the threat evolves. Further details on Physical barriers, including the MMR, are given in Appendix 2.

c. **Protective Structures.** These include operationally essential structures and high occupancy areas (including DFACS, RSOI, Welfare/Fitness facilities) and all other buildings where over 50 personnel

AD 80-25

gather. Infrastructure in High Occupancy Areas is to be of such a construction standard that, in the first instance, it is able to be upgraded to a higher level of FP without the need for works to dismantle large elements of the structure. (Where possible, existing reinforced concrete frame buildings are to be utilised thereby offering a certain minimal level of MilEng over and above that of temporary structures.) In instances where the threat is raised, such buildings are to be able to withstand the resulting blast, heat and fragmentation effects of an attack by the deemed scale of IED or IDF. Sufficient standoff, protection and compartmentalisation are to be provided to ensure that, in the event of a single attack, casualties are minimised and continued operational effectiveness is not eroded. All other critical infrastructure (including operations rooms and C3S facilities) is to be constructed with the required level of MilEng measures as dictated by the threat. Consideration should be given to Failure Mitigation measures. An assessment of existing structures should be carried out by a qualified engineer to assess the potential failure mechanisms and ways to reduce their likelihood and impact in the event of an enemy attack. Buildings that do not have structural redundancy should not be used. Further details on the classification of infrastructure are given in Para 10 below. For further details on the MilEng MMR for Protective Structures, see Appendix 4.

d. **Access Control (incl. ECPs).** All vehicle and pedestrian access control points for NATO facilities should be of such a design that, with the use of effective and efficient operating procedures, they can withstand a SUIVBIED attack with minimum casualties of those personnel operating the ECP and composite minimal reduction in operational effectiveness. In the first instance redundancy must be ensured with sufficient access capacity surplus to maintain operational effectiveness during and pos attack. As a baseline standard an ECP must:

- (1) allow quick entry to authorized vehicles and pedestrians;
- (2) be able to cope with visitors;
- (3) allow access to delivery vehicles;
- (4) have ability to reject unauthorized vehicles and personnel.

Unless otherwise specified, the Design Standard Threat to be considered is a VBIED of 1000kg TNT equiv. Appendix 3 gives further technical criteria and the MMR for ECPs.

e. **Hardened Fighting Positions.** There is a great variety of hardened fighting position designs available in NATO member nation FP field publications (e.g. References D and E). Specific details are therefore not given in this Annex other than to state that in the early stages of an operation designs should be constructed in accordance with the specifications at Appendix 1 and that the structural elements should be sufficient to meet the

AD 80-25

current and predicted threat. Further details to inform the MMR are given below and in the Overwatch Para in Appendix 3.

f. **Security Lighting.** Lighting can be utilised to enhance detection and deterrent effects on the perimeter or interior of a facility. However, it can also render other NATO night surveillance equipment less effective, as well as assist enemy forces in detection, and therefore it does not always provide the optimal solution. The FP team on the ground will need to make an assessment of the advantages and disadvantages before its use is confirmed. Further details of the MMR for such enhancements are given at Appendix 2.

g. **IDS and CCTV.** It is possible to enhance the 'detect' and 'deter' effects through the use of remote sensors such as CCTV / IDS. Whilst costly in the first instance, such systems can save manpower costs and deliver enhanced capability over and above that of the naked eye. In situations where the threat level demand, further details on the MMR are given at Appendix 2.

8. **Blast and Ballistic Protection.** When considering how to minimise the effects of blast and ballistics (or fragmentation) the measures given above should be considered in sequence as shown below.

a. Blast protection is achieved through, in priority order:

- (1) Standoff;
- (2) Control;
- (3) Cordon & Canalise; and
- (4) Protect the target (sand/water) – Compartmentalize.

b. Ballistic Protection is achieved by denying line-of-sight threats in priority:

- (1) Deny surveillance and target acquisition;
- (2) Deny the firing point;
- (3) Protect the target (gravel/steel/sand).

NB Compartmentalisation mitigates effects of both blast and ballistics.

9. **Construction Concept.** The overarching construction concept should aim to deliver the following:

- a. Synergy of infrastructure, equipment and personnel/procedures;
- b. Dispersion, Deception and Duplication;

AD 80-25

- c. Reaction time and standoff;
- d. Compartmentalization.

INFRASTRUCTURE MILENG CATEGORISATION

10. In order to prioritise the MilEng effort it is advisable to categorise the infrastructure across the FSB/FOB. Categories of fixed infrastructure on NATO facilities are:

- a. **MilEng Category 1 – Operationally Essential Infrastructure.** That infrastructure which, if destroyed would render NATO operations from the facility non-effective (e.g. Ops Room, Runway).
- b. **MilEng Category 2 – Key Supporting Infrastructure.** That infrastructure which, if destroyed would erode NATO operational capability in the facility but not cause operations to cease (e.g. Accommodation Block, DFAC).
- c. **MilEng Category 3 – Secondary Infrastructure.** That infrastructure which, if destroyed would erode NATO's operational activity through the negative effect on the surrounding populace, (e.g. pollution hazard, sewage farm).

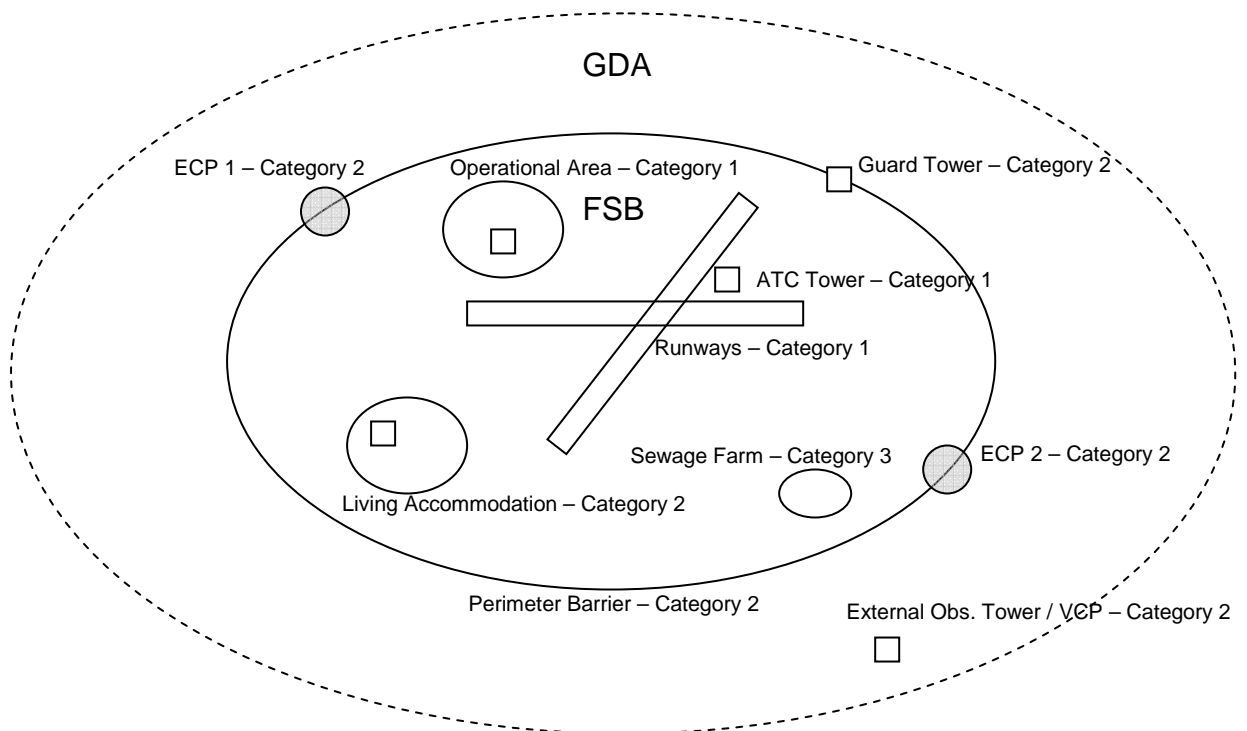


Figure 3 - NATO Facility, Physical FP Categorisation

LINKING THE DEFINED THREAT TO A DEFINED LEVEL OF MILENG MEASURES

11. Once the Threat Assessment has been carried out, and the threat level³ known, it is possible to define the minimum level of MilEng measures required for each piece of infrastructure on the facility. The table below links the *overall* threat level directly to a level of MilEng measures required. The simple matching of the threat level⁴ with the Category of infrastructure gives the guideline MMR MilEng Level. The structural form required for each MilEng Level has been subsequently defined in each of the relevant Appendices attached with this Annex.

NATO Threat Environment ⁵	NATO FP Level ⁶	MilEng Level		
		(Category 1 Infrastructure)	(Category 2 Infrastructure)	(Category 3 Infrastructure)
LOW	5	1B	1A	0
MEDIUM	4	2B	1B	0
SIGNIFICANT	3	2B	2A⁷	1A
HIGH	2	3	2B	1A
	1	3 (Post attack)	3 (Post attack)	2 (Post attack)

Figure 4 – Defined MilEng Level

12. Within the overall layered approach to security of the facility, the perimeter delineation itself must be of a standard that it can withstand an attack without NATO personnel within the facility becoming casualties, nor mission essential NATO equipment being rendered inoperable. Dependent on the terrain / layout, the use of cover from view, berms, fences, IDS, CCTV, routes and standoff is to be made as appropriate to ensure this requirement is met. Where an observation or guard tower is constructed it should as a minimum provide protection from SAF (Threat Category A3). If the tower is vulnerable to a higher level of threat then the requisite level of protection should be provided (i.e. where a tower is adjacent to a public road and a Significant VBIED threat exists then the tower should be protected against both fragmentation and blast effects.) Appendix 2 gives further technical criteria for perimeter protection.

³ In the form of a known standard NATO definition.

⁴ Note, where a specific threat type exists with a higher level than the overall threat level (e.g. overall threat MEDIUM but IDF threat HIGH) then the overall threat level should be used. Once the MilEng Level is defined, the design can then be refined to ensure the provision of specific protection measures to meet the specific threat which is considered to be higher.

⁵ As defined in AJP 3.14 Para 0203.

⁶ As specified in AJP 3.14 – Annex C. To be used in the absence of an overall specified Threat Environment.

⁷ Note for Perimeter Barriers and ECPs, MilEng level 2B applies.

DEFINING THE MILENG LEVEL DESIGN REQUIREMENTS

13. Once the initial assessment has been carried out (as outlined above) it is necessary to further define the Engineering requirements based on the weapons threat that it is assessed could be employed. The Appendices attached to this Annex give further guidelines. The NATO standard weapons threat table is given in STANAG 2280 (Reference C) Annex A. This table can be adapted to indicate for each weapon category the level to which it is assessed the enemy is likely to be able to employ and therefore to further refine the design specification of the MilEng measure to be employed⁸. The effects fall into two main categories, blast and fragmentation, and dependent on which is the greater links directly to the measure employed. Where the blast threat is high (e.g. large IED), and the proximity low, consideration must be given to the use of specialist blast mitigation structures.

14. The Threat Assessment will dictate the FP Level required (NATO FP Levels 1 – 5 as specified in Annex C to AJP-3.14). The Threat Environment will differ across theatre and therefore each facility must have its own unique Threat Assessment conducted. Once the threat level is known (current and future predicted) this Annex indicates the level of MilEng measures that it is appropriate to put in place as part of the overall layered FP plan.

An example of a MilEng MMR design threat is given below:

Baseline/Statistical threat (construct to meet this):

VBIED 350 kg TNT equiv / IDF 107mm rocket (NATO Threat Category E2/C4)

Full/Design threat (plan / design to meet this, i.e. structure capable of being upgraded to meet this threat in the future):

VBIED 1,000kg TNT equiv / IDF 122mm rocket (NATO Threat Category E3/C5)

15. The principle is to design to accommodate the full/design threat, but construct to accommodate the baseline/statistical threat, with the use of active measures to quickly meet rising threats on a local or site by site basis. Only in circumstances where MilEng infrastructure is not deliverable in a quick enough timeframe to meet the rising threat should a construction standard over and above the Baseline Threat be considered, normally provided through the NATO CUR delivery process (as outlined in Reference B).

⁸ This process is known as Measure Evaluation and involves the selection of the optimum construction solution based on an analysis of the range of protection measures available balanced against cost. It is a JEng led process that is not covered further in this document.

AD 80-25

USE OF SOFTWARE TO MODEL THREAT EFFECTS

16. A wide variety of different software exists, within individual member nation resources, to model the blast and fragmentation effects of various kinetic threats⁹. Such software provides a useful tool for estimating the effects of enemy weapon threats against existing structures and in justifying additional recommended MilEng measures. Its use should be considered in supporting the staff led risk assessment process and in assuring the risk owner that the correct MilEng MMR has been defined.

SUMMARY

17. In summary, MilEng measures provide an essential element to the overall FP plan. Full integration is essential and MilEng must be considered as part of the Threat and Vulnerability processes. The MilEng MMR must be defined and refined throughout the FP risk assessment process as a continual cyclical process. This Annex and supporting Appendices provide the necessary framework in which this is to be achieved.

APPENDICES¹⁰:

1. MilEng Design Guideline - Early Stages of a CRO.
2. Standard Perimeter Constructs for NATO facilities on CROs.
3. Standard Layout and Protection for Entry Control Points.
4. Standard Physical Protection Levels for Buildings within NATO facilities on CROs.

⁹ NB. At the JFC level 'AT Planner' software is used. (Blast effects modelling software developed by the US Army Engineer Research and Development Centre).

¹⁰ Elements of the material used in these Appendices have been sourced from UK Mil Engineering Vol. IX Part 1 – Force Protection Engineering.

MILENG DESIGN GUIDELINES FOR USE IN THE EARLY STAGES OF AN EXPEDITIONARY OPERATION

1. In the early stages of a CRO, expediency is likely to be the driving factor in implementing MilEng measures. As a guideline, the following generic design criteria are to be set when delivering MilEng measures in the early stages of an operation:

Se r	Criteria	Remarks
(a)	(b)	(c)
1	Matched to the threat	The structures are designed to be as light and simple as possible to match the <i>design threat</i> , but have the space/fittings to allow incremental increases in protection. Protection is expressed in terms of a series of incremental threat levels. These are given in Appendix 1 and are broadly compatible with STANAGs 2280 and 4184. Threats have been broken down into categories and appropriate distinguishing criteria selected within each category.
2	Basic protective design	All structures must comply with the protective engineering techniques laid down in Reference D/E or the appropriate equivalent standard. In particular, should they fail, they must do so safely without significantly increasing the hazard to personnel.

NATO RESTRICTED
Releasable to PfP

AD 80-25

Ser	Criteria	Remarks
(a)	(b)	(c)
3	Easily assembled	<p>Ideally (but not essentially) they can be erected without the need for plant.</p> <p>Any plant that is required is assumed to be that available to an Engr Sub-Unit from its own organic resources:</p> <ul style="list-style-type: none"> a. Crane: e.g. Coles 315M (Liebherr1030/2 Grove 3020 or Terex Demag AC30 post C vehicle PFI) b. LWT: e.g. JCB 4CX. c. SLDT: e.g. Volvo FL12 – with loading arm. d. MWT: e.g. Case 721. <p>Fabrication possible in a Deployable Engineer Workshop (DEW) and Deployable Machine Shop (DMS):</p> <ul style="list-style-type: none"> a. Steel sheet size: 8 m x 4 m x 5 mm (note 10 mm is a preferable size for protection therefore the capability of DEW will be reviewed). b. Maximum steel section size: 150 mm (based on capacity of reciprocating saw). c. Bolt size: 32 mm (maximum drill size), 20 mm preferred (maximum punch size tbc). d. Maximum timber bulk: 200 mm x 200 mm (based on capacity of circular saw).
4	Reasonable worst case site conditions	<p>Effective wind speed (V_e): 50 m/s. This equates to a reasonably exposed site.</p> <p>Ground bearing capacity: 100 kN/ m². This equates to medium dense sand or firm clay.</p>

NATO RESTRICTED
Releasable to PfP

AD 80-25

Ser	Criteria	Remarks
(a)	(b)	(c)
5	Reasonable availability of materials	<p>Aggregate: Fine grained silty sand 1.8 t/ m³. Denser aggregate is not assumed for protection purposes however 2 t/ m² assumed for deadload.</p> <p>Concrete: Grade C30 (4350 psi). This grade of concrete is readily achievable using hand batching with supervised but relatively unskilled labour. Higher quality concrete not assumed.</p> <p>Steel: Grade 43 (S275) "mild steel". Higher grade steels are harder to obtain, more difficult to work and are almost impossible to verify in the field. Higher quality steel not assumed.</p>
6	Adaptable to the environment	Options for environmental protection (Sun, rain, wind) should be incorporated as an upgrade to the basic structure where practical.
7	Transportation	<p>Wherever possible the components to be "flat packed" to site and bulk/mass derived from locally won material.</p> <p>Any pre-assembled items must be compatible with DROPs or NATO equivalent transportation: Max weight: 12.5 t Max width: 2.8 m</p> <p>All components must fit into a 20' ISO container; (< 5.2 m long)</p>

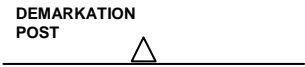
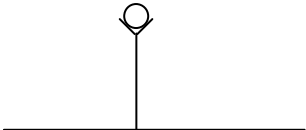
NATO RESTRICTED
Releasable to PfP

AD 80-25

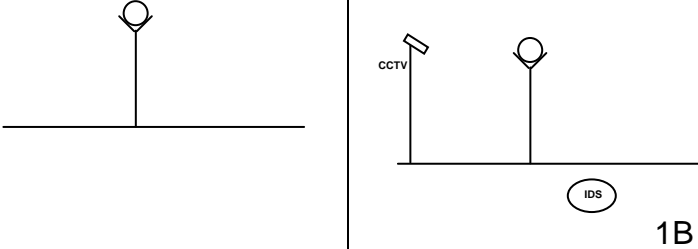
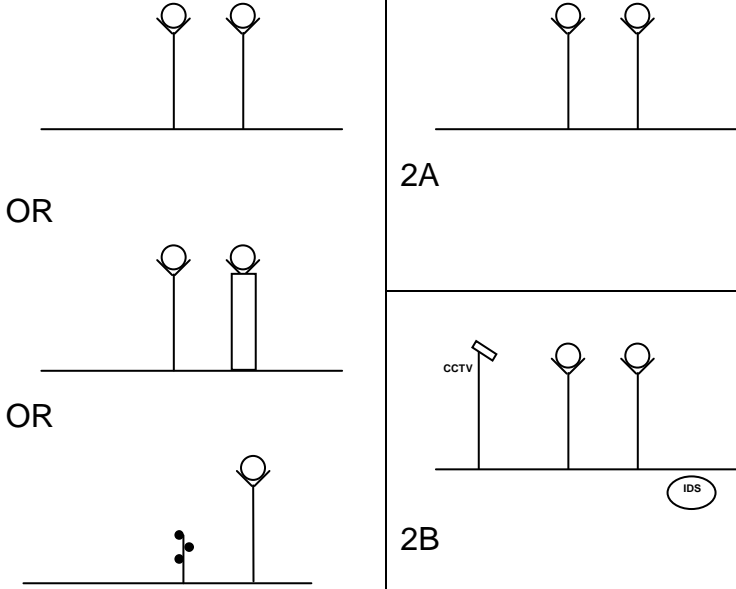
I1-4
Releasable to PfP
NATO RESTRICTED

LEVEL OF INFRASTRUCTURE PROTECTION – PERIMETER BARRIERS

1. The Table below highlights the Level of perimeter protection for NATO facilities on a CRO.

MilEng Level	Structural Form of Perimeter Barrier	Description
Level 0	 <p>DEMARKATION POST</p>	<p>No Perimeter barrier in place. As a minimum, the perimeter must be clearly demarcated on the ground to ensure all parties are clear on the ground considered as NATO operated. As far as possible, the perimeter must be positioned so that it can be easily covered by sight and fire from within the confines of the facility, as well as be easily accessible by wheeled vehicle. The perimeter must pass across ground on which Infrastructure can easily be placed at a later stage without undue disruption to the continued operational function of the facility.</p>
Level 1	 <p>1A</p>	<p>Form: Single barrier (fence only). Dependent on surrounding environment (i.e. rural / urban) cover from view screens can be fitted in areas where required. See below for further detailed specifications.</p> <p>Protection: Protects against entry by foot only. The barrier</p>

AD 80-25

MilEng Level	Structural Form of Perimeter Barrier	Description
		<p>achieves a deter / delay effect only.</p> <p>Construction: See below for further details.</p> <p>A – Fence Only.</p> <p>B – Fence enhance with centrally controlled IDS / CCTV system.</p>
<p>Level 2</p>		<p>Form: Double barrier (fence / wall or double fence). The selection of the secondary barrier type is dependent on the surrounding environment (i.e. rural / urban) and therefore the proximity of the enemy threat. Three examples are shown, being second fence, outer layer blast wall and inner layer cable and bollard system. Cover from view screens should be fitted in areas where required (i.e. enemy over-watch possible). Where a wall/screen is used a method of observation beyond the perimeter must be in place (i.e. watch towers at mutually supporting intervals). See below for further detailed specifications.</p> <p>Protection: Protects from entry by foot and offers limited protection from vehicle access. Degree of protection depends on actual measures used.</p> <p>A – Double Barrier Only.</p> <p>B – Double Barrier enhance with centrally controlled CCTV / IDS system.</p> <p>Construction: Time and cost vary depending on solution</p>

AD 80-25

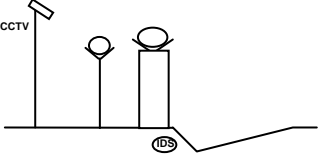
MilEng Level	Structural Form of Perimeter Barrier	Description
		and whether retrofit or new-build. Note if required cover from view panels should be fixed to the external fence.
Level 3		<p>Form: Triple barrier fence / berm, or double fence with physical presence on perimeter (towers / standing patrols / dogs). Enhance with watch towers, and CCTV / IDS as a standard. Bund and wall must be of a standard to block design VBIED threat both from vehicle entry and blast effects.</p> <p>Construction: More expensive (x5) lengthy build-time (x2).</p>

Figure 1 – Design MilEng Level for perimeter barriers.

2. **Perimeter barriers.** When developing plans for the provision of perimeter barriers, the following principles should be adhered to:

- a. Barriers should be emplaced in concert with each other, the natural terrain, and any man-made obstructions.
- b. Combinations or layers of barriers are more effective than a single barrier in high-threat environments.
- c. If used in combinations, barriers must afford an equal degree of continuous protection along the entire perimeter of the facility.
- d. Combinations or layers of barriers should be separated by a minimum of 10m for optimum protection and control.

AD 80-25

- e. When a section or sections of natural/man-made barriers provide less than optimum protection, other supplementary means to detect and assess intrusion attempts should be used.
- f. Barriers should be augmented by security force personnel or other means of observation and assessment. An unobstructed area or clear zone should be maintained on both sides of and between physical barriers.
- g. Barriers should be positioned far enough away from other structures (trees, telephone poles, antenna masts, or adjacent structures) that may be used as aids to circumvent the barrier.
- h. Barriers should not be placed where vehicles can park immediately adjacent to them, thereby affording attackers a platform from which to mount an attack.
- i. Additional toppings on barriers should be considered. These include concertina wire, multiple-strand razor or barbed wire, or other devices that inhibit enemy efforts to vault or go over the top of the barrier.
- j. Barriers should be considered as excellent platforms on which to mount surveillance systems and intrusion detection devices.
- k. For MilEng Level 2 or above, temporary walls or rigid barriers should be considered in areas where vehicles can approach the perimeter unhindered. They deny access and protect against high-speed vehicle penetrations. Types of materials for consideration include:
 - (1) Concrete barriers (Jersey, Texas, Alaska, "Bitburg" barriers)
 - (2) Concrete or sand-filled oil drums
 - (3) Concrete bollards or planters
 - (4) Steel or steel-reinforced concrete posts
 - (5) Sand or water-filled plastic vehicle barriers

AD 80-25

(6) Earth-filled barriers (HESCO™ bastions, metal revetment)

- l. The potential for debris and fragment hazard should be considered when concrete barriers are used; soil-backed concrete barriers help to mitigate debris and fragments.
 - m. Vehicles in all sizes and configurations should be considered as expedient barriers. Parked bumper-to-bumper, vehicles provide an effective barrier to personnel. Large construction-type vehicles or armoured vehicles (including destroyed and captured enemy vehicles) can be very effective as supplemental barriers behind gates to facilities or as a temporary serpentine in entry control points.
 - n. Barriers installed in clear zones must be designed so that they do not provide terrorists with a protective hiding place or shield.
 - o. Perimeter barriers should be kept under observation and patrolled frequently.
 - p. The placement of barriers should maximise standoff; for example, perimeter barriers should be located as far from critical assets as possible to mitigate blast effects.
 - q. Barriers should be fully integrated to form a continuous obstacle around the facility, capable of stopping possible vehicle borne threats where they exist. In many instances when a single barrier cannot stop a vehicle, a combination of barriers can.
 - r. Barriers, sensors, and final protective and overwatch fires should be integrated and should fully support each other.
 - s. Barriers can be compromised through breaching (i.e., cutting a hole through a fence) or by nature (i.e., berms eroded by the wind and rain); therefore, barriers should be inspected and maintained routinely.
 - t. Barriers at the perimeter can help conceal and shield facility activities from direct observation and surveillance.
 - u. Man-made perimeter barriers can assume a wide range of forms, to include fences, walls, ditches, berms, barricades, and vehicle barriers (active and passive). Perimeter barriers are further distinguished as either antipersonnel or anti-vehicular.
3. **Anti-personnel Barriers.** These barriers aim to protect against infiltrators who may try to place small explosive charges, tamper with supplies and equipment, or attack friendly personnel or critical assets once they are inside the facility. However antipersonnel

AD 80-25

barriers can only realistically deter and delay an enemy attack. Typical antipersonnel barriers include chain link fences with barbed wire outriggers, triple-strand concertina fences, wire obstacles, concrete walls, and barbed wire fences. In most instances, antipersonnel barriers can be penetrated by the enemies' climbing over them or using wire cutters. Consequently, antipersonnel barriers must remain subject to constant observation/patrolling. There are many options for fencing material; however, the most commonly used are:

- a. **Triple-strand Concertina Fence.** Triple-strand concertina fences are easy to set up and can be rapidly emplaced by unskilled labor. Triple-strand concertina fences can be breached by an intruder's cutting the wire, disassembling the fence, or flattening down the concertina with a board or similar object. A poorly constructed concertina fence (i.e., one with no horizontal support wire) is especially susceptible to the latter two methods. The most common mistakes security forces make in constructing concertina fences are spacing engineer stakes too far apart, not using intermediate short pickets, stretching the concertina so the gaps between the wire are too large, neglecting to add horizontal wire, and failing to tie the concertina together.
- b. **Chain Link.** Chain link fence (see Figure 2 below) is very common and widely used. The main advantage of this form of fencing is the minimal cost; however, it has many drawbacks. The fencing fabric is easy to climb because of its diamond shape. It is susceptible to single cut penetration and, while it can support PIDS, its lack of robustness makes it prone to false alarms. This form of fencing should ideally only be used for demarcation as it offers very little deterrence or delay to an intruder when used in isolation. Where used it should be enhanced with razor wire as shown in Figure 2 below and constructed to the minimum standard shown in Figure 3 below.

AD 80-25



Figure 2 - Metal mesh fence with razor wire and barbed wire outriggers

AD 80-25

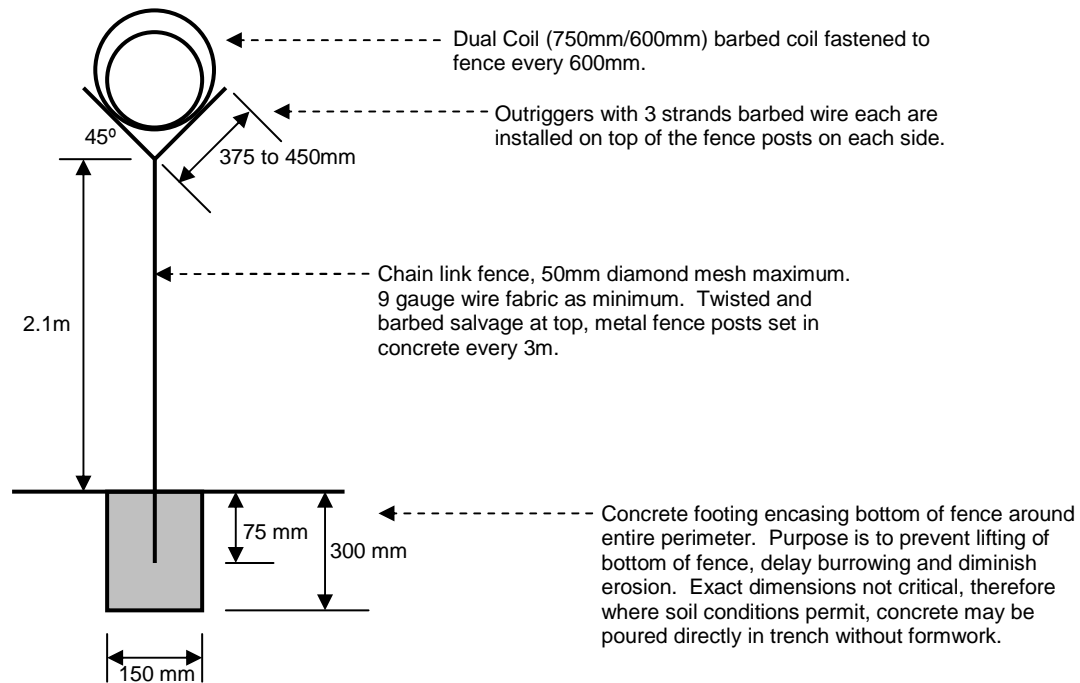


Figure 3 - Diagram of Chain Link Fence (MilEng Level 1 standard).

c. **Others (including Expanded Metal Mesh and Steel Profile Fencing).** Expanded metal fence is a type of 'anti-intruder fence' and is well suited to securing a perimeter. Unlike the chain mail fence, it does not have ready footholds, which makes climbing difficult; it is also resistant to cutting. The disadvantage of this form of fencing is that its thickness makes it prone to blind spots. Steel profile fencing has the advantage of not having any footholds, which makes vertical breaching difficult. It can also offer a screen and limit visibility and is very noisy to penetrate. As the fence is a sheet, it is susceptible to wind loading and, while it provides cover from view, it does not allow view of the outside of the perimeter from inside the fence.

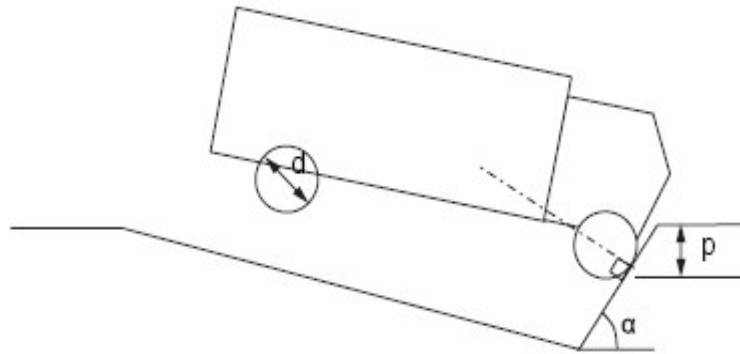
d. **Anti-personnel barriers best practice.** The following guidelines meet the MMR design specification for a MilEng Level 1 barrier:

AD 80-25

- (1) Fences should not be located so that terrain features or structures (buildings, utility tunnels, light and telephone poles, ladders, etc.) allow passage over, around, or under them.
- (2) Chain link and metal mesh fences should be anchored with metal posts placed in concrete at intervals no greater than 3m.
- (3) Fences should be topped with razor wire, general purpose tape obstacle (GPTO), barbed concertina wire, or barbed wire outriggers (listed in order of most effective to least effective).
- (4) Fence height, including outriggers, should be a minimum of 2.5m.
- (5) Horizontal wire should be laced along the bottom and top of the fence to keep the edges rigid.
- (6) The bottom edge of the fence should not rise above the ground level. The preferred installation method makes use of a concrete footing that encases the bottom of the fence around the entire perimeter. This method prevents an intruder from lifting the bottom of the fence, delays him from burrowing under it, and diminishes erosion.
- (7) A synthetic screen can be woven into the fence to prevent observation of the facility, but care should be taken to ensure that the screen does not also block observation from within.

4. **Anti-vehicle Barriers.** Anti-vehicle barriers are designed to deter personnel in vehicles from entering a facility by force. Solid barriers such as the US 'Jersey' barrier, a pre-cast concrete barrier, are commonly used to stop vehicles. Ditches and even barbed wire may stop a vehicle, depending on its size and speed. Unless the threat is from a tracked vehicle, standard antitank ditches should be avoided as they may be lethal to the occupants of a car or light vehicle in the event of an accident. This Annex concentrates on the threat from fast-moving civilian vehicles rather than tracked or armoured ones. A number of options exist as follows:

- a. **Anti-vehicle Ditch.** The optimum ditch profile is an asymmetric 'V' as shown in Figure 4 below. Typically, it should be at least 5 m wide and around 1.2 m deep. Other ditch profiles may also stop vehicles but they have not been tested. Trapezoidal ditches should be avoided as a vehicle may be able to drive in and out, albeit at an angle to the ditch. The design of the approach leading to the ditch is at least as significant as the ditch shape itself. Every effort should be made to limit the speed at which the vehicle approaches the ditch. This can be achieved by using such a ditch in combination with other vehicle delaying techniques below.



Vehicle will probably be stopped if:

- Depth of drop (p) is greater than 75% of wheel diameter (d).
- Slope angle α° makes vehicle strike bank at 90° .
- Ditch is at least 2 m wide.

Serial	Speed (mph)	Impact bank slope ' α ' (degrees)				
		Ditch width				
		2 m	3 m	4 m	5 m	6 m
(a)	(b)	(c)	(d)	(e)	(f)	(g)
1	10	46	34	-	-	-
2	20	76	70	63	-	-
3	30	84	81	78	75	72
4	40	87	85	83	81	80
5	50	-	87	86	86	84

Serial	Speed (mph)	Vehicle front wheel drop 'p' (mm)				
		Ditch width				
		2 m	3 m	4 m	5 m	6 m
(a)	(b)	(c)	(d)	(e)	(f)	(g)
1	10	1000	2260	-	-	-
2	20	280	550	1050	-	-
3	30	120	250	470	730	1050
4	40	70	150	260	390	600
5	50	-	100	170	260	380

Figure 4 - Diagram of Anti-vehicle Ditch (MilEng Level 2/3 standard).

AD 80-25

b. **Berms.** Berms can be used to effectively stop vehicles from penetrating the facility perimeter. Native soils and rock can also be effective in explosive blast / fragment mitigation since they have the ability to absorb large amounts of kinetic energy. Excavated soil can be placed on the protected bank of the ditch to increase its height. However, a berm reduces the field of view for the guard force. It may be more effective to use the spoil to form moguls. A suitable berm profile is shown in Figure 5 below.

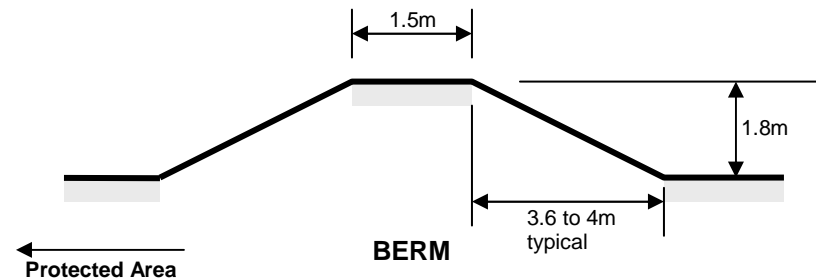


Figure 5 - Diagram of Anti-vehicle Berm (MilEng Level 2/3 standard).

c. **Random Boulder Field.** A field of randomly placed, 400 mm diameter boulders spaced no more than 2 m apart helps to reduce speed. They should be used in a field 2 m from the ditch and no less than 6 m deep. Randomly aligned timber baulks 400 mm in diameter can be used in place of, or with, a random boulder field.

d. **Moguls.** Moguls, uneven earth mounds 1 m high, can be used in a field at least 6 m deep. Spoil excavated from the ditch is ideal for this purpose. Placed around 1 m to 2 m apart, not only do they slow an attacking vehicle, but they also make it very difficult for it to cross the ditch at right angles.

e. **Ploughed Land.** Ploughed and furrowed land limits the speed of some vehicles. It is unlikely to affect off-road vehicles significantly.

f. **Arrester Bed.** Aggregate arrester beds are used on roads with long steep gradients to stop runaway vehicles. Although not advised for long stretches of perimeter protection, arrester beds can be used to prevent bypass of a control point. To stop a vehicle travelling at 40 mph, a bed 45 m long and 450 mm deep is used. The quality of its aggregate is critical. Clean, smooth,

AD 80-25

uncrushed, hard, natural gravel with a nominal diameter of 5 to 10 mm is used. Arrester bed material must be free draining, especially where there is a risk of freezing.

5. **Perimeter Lighting.** Security lighting serves a number of functions. It should be considered where MilEng Level 1 or above applies. It creates a sense of uncertainty in an intruder, protects the guard force and helps identify and stop an intrusion. As with all security enhancement equipment, it is vital that the system design is closely coordinated with all the other in place security systems and procedures. Security lighting can make an important contribution to physical security but, to be effective, it should be used in association with guards or detection systems, or both. If incorrectly applied, it can assist intruders more than the guard force. Ideally, security lighting should:

- a. Allow guards to see intruders before they reach their objectives.
- b. Conceal the guards from intruders while avoiding the creation of shadows that can offer concealment.
- c. Deter intruders or hinder them in their purpose.
- d. Enhance, and not diminish, other detection aids such as night vision equipment.

There are a number of perimeter lighting techniques as follows:

a. **Perimeter lighting.** Perimeter lighting provides the illumination of a well-defined strip around the protected site, through which an intruder must pass. The ability and speed of detection of an intruder in the protected zone is critical. Ideally, the area immediately outside the fence line is illuminated and the area inside the fence is not. This provides clear vision through most types of fence and allows the guards to detect intruders who may be attempting to defeat the barrier system. It is difficult to achieve in practice and often lights are placed further back to create a sterile zone inside the fence line. Figure 6 below illustrates this:

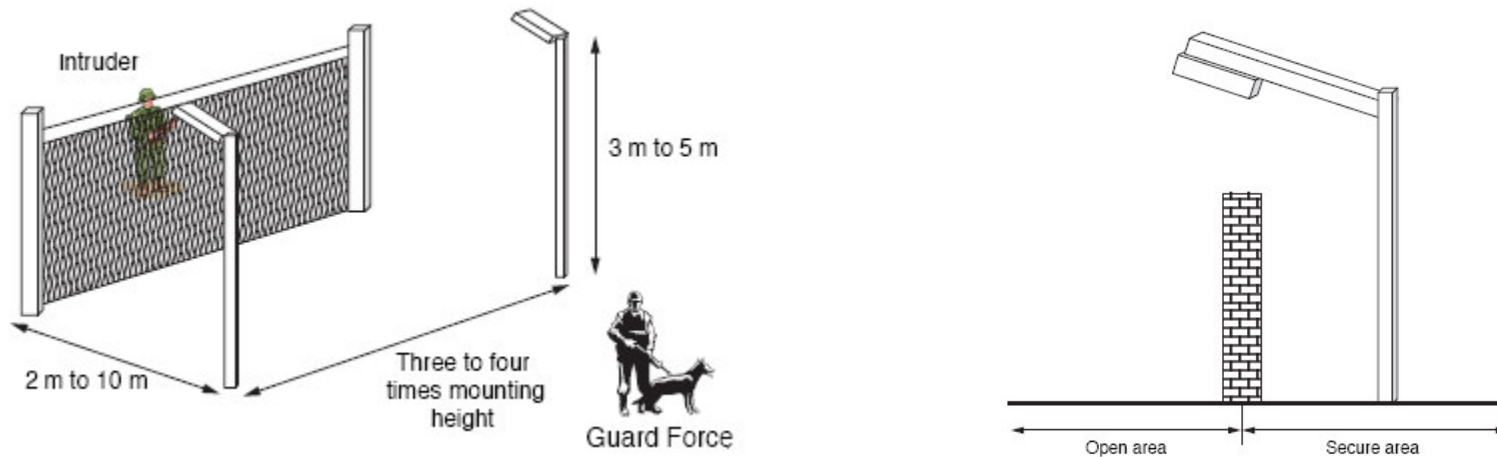


Figure 6 – Typical Perimeter Lighting Profile.

Detailed specifications for perimeter lighting are as follows:

- (1) Lighting columns are placed 2 m to 10 m from the fence and mounted around 3 m to 5 m high. They are spaced between three and four times the mounting height apart (see Figure 6 above).
- (2) Lighting columns may have extended outreach arms holding the luminaries closer to the line of the wall or beyond, or be aimed at a point some 10 m to 25 m beyond the perimeter (see RH side of Figure 6 above).
- (3) If used with CCTV, the horizontal luminance and colour rendering must be correct.
- (4) A uniformity of 3:1 is recommended with an emergency default of 10:1 on the loss of luminaries. Generally, perimeter schemes are specified between 2 lux and 5 lux over the protected area.
- (5) This type of lighting usually has an inherent re-strike time and the provision of a no-break supply is often very expensive.
- (6) Running costs, in comparison with other systems, are very low.

AD 80-25

- b. **Glare lighting.** Glare lighting is installed slightly inside a security perimeter and directed outward. It is considered a deterrent to a potential intruder because it makes it difficult for him to see inside the area being protected. It also protects the guard by keeping him in comparative darkness and enabling him to observe intruders at considerable distance beyond the perimeter.
- c. **Motion-Activated Lighting.** Motion-activated lighting can be very effective in deterring intruders as it is turned on by the intruder's movement into a protected area. Its use should be considered around areas of the perimeter close to Category 1 infrastructure.
- d. **Perimeter Lighting Best Practices.** To be effective, installed security lighting should accomplish the following:
- (1) Provide adequate illumination or compensating measures to discourage or detect attempts to enter the facility or restricted areas and to reveal the presence of unauthorized persons within such areas.
 - (2) Avoid glare that handicaps security force personnel or is objectionable to air, rail, highway or navigable water traffic.
 - (3) Direct illumination toward likely avenues of approach and provide relative darkness for patrol roads, paths and posts. To minimize exposure of security force personnel, lighting at entry points should be directed at the gate and the guard should be in the shadows. This type of lighting technique is often called glare projection.
 - (4) Illuminate shadowed areas caused by structures within or adjacent to restricted areas.
 - (5) Provide overlapping light distribution. Equipment selection should be designed to resist the effects of environmental conditions, and all components of the system should be located to provide maximum protection against intentional damage.
 - (6) Avoid drawing unwanted attention to restricted areas.
 - (7) Be expandable so that future requirements of electronic security systems (i.e., CCTV) and recognition factors can be installed. Where color recognition will be a factor, full-spectrum (high pressure sodium vapor, etc.) lighting vice single color should be used.

AD 80-25

(8) Use lights that illuminate the ground or water but not the air above. These lights must penetrate fog and rain.

e. **Lighting Considerations for Guardhouses / Guardtowers.** Exterior lighting for sentry booths and guardhouses should be designed to minimize exposure of security personnel. "Glare protection" lighting is directed at the gate while the guardhouse remains in the shadows. The interior lighting in the guardhouse should be diffused lighting designed to aid night vision and provide additional security to the occupants. Night light units with a red lens enhance the occupant's night time vision. Guardhouses should have a standby power source.

AD 80-25

6. **Intrusion Detection (IDS) and Surveillance Systems**{ TC "Intrusion Detection (IDS) and Surveillance Systems" \f H \l "9" }. IDS systems can be used for MilEng level 1 and above and must be included where MilEng Level 3 applies. The function of perimeter IDS is to detect a threat and initiate a response by security personnel. Relying on perimeter IDS involves inherent risks. In high-threat environments security personnel cannot rely solely on IDS. Rather, IDS should be an essential part of an integrated and layered approach to facility force protection. There are a wide variety of IDS systems available, as illustrated in Figure 7 below.

Serial	Detector	Fence	Perimeter	Underground	Interior/ building	Key characteristics	False alarms/evasion
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
1	Vibration	Yes			Yes		Primitive variable control method. Fences need to be taut.
2	Shock	Yes					Fences need to be taut.
3	Linear shock	Yes					
4	Fibre optic	Yes		Yes			
5	PIR				Yes	1-40 m (internal) 15-100 m (external) Price £50 (internal) £120-600 (external)	Sensitivity decreases with distance and rising temperature. Background temperature can cause blind spot. Susceptible to wildlife and sunshine. Can be confused by distant hot objects.
6	Active IR	Yes	Yes		Yes	0.5-150 m. Price for 3 m tower - £1,700.	Best used in sterile areas with line-of-sight and effective alignment. Fog reduces sensitivity. Susceptible to ground undulations. Beams detectable and may be avoided.
7	Microwave - bi-static	Yes	Yes, line-of-sight required		Yes	Range 5-150 m (bi-static). Price £6,000.	Sterile areas optimum. Line-of-sight and effective alignment. requires flat ground. Dead zone requires cover. Metal objects can cause reflections.

AD 80-25

Serial	Detector	Fence	Perimeter	Underground	Interior/ building	Key characteristics	False alarms/evasion
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
8	Microwave – Doppler	Best for sterile areas	Yes		Yes	5-60 m (mono-static)	
9	Acoustic	Can detect climbing		Yes		25-150 m. Price £25/m.	
10	Pressure			Yes		25-150 m. Price £110/m.	Requires consistent ground type. Affected by nearby trees or roadways. Verification essential.

Figure 7 - Guide To Selection Of Perimeter Intruder Detection System (PIDS).

a. **Objectives of IDS and Surveillance Systems.** IDS are used to accomplish the following:

- (1) Permit more economical and efficient use of security personnel.
- (2) Provide additional controls at critical areas or points.
- (3) Enhance the security force capability to detect and defeat intruders.
- (4) Provide the earliest practical warning to security forces of any attempted penetration of protected areas.

b. **IDS Selection Considerations.** The requirement for an IDS must be identified and determined during the site selection and facility layout planning process. The IDS required cannot be completely identified until the proposed facility layout plan has been developed. A perimeter IDS designed to provide detection along a long perimeter may result in high system costs for installation, operation and maintenance. Regardless, the standard for selection of an IDS should be optimal performance achievable in local environmental conditions, such as soil, topography, weather, and other factors. These factors can adversely

AD 80-25

affect performance or increase false alarm (an alarm without a known cause) rates. Therefore, to ensure an effective system is selected, the performance parameters of the system should be primary concerns, including:

- (1) Completeness of coverage
- (2) False and nuisance alarm rates
- (3) Probability of detection
- (4) Zone at which the alarm occurred
- (5) Delay time

If the delay time is too low, then the time available for effective security force response may not be adequate. The relationship between perimeter sensor location, delay times, and security force response times must be carefully examined.

7. **Perimeter Surveillance using CCTV.** Though not as effective as direct observation, CCTV is often used to augment security forces when manpower is limited. Closed circuit television (CCTV) enables an area or target to be overtly or covertly observed from a remote location. A CCTV is most effective when it is linked to IDS and has a dedicated operator monitoring the system. CCTV cameras should have pan, tilt, and zoom capability to allow the operator to track suspicious activities, as well as a means of recording. A basic CCTV system comprises a camera and lens with a power source and lighting, a means of picture transmission to a monitor and a recorder. Systems are generally mains powered; though 12 volt and 24 volt DC equipment is available for vehicle or remote deployment. CCTV can make an important contribution to physical security in the following ways:

- a. Command and control of a large area from one or more remote locations.
- b. Provision of a high profile deterrent.
- c. Assistance to patrols by guidance, early warning, confirmation of reports, and provision of up to date situation reports.

Perimeter surveillance is achieved by overlapping the coverage of static cameras (see Figure 8 below). Cameras should, ideally, be positioned on the outside of any fences or other physical perimeter security measures to ensure any intruder is delayed for the maximum possible time in the camera view.

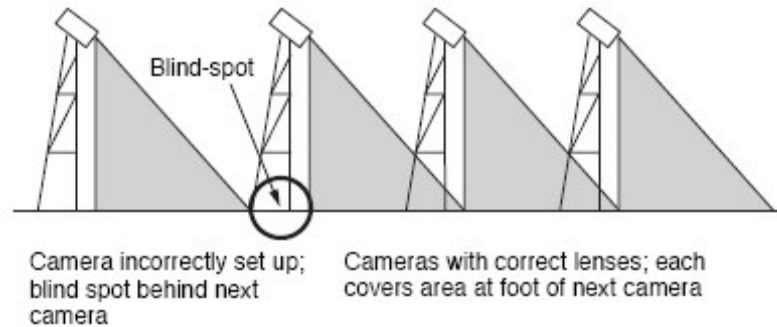


Figure 8 - Optimal positioning of CCTV cameras.

- d. **Statement of Requirement.** To select the most appropriate CCTV system, the designer should determine a clear statement of requirement as part of the planning process. It is essential that the process:
- (1) Identifies the role of the CCTV system in the overall security strategy and the priorities for implementation and operation.
 - (2) Provides a framework for collation and discussion of the views of all agencies and identifies conflicts of options in multi-agency systems.
 - (3) Defines relevant and realistic performance goals and acts as a reference point for system testing.
 - (4) Allows, at the outset, for the possibility of future expansion.

More complex systems can include telemetry control for remote operation and additional functions such as lighting, wipers, low light enhancement features, iris and focus control and audio. Systems can also incorporate video motion detection for automatic triggering of cameras or recorders on movement sensing. Multiple camera systems may have multi-screen displays via video switching, split screen displays via quads or splitters and multiplexing for recording multiple cameras on one recorder. Of note, even the most basic systems require some form of training for those intending to operate them.

AD 80-25

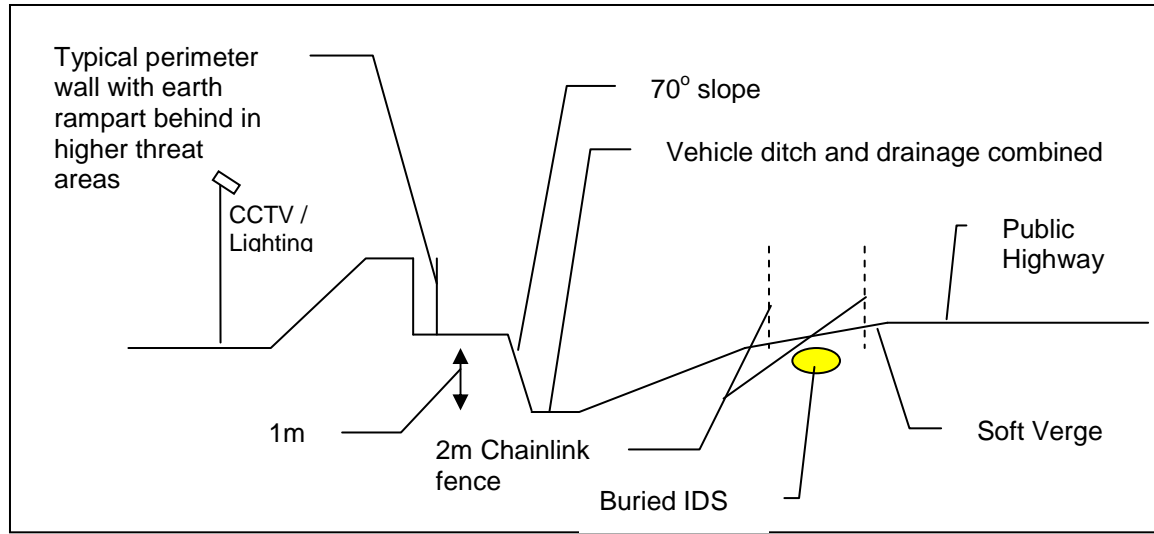


Figure 9 – MilEng Level 3, Possible Security Solution, Section Through Roadside Perimeter.

ENTRY CONTROL POINTS

1. All ECPs should be set out in such a way that they incorporate and demarcate each of the areas as shown on the figure below.

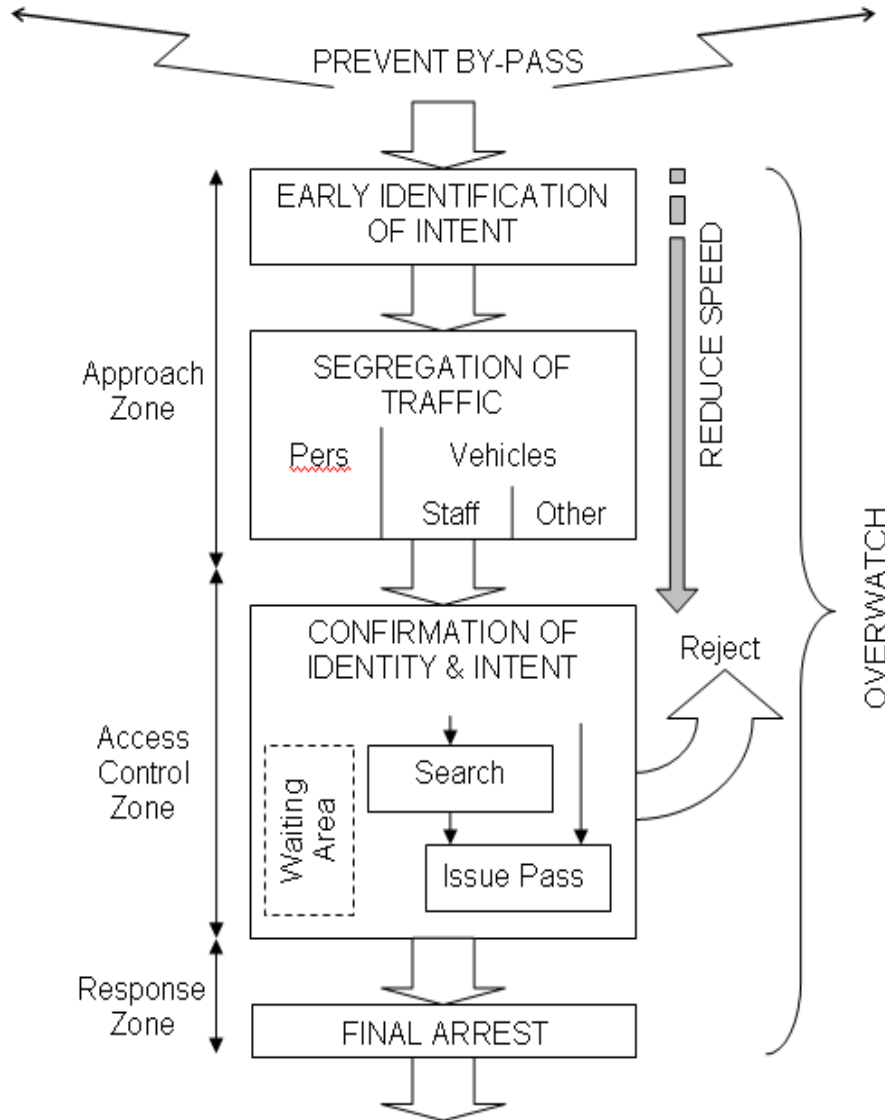


Figure 1 – ECP Concept Layout.

2. Examples of ECP layouts for each MilEng Level are shown in the next three diagrams. For MilEng Levels 1 and 2 there is a further delineation A and B. MilEng Levels 1B, 2B include automated personnel and vehicles search/scanning facilities.

AD 80-25

MilEng levels 1A and 2A do not. For MilEng Level 3 scanners are always in place. For the overwatch tower and building structures the design MMR for each MilEng Level is to follow guidelines as set out in Appendix 4.

3. **MilEng Level 0.** MilEng Level 0 is effectively a VCP provided by Troops and their vehicles alone, with no protective structures or fixed equipment in place. The layout of the VCP should make use of the maximum real estate available in order to maximise stand off of NATO troops from the threat.

4. **MilEng Level 1.** The diagram below shows a typical layout for a MilEng Level 1A design ECP.

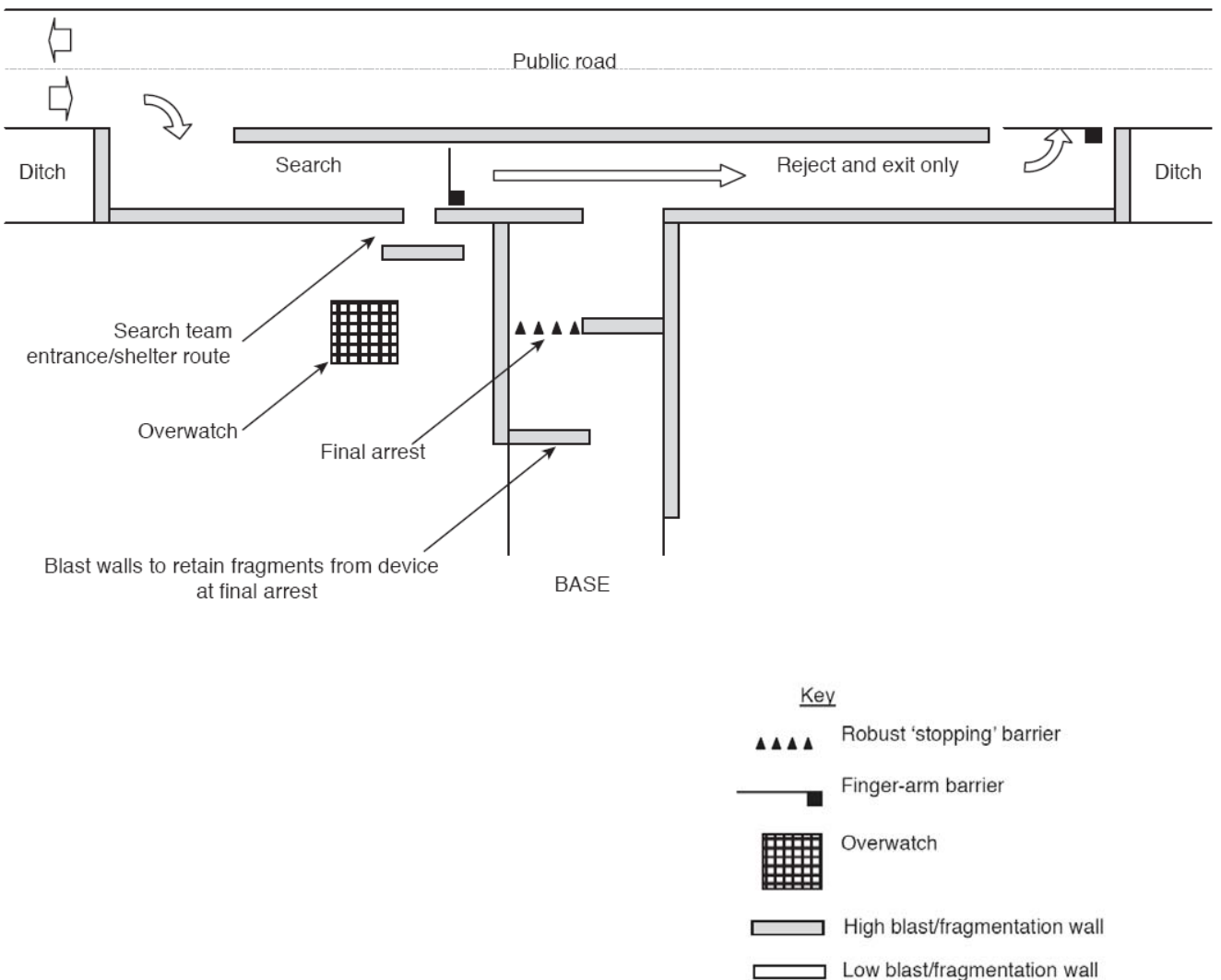


Figure 2 – MilEng Level 1A ECP Concept Layout.

AD 80-25

5. **MilEng Level 2.** The diagram below shows a typical layout for a MilEng Level 2B design ECP.

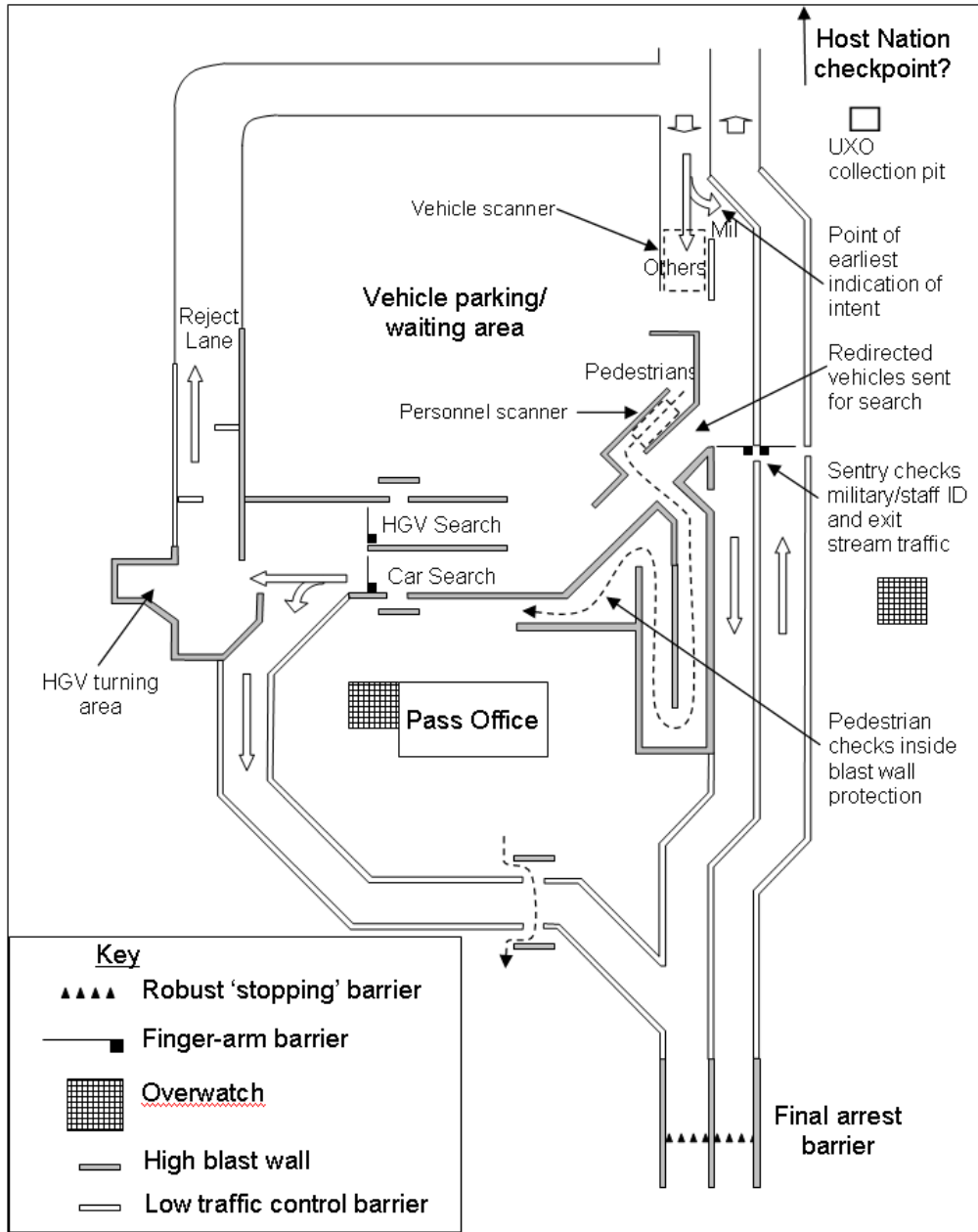


Figure 3 –MilEng Level 2B ECP Concept Layout.

6. **MilEng Level 3.** An ECP constructed to MilEng Level 3 should incorporate all of the facilities of MilEng Level 2B above. In addition, all demarcation barriers should offer

AD 80-25

full blast protection. All structures should be fully blast protected and all NATO operating personnel should work from blast protected structures making maximum use of automation technology to minimise the risk. Automated scanner facilities (vehicle and personnel) must be positioned in the Approach zone to maximise standoff.

7. **Operational Considerations.** Further ECP design considerations are as follows:

- a. **Risk Analysis.** Regardless of the Threat Level, effective access control is a primary requirement. A thorough risk analysis is therefore essential when planning every element of the ECP design.
- b. **Integration.** The design is to be fully integrated with the security facilities afforded to the facility. Existing and planned technology for the control of entry of both vehicles and personnel must be incorporated into the design.
- c. **Minimum Security Requirements.** The design of the principal access to the facility must provide the capability to conduct a full security check of all vehicles, equipment and personnel seeking access to the establishment.
- d. **Access Performance Requirement.** As a guideline, the ECP should be capable of processing a minimum throughput of 10 uncleared vehicles an hour to a maximum of 15 uncleared vehicles for limited periods. Additionally, the ECP must be capable of continuous processing of pedestrian access. The design of the ECP should afford the routine ingress of light tactical vehicles and commercial and civilian passenger vehicle up to 8 tons. The design of the ECP must enable security forces to conduct clearance of personnel and vehicles making deliveries to the facility. Under exceptional circumstances HGV access will be required. The design will separate high risk vehicles and pedestrians from low risk while providing separate identification and search corridors for each.
- e. **Security Clearances and Passes.** As the primary ECP for the facility, all levels of security clearances are to be catered for. The design must provide security forces with the facilities to implement all current and planned future equipment for the clearance and inspection of personnel seeking entry to the establishment.
- f. **Control Room.** The design should incorporate the ability for personnel to control the entry control point facility, with the ability to monitor activity and exercise effective control.
- g. **Fire.** Emergency egress must be possible with un-conflicted exit routes through the main gate. Similarly, emergency vehicles arriving at the main gate must be able to rapidly pass through the gate with reduced scrutiny. Occupants of the main gate must be able to evacuate to a safe muster point within the perimeter and the gate closed to all traffic, if necessary. The control room must

AD 80-25

hold the muster sheets for each building with a daily copy held in the operations centre.

h. **Management Issues.** Periodic testing of the facility and entry processes will be conducted in order to evaluate the continued integrity of the ECP function and of the performance of staff and equipment.

8. **Personnel Access Considerations.** Careful consideration must be made to minimise the threat to NATO and civilian personnel at the ECP. The design should maximise the dispersion and stand off available to personnel as well as provide adequate protection where they are vulnerable. The figures below illustrate available techniques:

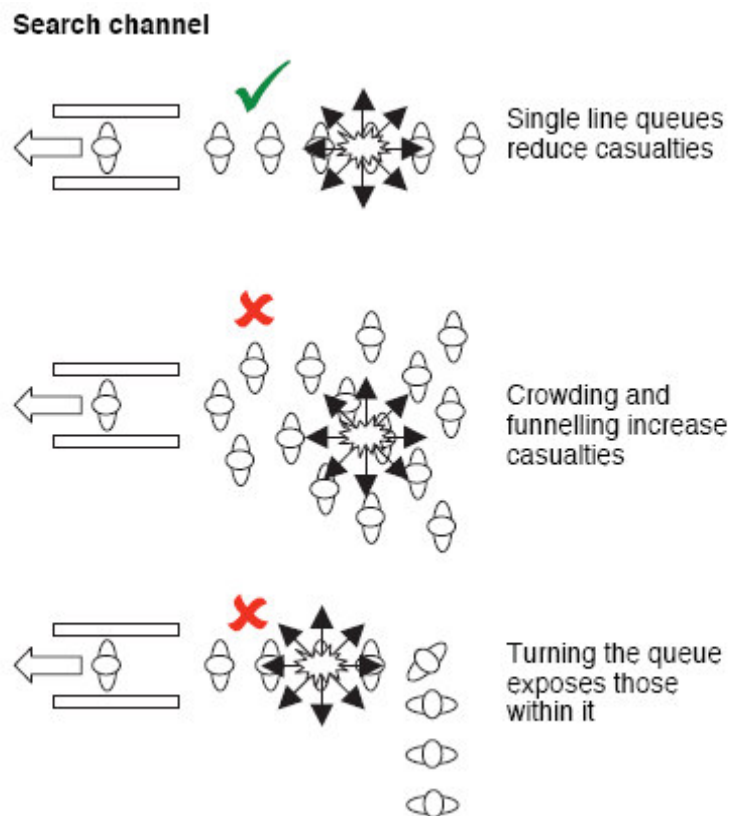


Figure 4 - Queue control to limit casualties.

AD 80-25

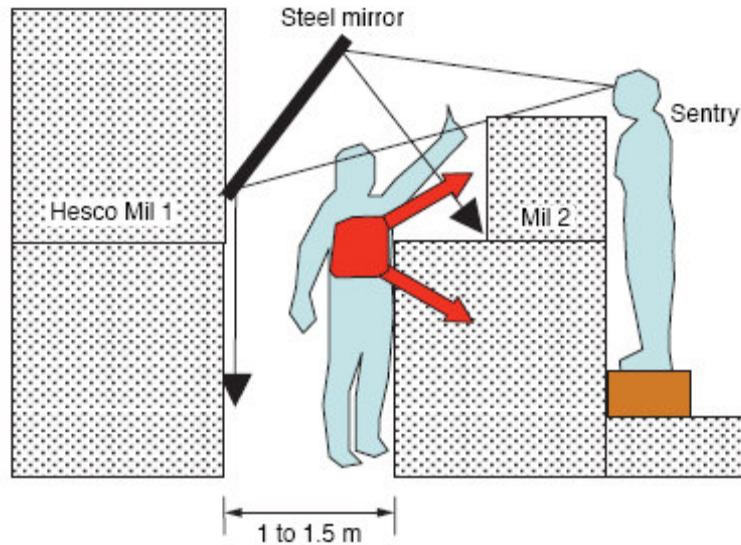


Figure 5 – Protection for Sentries in close contact with uncleared personnel.

9. **Vehicle Access Considerations.** Careful consideration must be made to minimize the threat from uncleared vehicles at the ECP. Two elements affect a vehicle's ability to breach an obstacle: speed and weight. The speed of a hostile vehicle can be managed by use of techniques in the design that force the vehicle to slow down in order to enter or negotiate the traffic lanes. Ultimately, vehicles can be blocked by the use of

a. **Vehicle slowing techniques.** Speed management techniques and considerations include:

- (1) Sharp 90 degree turns into the ECP from surrounding road network.
- (2) Traffic circles leading into the ECP.
- (3) Nonlinear lane designs.
- (4) Chicane layout of lanes with anti-vehicular barriers, such as concrete barriers (Jersey, Alaska), concrete blocks, earth-filled barriers (HESCOs™, metal revetment), and cabled steel hedgehogs. The tighter the chicane or "S" turns, the more the vehicle must slow down (see Figures 5 and 6 below). In terms of specification, the following applies.

(a) **Road and Lane Width.** The road width should be neither too wide nor too narrow. Each lane should be a minimum of 3.0 m wide, but preferably 3.6 m wide. The preferred road width is therefore 7.2 m.

(b) **Free-view Width.** It is often useful to arrange the barriers in a chicane to leave a free-view through the speed control measure.

AD 80-25

This helps avoid accidents that would otherwise temporarily close the control point.

(c) **Stagger Length.** The stagger length is the length from face-to-face of alternate barriers. Figure 6 gives dimensions of stagger length to control the speeds of different vehicle types.

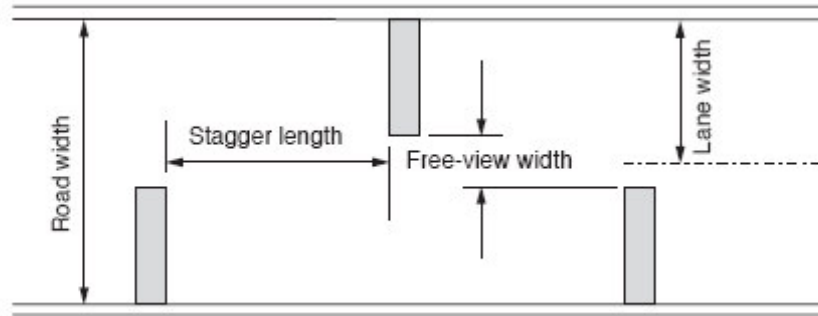


Figure 6 - Concrete barrier/block serpentine layout to reduce speed.

Serial		Stagger length (m)		
		10 l 15 kph	20 l 30 kph	30 l 50 kph
(a)	(b)	(c)	(d)	(e)
1	Medium car	5.8	6.7	10.5
2	7.5 t van	7.8	9.6	11.7
3	30 t rigid-body truck	12.1	14.2	16.2
4	Articulated lorry	12.7	14.6	14.8
5	Warrior AFV	?	?	?

Figure 7 - Separation distance for barriers to reduce speed on a straight path

(5) Speed bumps and tables large enough to cause small vehicles to bottom out, thus slowing the vehicle or denying access through the lane. Speed tables slow vehicles to a lesser degree than speed bumps do.

b. **Vehicle blocking techniques.** A moving vehicle has significant kinetic energy and momentum. A barrier must be able to absorb that energy and counter the momentum. Vehicles can defeat a barrier by either breaching it or riding over it. Invariably, a barrier must be able to mobilize sufficient effective mass. This can be achieved in a number of ways (see Figure 7 below):

AD 80-25

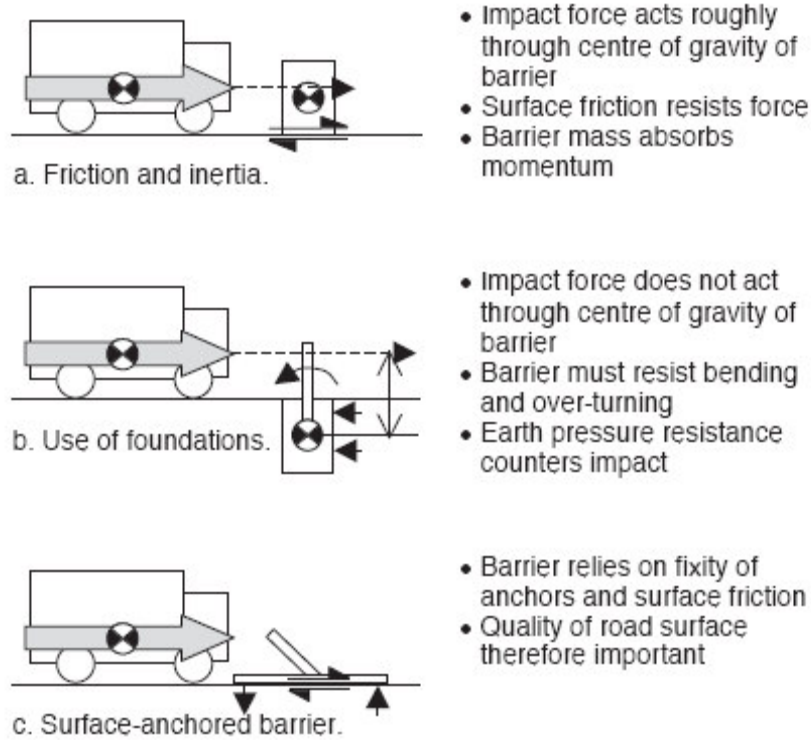


Figure 8 - Techniques for resisting Vehicle Impact.

(1) **Barriers.** When specifying the blocking ability of a static/movable barrier at an ECP, the most commonly understood design specification is the US Dept of State standard (illustrated in Figure 8 below). Barriers should be used in conjunction with

US VEHICLE IMPACT TEST CLASSIFICATIONS

Serial	Classification	Impact speed (m/s (kph))
(a)	(b)	(c)
1	K12	50 80
2	K8	40 65
3	K4	30 50

Figure 9 - Vehicle Impact test classification (Rigid truck of weight 6,810kg not able to penetrate further than 0.9m at the specified speed).

(2) **Bollards.** Bollards are metal or concrete columns which are anchored into the ground. Bollards can be used as static/movable barriers. Static bollards can be placed on either the inside or the outside of existing fences. Movable (or retractable) bollards can be pulled out of the ground by hand or raised and retracted by a hydraulic / pneumatic

AD 80-25

system to control entry at a facility ECP. An effective passive bollard system consists of 2.1m long steel pipes, a minimum of 20cm to 25cm in diameter filled with concrete. The pipes should be spaced as shown in Figure 9 below. The footing should be continuous, but individual footing depth should be at least twice the width, and the width should be three times the diameter of the pipe.

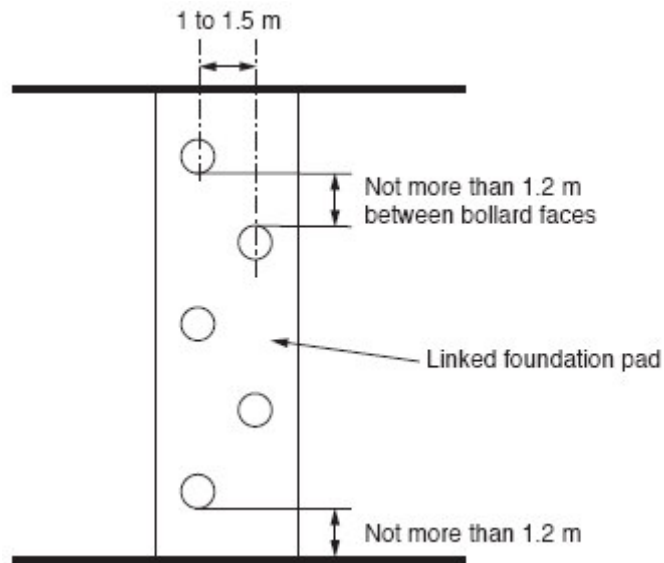


Figure 10 – Rising Bollard Final Arrest Barrier layout.

(3) **Removable Beam or Post.** Removable beams and posts are designed to be slotted into pre-cast holes in the road pavement. They must be light enough and fit with sufficient clearance to allow a single sentry to insert and remove them fairly easily. This limits their length and section strength. They are well suited to act as reinforcement behind a closed vehicle gate. They are not well suited as chicane barriers as they are likely to jam in place if they are struck by an armoured or other heavy vehicle.

(4) **Drop Arm.** Drop-arm barriers are made from heavy steel sections and may have an internal reinforcing cable. They are normally held up to allow traffic to flow and fall into place to close the gate when the restraining solenoid bolt is released. The release mechanism of this type of barrier is usually exposed to the environment and consequently at greater risk of seizure or premature firing. The closing action of this type of gate is inherently dangerous as the falling barrier may strike a vehicle on its relatively unprotected roof and may easily injure or kill the occupants. Furthermore, drop-arm barriers only provide full closure when they have engaged and locked in the catcher post; when they fall, they may miss the catcher post or bounce up off it.

AD 80-25

- (5) **Concrete Sections.** Concrete barriers such as the US Jersey barriers are useful static barriers. Where practical to do so, they should be cabled together to increase resistance. They will not stop a truck.
- (6) **Gabions and other Earth-filled Barriers.** Hesco™ Bastion gabions burst on impact and are highly efficient at absorbing kinetic energy as the vehicle passes through a dense 'cloud' of aggregate. They have been used effectively at control points on operations. However, as they are prone to damage from passing vehicles, their ends should be protected by concrete blocks, particularly when they are used to form a chicane.
- (7) **Metal Motorway Barriers.** Metal motorway barriers are designed to resist shallow angle impacts and deflect the vehicle back on to the carriageway. They are particularly poor at resisting impact at right angles. They should not be used in a control point.
- (8) **ISO Containers.** ISO containers can make effective static barriers but they are relatively light when empty. On a concrete surface, a 7 tonne truck travelling at approx 50kph easily pushes two empty 40-foot ISO containers apart. To work effectively, they must either be cabled together or have a weighty load, or both. Alternatively, two layers may be used. The friction of the surface on which they sit influences their resistance to impact. If they can be stopped from sliding, their sides crumple on impact and they can absorb considerable impact forces.

10. **Lighting Considerations for ECPs.** Within the ECP, the lighting requirements vary, depending on the type of zone and light discipline restrictions. Appendix 2 provides specific details and requirements concerning security lighting and recommends capabilities.

- (a) **General Requirements.** The ECP should be provided with multiple, redundant lighting to ensure that the loss of a single luminary does not seriously degrade the total lighting available for security personnel. The lighting at the ECP should be designed as controlled lighting to increase traffic safety. Glare projection, or glare lighting, should be avoided where a safety hazard would be created.
- (b) **Approach and Response Zone Lighting.** The approach and response zones require typical roadway lighting. The roadway lighting should provide enough intensity so that pedestrians, security personnel, islands, signage, and other hazards are visible. The lighting should not be directed in the driver's eyes and should not backlight important signage or security personnel. Transitional lighting is necessary on approaches to the ECP so that drivers are not blinded during arrival and departure.

AD 80-25

(c) **Access Control Zone Lighting.** In the access control zone, area lighting provided in the vicinity of the search facilities should be at a higher level to facilitate identification and inspection procedures. The lighting should illuminate the exterior and interior of a vehicle. In addition to good vertical illumination, additional task lighting may be necessary for adequate identification of vehicle occupants and contents. Such lighting should be directed across the roadway; it will then illuminate the roadway in front of the guardhouse, the driver, and the security personnel. Lighting may also be mounted at or below pavement level to facilitate under-vehicle inspection.

11. **Overwatch considerations.** The overwatch for an ECP is a manned position that provides observation and has the ability to cue reactive forces as well as employ deadly force against vehicles and attackers that attempt to bypass, ram, or otherwise run through an ECP. The overwatch position is an essential element of the ECP that must provide suitable MilEng protection to the operators from close proximity blast and fragmentation weapon effects. This is especially the case where the tower is positioned forward of the main vehicle scanning area and is therefore in close proximity to large blast threats. The optimum location is one which has both standoff and complete overwatch with clear arcs, however one is often at the expense of the other and hence the need for a higher level of protection (reinforced concrete blast rated structures being a common requirement). The following guidelines should be employed when planning the provision of overwatch.

a. **Purpose.** At any base or other static location where there is a need for a guard, there is likely to be a requirement for protective infrastructure to support it. Sangars, towers and rocket screens are commonly used. To be effective, they must be designed and deployed as an integrated system. The system must provide:

(1) **Weapon Platform.** A sentry must be able to fire his weapon. If he cannot, the use of a CCTV camera should be considered as this is simpler to erect and places a sentry at less risk.

(2) **Observation.** Implicit in the first requirement is the need for good all-round fields of view. Additionally, an overwatch sentry with good observation helps provide a commander with situational awareness.

(3) **Communications.** It is essential that sentries have adequate means of communicating what they can see to other members of the guard. As they may be the first to be involved in an incident, they must be able to pass information to a superior, call for assistance or give directions to others.

(4) **Protection.** In an attack, the sentry position is often vulnerable and may indeed be the focus of the attack itself. Effective protection is required for the sentry in the tower. Specifically the overwatch tower must

AD 80-25

be designed to withstand the specified design threat at its closest possible proximity without compromise the other requirements.

(5) **Operation of Alarm and Barriers.** The sentry should be able to sound any local alarm system and seal an entry control point (ECP) using a remotely-operated final arrest barrier where such is provided.

(6) **Visible Deterrent.** A sangar presents an assertive force posture, especially if elevated. A well-positioned sangar with good arcs of fire and an alert sentry can act as a considerable deterrent to an attacker.

(7) **Environmental Shelter.** To remain alert and hence effective, the sentry must be given some shelter from the environment: sun, rain, wind and cold.

b. **Threats.** Sangars and other sentry positions are vulnerable to the following threats:

(1) **Small Arms Fire.** The small arms threat comes primarily from sniper fire and assault. By making it difficult to see the sentry, a sniper is unable to make aimed shots. If a base is assaulted, an elevated sentry relies on other members of the guard force to give mutually supporting fire, particularly into the dead ground around the bottom of the sangar. Walls in and around an ECP should be kept as low as practicable to minimize their obstruction to the line of fire. Shrouds should be used to prevent silhouetting of the sentry. Where the climate dictates glass is necessary it should be of sufficient strength and thickness to counter the design threat.

(2) **Shoulder-launched Weapons.** An overwatch tower presents much the same sized target as a static, lightly armoured vehicle. Shoulder-launched antitank weapons are a potential threat. Sangars may also be attacked by hand-held anti-structures munitions. A stand-off screen may be added as part of the overall protective system where practical and where the specific design threat specifies (e.g. high threat of RPG attack where enemy can approach close to tower (<300m unsighted)).

(3) **Exploding Weapons.** Fragmentation and blast pressure are the significant threats from exploding weapons such as vehicle-borne IEDs (VBIEDs) and mortars. As the walls of sangars are designed to defeat small arms, fragment perforation is not likely. However, the underside of an elevated sangar is a potential weakness. Large explosive weapons may topple a structure through blast pressure, but, at ranges close enough for this to occur, the damage done to the structure from fragments alone may cause collapse. The effects of blast on sangar occupants are very difficult to determine. It is easier to make a qualitative assessment

AD 80-25

than a quantitative one. Large openings allow more pressure to enter the sangar than small ones. Pressure reflections are complex inside a sangar; the highest concentrations occur in the bottom corner furthest from the explosion.

(4) **Hostile Crowds.** As they are positioned along a perimeter and at ECPs, sangars are likely to be the focus of any hostile crowd. Stones, petrol bombs and other missiles may be thrown. The response to public order problems must be carefully considered beforehand and reflected in the overall design, e.g. should a guard abandon a position, or take cover and await the quick reaction force?

c. **Protective System.** The sangar, its elevation and any protective screening must be considered as a whole system if it is to be effective. The system must be simple, quick and safe to construct.

(1) **Sangar.** The sangar is the basic element of the system. It is, in effect, an above-ground fighting position in which sentries take post and from which they may be expected to fire their weapons. It should be compatible with the other elements of the system.

(2) **Elevation.** To provide an adequate field of view, it is often necessary to elevate a sangar. This can be accomplished by placing it on top of a tower, earth bank, ISO container or existing structure.

(3) **Screen.** To defeat some weapons, a stand-off screen is required. The stand-off is determined by the weapon it is to counter and by the protection afforded by a sangar itself. When elevating a sangar, the most difficult engineering challenge is often providing support to the screen whilst keeping it at the required stand-off (>3m).

(4) **Sighting.** As a sangar has a key role in the protection of a base or static facility, its sighting must involve the guard force commander. It should not be considered as merely a structure to be positioned only by those responsible for managing the base infrastructure. To ensure good observation and arcs of fire, the position and elevation of a sangar may be confirmed before construction using either a remote camera or temporary elevated platform.

(5) **Escape.** It is not just hostile crowds that a sentry may have to escape from; a fire may start accidentally or be the result of an attack. For a sangar elevated on a tower, it is only practical to provide one stairway. To mitigate the risk to the sentry, the tower structure must not be made of a combustible material (i.e. the material must not be higher than Class 01) nor should anything be stored inside the tower.



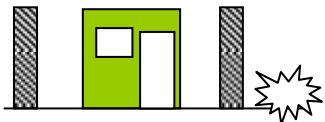
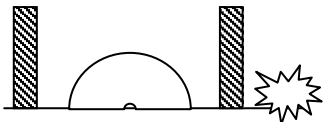
AD 80-25

(6) **Electronic Counter Measures.** If a sangar is close to a road with public access, it is strongly recommended that it is fitted with an electronic counter measures (ECM) suite. If the sangar is elevated at an ECP, it is an ideal location for the ECM transmitter to help ensure the guard force on the ground is working inside the ECM 'bubble'.

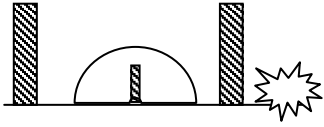

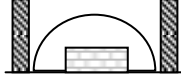
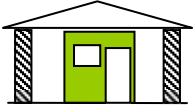
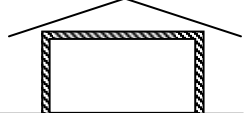
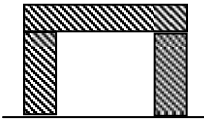
Note: Further specification details regarding the use of lighting and CCTV are given in Appendix 2.

**FORCE PROTECTION ENGINEERING MEASURES FOR NATO CROs
 DEFINED LEVEL OF INFRASTRUCTURE PROTECTION – LIVING AND WORKING ACCOMMODATION STRUCTURES**

1. The table above defines the level of MilEng measures to be applied to buildings and fixed infrastructure.

MilEng Level	Structural Form		Description
Level 0			<p>No FP Protective measures in place. However, structures are positioned and built in such a way that MilEng measures can be implemented at a later stage without undue disruption to the continued operational function of the building (e.g. DFAC floors to be capable of supporting weight of additional compartmentalisation if the threat level increases).</p> <p>When carrying out camp planning, no living / working accommodation should be positioned within 100m of the base perimeter.</p>
Level 1		 <p style="text-align: right;">1A</p>	<p>Form: Compartmentalisation using anti-fragmentation walls.</p> <p>Protection: Protects against fragments from weapon landing outside compartment. Mitigates number of casualties from a direct hit. Also vulnerable to fragments falling over the wall.</p>

AD 80-25

MilEng Level	Structural Form		Description
		 <p>1B</p>	<p>A – Compartmentalisation external to the structure only.</p> <p>B – External and Internal compartmentalisation.</p> <p>Construction: Can be retrofit only if space allocated from outset and internal flooring has load capacity to accommodate the additional internal loading.</p>
Level 2		 <p>2A</p>  <p>2B1</p>  <p>2B2</p>  <p>2B3</p>	<p>Form: MilEng Level 1 plus limited overhead protection.</p> <p>Protection: Limited protection from small, impact-fused IDF rounds landing on roof. Degree of protection depends on actual measures used.</p> <p>A – Retrofit Tier 1. “micro-compartment” built around bunk, including overhead protection (e.g. e-glass or sandbags on steel sheet).</p> <p>B1 – Retrofit Tier 2. Roof provides stand-off and may allow additional hardening layer to be fitted to cabin roof and/or micro-compartment built around bunk if practicable.</p> <p>B2 – Purpose-built concrete-walled structure with roof for stand-off. Windows remain vulnerability if installed. Building also has internal compartment walls.</p> <p>B3 – Expedient structure using <i>Hesco™</i> gabion walls and a thick roof. Few materials require import, relies on locally-won aggregate. Simple and quick to erect. Short building life.</p>

AD 80-25

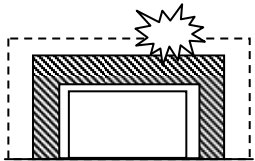
MilEng Level	Structural Form	Description
		Construction: Time and cost vary depending on solution and whether retrofit or new-build.
Level 3		Form: Tripartite protection from stand-off screen (2m), thick concrete/steel wall and internal stand-off. Protection: High degree of assured protection from wide range of dud, delay and impact-fused IDF weapons. Construction: Extremely expensive (x10) lengthy build-time (x2)

Figure 1 – Design MilEng Level for buildings and other fixed infrastructure.

2. The exact MilEng Level specified results from the Staffs' analysis of the threat and the Commander's risk assessment, in accordance with the guidelines given in the covering Annex I. It is dependent on the nature of the building's utility, its design life¹¹ and the Threat Assessment. The prevailing type of threat will also have an effect on the exact structural form specified as well as a measure of engineering judgement. As an example, for MilEng Level 2 where the IDF threat predominates structural form 2B2 (offering a good level of over head protection) may be considered suitable, however where a close in VBIED blast threat predominates structural form 2B3, with its continual structural form and thicker blast walls, may be considered more suitable. In buildings where personnel gather (high population structures) and where the IDF threat is considered SIGNIFICANT or HIGH as a minimum MilEng Level 2 protection must be provided.

3. **MilEng Level 0 Measures.** Whilst no protective structures are present at this MilEng level, a number of key considerations must be observed to ensure structures are safe and future proof to evolving threats. Accommodation must be spaced to provide sufficient space for blast walls. Where containerised accommodation is used, double stacking of new containers with ISO certified frame loading capacity is only to be permitted with full stud plate and clamp connections. Relocated containerised accommodation is not to be double stacked unless within a structural frame of appropriate resilience. Wall-mounted air-conditioning units are to be avoided wherever possible. When necessary, these must be the 2-part air-conditioners to minimise any loss of wall panel integrity.

¹¹ NATO specifies the design life for NSIP funded infrastructure and communications equipment on CROs in SHAPE Ref 6100/SHRIM/008/03 dated Jan 03. It specifies a Tier system, with Tier 1 being several weeks/months, Tier 2 being 2 months to 2 years, Tier 3 being 6 months to 10 years and Tier 4 being permanent.

AD 80-25

4. **MilEng Level 1 Protective Measures.** Where MilEng Level 1 is designated, the following detailed design issues must be considered:
 - a. **External Sidewalls.** The side walls must provide protection from the blast and fragmentation effects of external explosions. Any sturdy wall will reduce the effects of blast and fragmentation, up to a point! A 'blast wall' is designed to resist the pressure, impulse and fragmentation caused by a close-in or large explosion. A 'fragmentation wall' is less robust and is optimised to act as a shield against the primary fragments of a weapon, without itself becoming a secondary fragmentation hazard. For IDF threats the fragmentations effects are likely to govern over all but the very smallest of distances from the point of impact. Methods such as Sandbags, HESCO™ and pre-cast Concrete sections are commonly used. Where a direct fire threat exists, the use of a Pre-detonation layer should be considered. Sidewalls must be placed either close to the weapon or next to the asset to be protected. Intermediate positions are far less effective! The pressure pulse from an explosion will propagate around corners and over walls. A blast wall will create a shadow of reduced pressure on its shielded side, for a distance of up to 5-7 times the height of the wall. Similarly a fragmentation wall should be placed close to the asset, to prevent fragments falling behind the wall. For larger IED threats where blast governs corrugated Metal Bin Revetments of similar size, such as Metalith™ can be used. For a more permanent solution, specialist blast energy absorption walls¹² can be used. As a general rule, the more specialist the product, the greater the requirement for specialist engineer advice during design and installation. Figure 2 below indicates optimal positioning for blast walls.

¹² Such as Dynabloc™, Paxcon™, or Tabreshield™ to name a selection.

AD 80-25

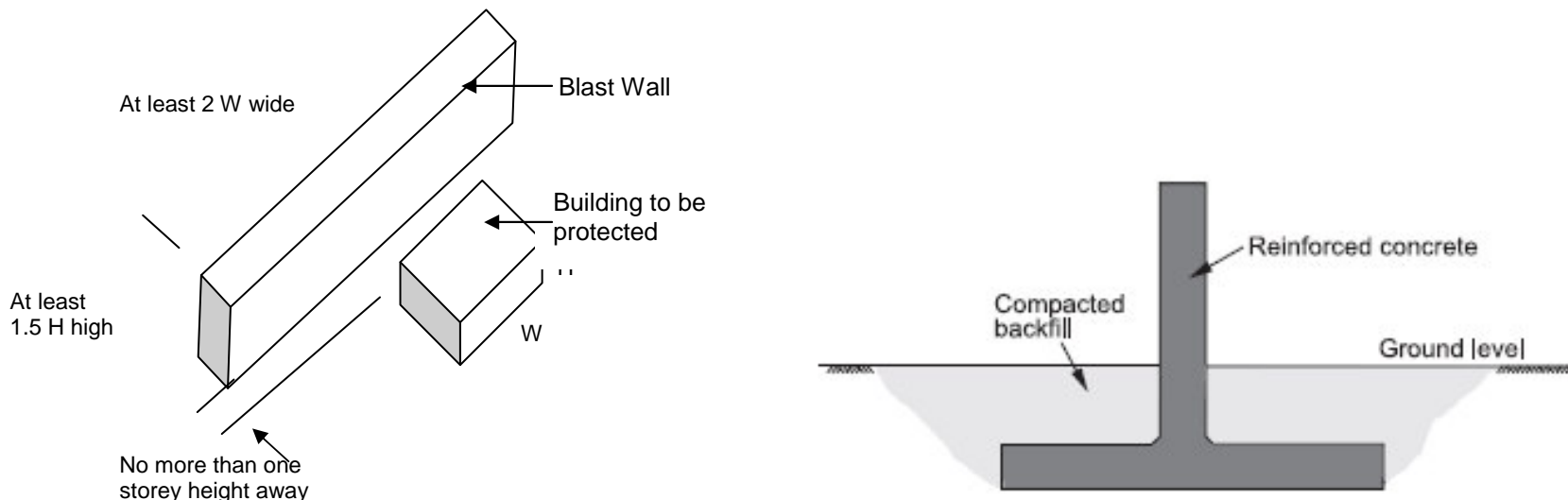


Figure 2 - Diagram illustrating optimal blast wall positioning and scale. Ideally blast walls should be dug in as shown on the right.

Structure Design. The simplest structures designed to resist the effects of an explosion rely on their size and mass alone. These massive structures absorb and dissipate a weapon's effects simply by overwhelming them. A more efficient technique is to use a tripartite system, where each layer is optimised to achieve a specific effect. Such systems can be retrofitted onto existing structures to enhance the protection they offer. This is illustrated in Figure 3 below.

AD 80-25

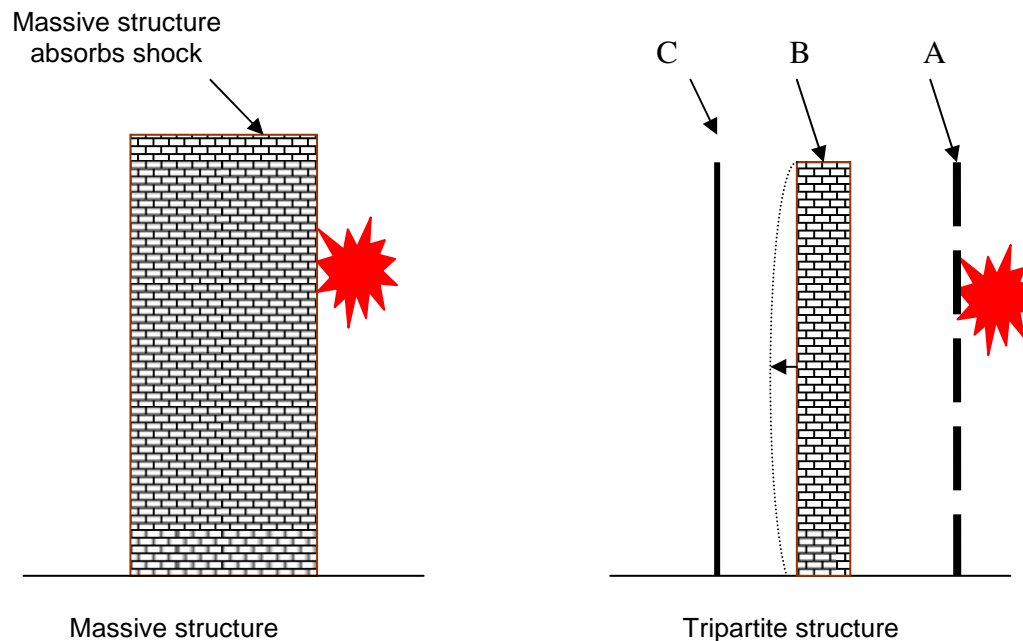


Figure 3 – Protective Wall design principles.

A = External Stand-off Screen. It is used to ensure the weapon functions no closer than a predetermined stand-off from the main structure.

B = Main (Deflecting) Wall. It is used to deflect and absorb the blast energy. The best results are achieved using specially designed reinforced concrete panels with steel backing plates, or masonry coated with plastic polymer.

C = Internal Stand-off. As the main wall can be expected to deflect extremely rapidly into the protected space, it is important to ensure that the occupants or equipment within are kept away from the wall.

AD 80-25

Figure 4 below illustrates further 'do's and don'ts' regarding the positioning of protective side walls.

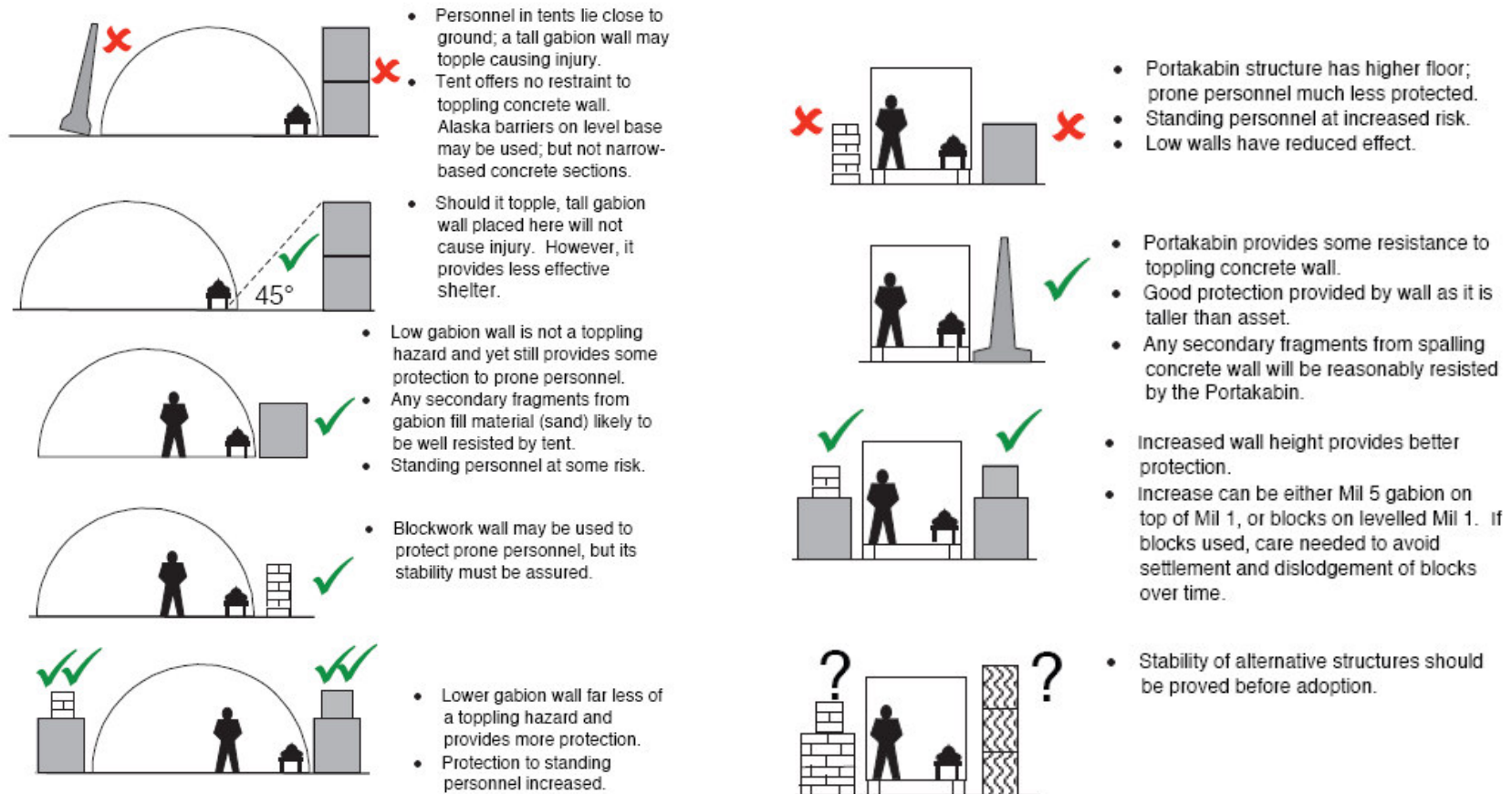


Figure 4 –MilEng Level 1 protection measures (tentage and containers).

AD 80-25

b. **Internal Compartmentalisation Walls.** Discrete compartments may be formed around groups of assets using protective structures, usually blast or fragmentation walls. Their purpose is to ensure that the damaging effects of an attack are contained within the compartment attacked. This technique inherently accepts the loss of assets within the compartment. The effectiveness of this technique is also sensitive to the specific threat faced. For this technique to work, the effect of the attack must be contained within the compartment. For example, within a temporary camp threatened by mortar fire, the walls must be sufficiently high to ensure the weapon functions inside the compartmental cell.

Furthermore, the cell walls must be robust enough to withstand the close or in-contact detonation of the round and avoid hazarding the adjacent cell through breaching. Provided the integrity of the compartment walls can be assured, greater protection comes from smaller cell sizes. However, smaller cells require more construction time and resources. A law of diminishing returns is observed; ever more effort is required for smaller incremental improvements in protection. In most cases, an optimum size of compartment can be determined. It will almost certainly not deliver the greatest level of protection possible, but it will allow more resources to be committed elsewhere, possibly to improve protection at other locations. Figure 5 below shows an example of internal compartmentalization. A number of techniques exist for creating the compartment walls including:

(1) **Soil or sand enclosed in timber revetment.** This method is relatively cheap and easy to install and is suitable for tented accommodation. The wooden partition wall is constructed of 18mm plywood over 50mm x 200mm. x 57 in.-long studs with 50mm x 100mm whaling along the outside. The 180mm cavity that is formed is filled with soil and capped with 50mm x 200mm timber. The fill material is the primary element for stopping weapon fragmentation. The walls are attached to the floor of the facility to provide stability and prevent overturning from the blast of weapon detonation. Care must be taken to ensure only fine soil/sand is used and no solid objects, which could act as secondary fragmentation, are present in the fill material.

(2) **e-glass.** Partitions can be separated using multi-layered (3-layer and 5-layer) wall panels of ballistic grade e glass (NSN 9340-01-533-5758) supported by custom manufactured steel stands fixed to columns and the floor. For 122mm rocket / 120mm mortar threats 5- layer panels should be used. If e-glass is not available steel sheet can be used in the same way.

(3) **Concrete Blocks.** This method uses concrete blocks loose or bound to create partition walls. The walls are particularly good at resisting penetration by primary fragments. Normal, rather than lightweight, concrete is used. Each block is 400 mm x 200mm x 200 mm in size. At over 30 kg each, the individual blocks are rather heavy. Walls can be built in a number on configurations but must be sufficiently stable (no higher than 3 times their thickness and ideally constructed at double thickness to a height of 1.2m). Care must be taken to ensure the floor is strong enough to support the additional loading. The high mass of the separate blocks gives the wall just sufficient inertia to resist collapse except when attacked by a very close-in weapon. It must be

AD 80-25

stressed that this type of structure is less effective against weapons with a large explosive warhead (bigger than 107mm rocket / 82mm mortar) due to additional secondary fragmentation hazard.

(4) **Proprietary Products.** Hesco™ Bastion soil-filled revetments can also be use for compartmentalization. As an example a small dining facility can be compartmentalized with 2 ft thick Hesco™ Bastion soil-filled revetments constructed to a height of two baskets (4 feet). Care must be taken to ensure only fine soil/sand is used and no solid objects, which could act as secondary fragmentation, are present in the fill material. Corrugated Metal Bin Revetments of similar size, such as Metalith™ can also be used for this application. As a general rule, the more specialist the product the greater the requirement for specialist engineer advice during design and installation, however most products come with clear construction guidelines for ease of use by troops on the ground.

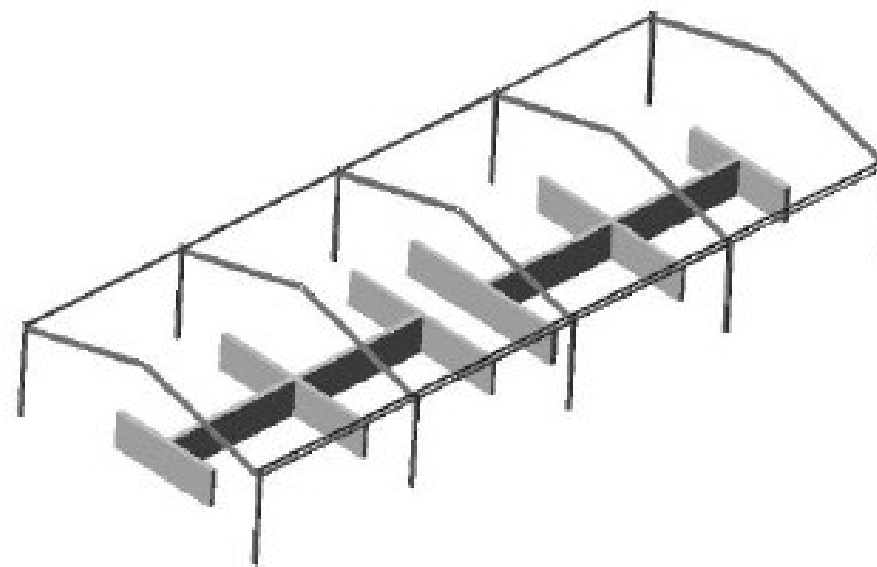
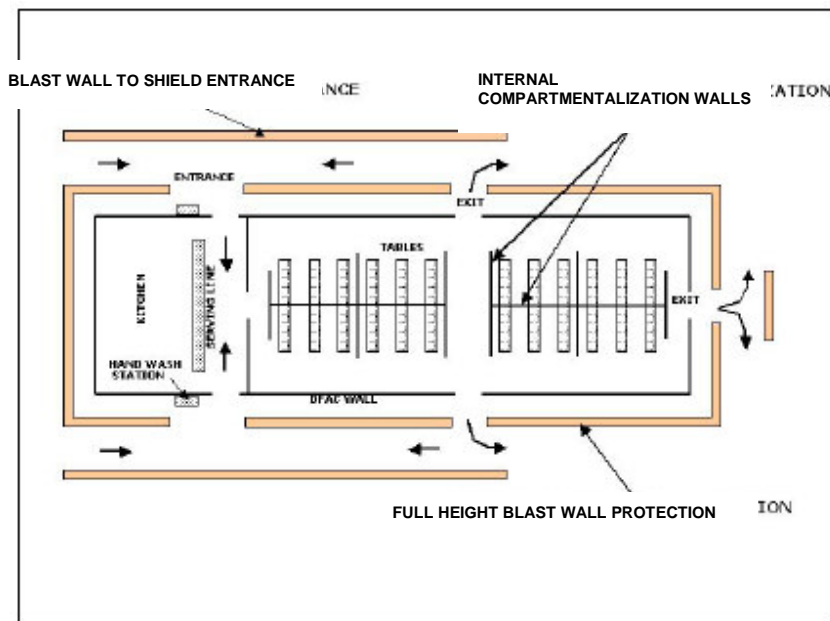


Figure 5 –MilEng Level 1 (Structural Form 1B) protection measures (internal compartmentalisation for tentage and containers).

AD 80-25

5. **MilEng Level 2 Protective Measures.** Where MilEng Level 2 is designated, overhead protection must be provided. This can be done on an individual basis (Structural form MilEng Level 2A) or for the whole structure (Structural form MilEng Level 2B). In developing the structural design, the following detailed design issues must be considered:

a. **Individual Protection (Structural Form MilEng Level 2A).** Measures can be taken to protect individuals in their living and working accommodation. This includes the construction of individually protected bed spaces and the provision of reinforcing panels to working accommodation containers. Common materials for the provision of this protection include concrete blocks, steel sheet, sandbags, plywood and e-glass or other similar composite materials. Figure 6 below illustrates MilEng Level 2A measures.

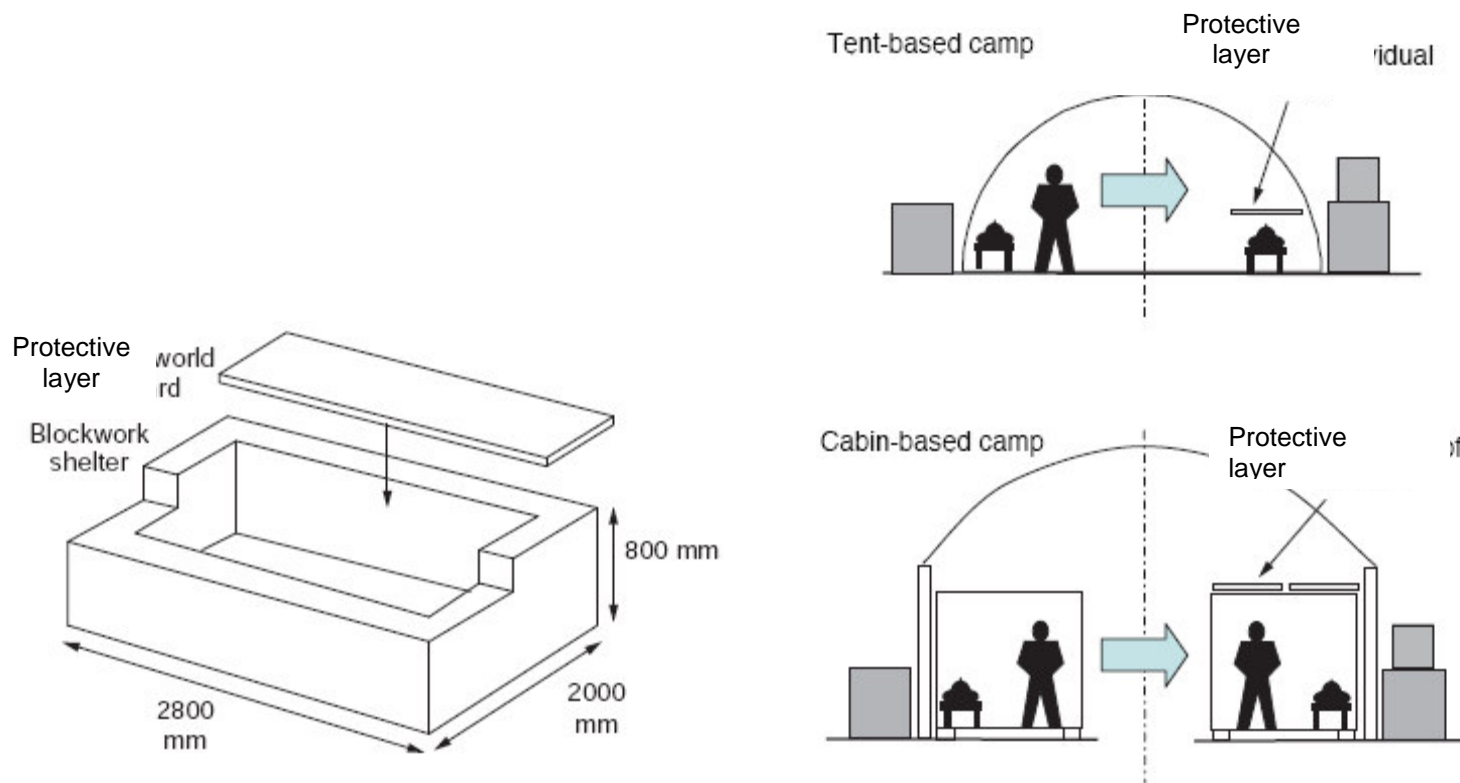


Figure 6 – MilEng Level 2 (Structural Form 2A) protection measures (OHP for tentage and containers).

AD 80-25

- b. **Overhead Protection (Structural Form MilEng Level 2B).** This is made up of two elements, as illustrated in Figure 7 below.
- (1) **Pre-detonation.** The pre-detonation layer must be sufficiently robust to cause the fuse to function. It should be positioned sufficiently higher above the protective layer to give sufficient standoff which in itself reduces the chance of fragments penetrating the shielding layer. As a guide, for a 122mm rocket / 120mm mortar threat, the pre-detonation layer must be positioned at least 1.2m above the shielding layer.
- (2) **Shielding.** The thickness and composition of the shielding layer is dictated by the weapon threat. It must be capable of blocking fragmentation. References D and E contain further detailed design options, with test data to show what structural solutions are capable of countering what weapon system. (As an illustrative example only, a MilEng Level 2B2 construction may utilise a 200mm RC outer skin (walls and roof) with a steel frame above supporting an 18mm plywood and 0.5mm steel clad roof structure.)

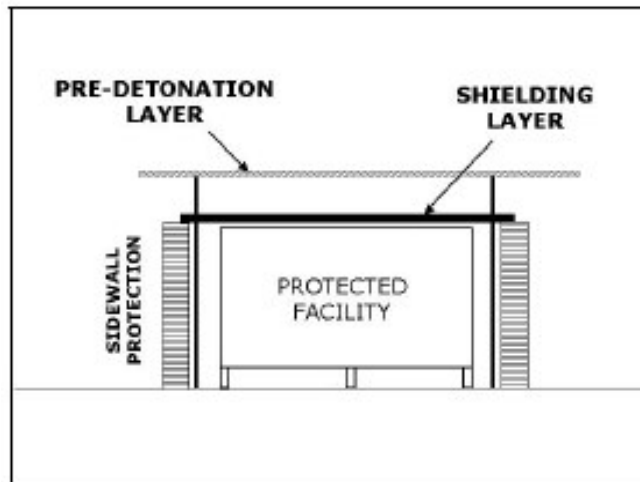
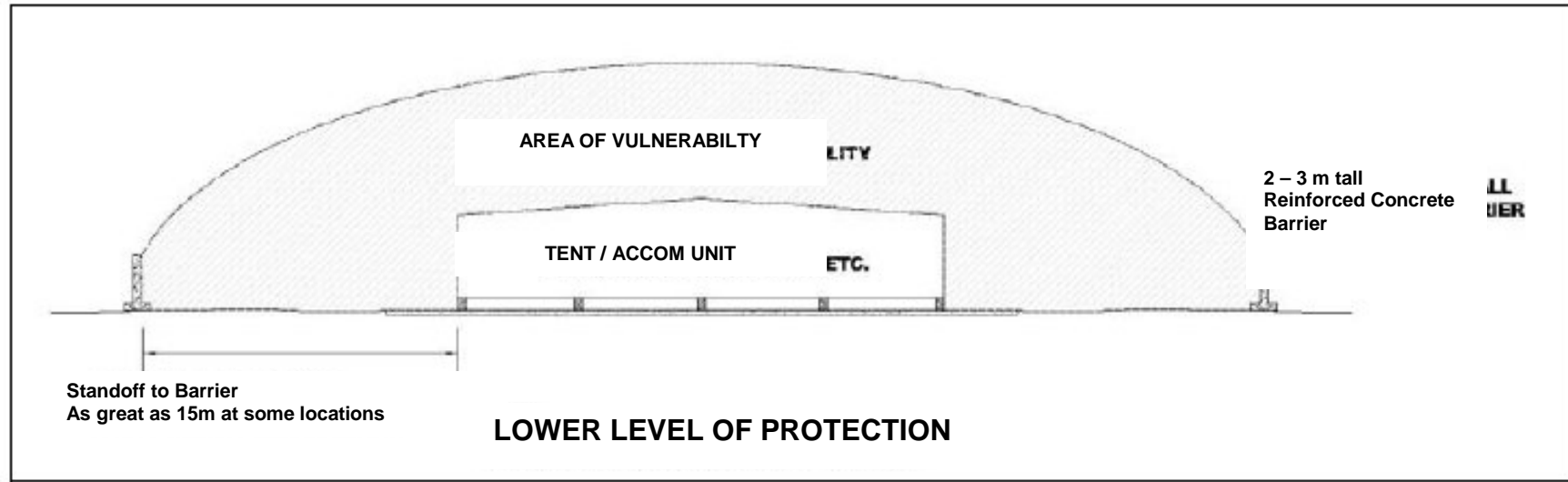


Figure 7 – Overhead protection concept.

Figure 8 below illustrates the enhanced protection achieved by the construction of a MilEng Level 2 (Structural form 2B2) building over existing modular accommodation.

AD 80-25



AD 80-25

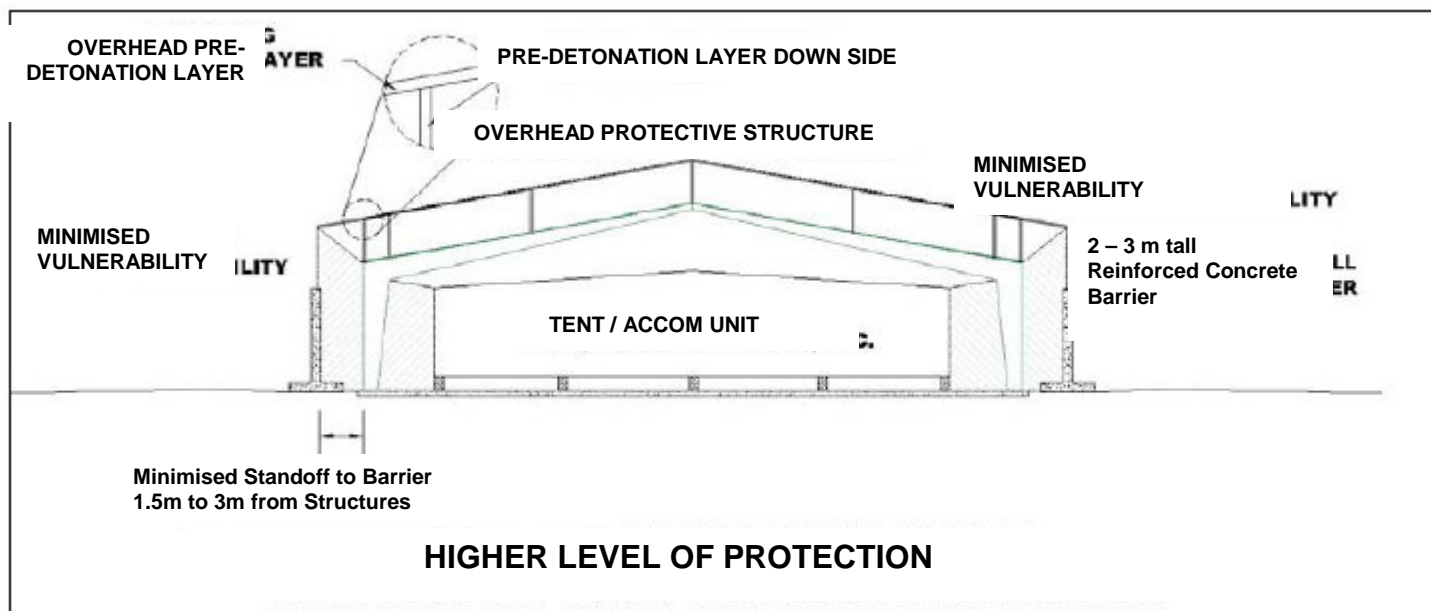


Figure 8 – MilEng Level 1 (above) and 2 (below) protection of existing modular accommodation structure.

6. **MilEng Level 3 Protective Measures.** Where MilEng Level 3 is designated, a structural / civil engineer must be employed to carry out the detailed specification and design work. Construction of this infrastructure is normally conducted by a civil contractor, being beyond the capability of most military engineer forces. These structures are therefore likely to be developed in a deliberate way later in the life of a CRO.

7. **Windows and Frames.** Windows represent an inherent vulnerability to weapon effects. For existing structures it is likely that glass is not strengthened and therefore the glass should either, dependent on threat proximity, be removed and replaced with sandbags or strengthened with the application of anti-shatter film (ASF)¹³ in combination with catcher bars. For new structures, the vulnerability should be minimised where practicable with the positioning of windows above head height. For MilEng Level 1 structures, ASF should be fitted to all windows on the site. For MilEng Level 2 and above, the progressive upgrade of all glazing to a minimum of 7.5mm laminate internal pane¹⁴ and 6.4mm toughened

¹³ 175 ASF, (175µm thick). This must be properly installed in accordance with the product specifications.

¹⁴ With a minimum of 1.5mm thick PVB layer internal lamination bonding material.

AD 80-25

glass external pane double glazing is very strongly recommended. For all MilEng levels, windows must be fitted using appropriate frames with a comparable strength to prevent the window being forced in as a single projectile as a result of a large proximity blast event. Catcher bars, or similar systems to arrest the movement of the whole window and frame out of the wall, should be used where frame strength cannot be guaranteed.

8. **Use of existing structures.** Existing structures can provide a level of protection if sufficiently robust. A structural / civil engineer is required make such an assessment. Ideally, buildings should have the inherent structural redundancy to accept the traumatic *local* failure of one structural element without this overloading the other elements of the structure and leading to a progressive large scale collapse; this is shown in Figure 9 below. Some forms of structure are intrinsically better at providing alternative load paths than others. The best structures are usually reinforced concrete frames that have been cast in situ; mass masonry structures are the worst. A structural resilience of 2 (adjacent columns) needs to be used as a minimum standard for the seismic load conditions, increasing to 2+1 (2 adjacent columns and a corner column within 2 bays).



Figure 9 – Structural Redundancy.

9. **Site Protective Techniques.** There are a large variety of construction methods available to provide the protective structural elements specified in Figure 1 above. Further details are given in References D and E and other similar NATO member nation standard documents. These documents should be used by MilEng engineers to determine the suitable materials and dimensions to be used for the construction. (As an illustrative example only, a MilEng Level 2B2 construction may utilise a 250mm RC outer skin with a steel ram roof with minimum 1.5m standoff to counter a 107mm rocket/120mm mortar IDF threat).

10. **Collective Infrastructure MilEng Measures.** Other MilEng site wide measures for implementation include:

a. **Deception.** Within practical limits, all buildings should be of similar construction type and outward appearance, irrespective of function. Where possible, staircases should be internal and all building and compound entrances face away from the perimeter.

AD 80-25

- b. **Duplication.** Critical infrastructure needs to be duplicated or an alternative provided as a secondary role. In particular, alternates for the FP Company control room, the base operations room and emergency overspill/relocation of Role 2 and AeroMed facilities.
- c. **Dispersal.** High value assets should be dispersed to minimise the consequence of any single attack. This will include dispersing the principal staff accommodation and any on-call personnel and Quick Reaction Force teams.

EXAMPLE ANNEX J FOR FP

N.B. This Annex would be naturally produced after following the questions laid out in Annex D (Template Plan). That information can be pasted into this format to create an FP Plan (commonly known as Annex J in NATO OPLANs / OPORDs). The deductions made during this process effectively become the 'tasks' within this Annex.

REFERENCES:

- A. SHAPE's OPLAN.
- B. Joint Force Command's OPLAN.
- C. Theatre Commander's OPLAN.
- D. AJP-3.14 – Allied Joint Doctrine for Force Protection, dated 26 Nov 07.
- E. AD 80-25 – ACO Directive for Force Protection, dated 15 Apr 09.
- F. CM (2002)50 - Protection Measures for NATO Civil and Military Bodies, Deployed NATO Forces and Installations (Assets) Against Terrorist Threats.
- G. STANAGs (list relevant ones).
- H. Theatre SOPs (list relevant ones).
- I. Base Special Operating Instructions (SOIs).

SITUATION

1. **Introduction.** FP provides the *'measures and means to minimise the vulnerability of personnel, facilities, material, operations and activities from threats and hazards in order to preserve freedom of action and operational effectiveness thereby contributing to mission success'* (Reference D).
2. **Situation.** This paragraph outlines the specific details and functions of the individual facility / location. This is used to set the scene for priorities and significant aspects of the facility / location that are of concern to FP operations.
3. **Generic Threats.** ISAF personnel, civilian employees, equipment and facilities face a wide range of threats in-theatre, ranging from the environment to direct action from hostile and criminal opposing forces. The most likely kinetic threats include Direct Fire (DF) from Small Arms Fire (SAF) and Rocket Propelled Grenades (RPG), Improvised Explosive Devices (IED) of many types including suicide, and Indirect Fire (IDF) from rockets and mortars. A highly dangerous threat exists from Surface to Air Fire (SAFIRE) by Man-portable Air Defence Systems (MANPAD), particularly against large passenger aircraft. Opposing forces understand that carefully targeted tactical operations can affect Alliance cohesion. The use of MANPADs is unlikely given the lack of training that is required to operate them effectively. IEDs are becoming increasingly sophisticated and involve use of

AD 80-25

anti-personnel (AP) and anti-tank (ATk) mines as well as commercial explosives and elements of dismantled ordnance. IED initiation methods range from Radio Control (RCIED) to Victim-Operated (VOIED) from pressure plates, etc. An ever-present threat is unexploded ordnance (UXOs) from recent conflicts and Road Traffic Accidents (RTA) caused by poor road conditions, bad weather and a lack of traffic policing.

4. **General Threat Analysis.** No change to Reference A-C.
5. **Specific Threat Analysis.** Specific threat levels relevant to the facility / location are given in detail in this section or at an Appendix.
 - a. **CBRN/ROTA.** As per guidance given in para 5.
 - b. **Friendly Forces.** As per guidance given in para 5.
 - c. **Opposing Forces.** As per guidance given in para 5.
6. **FP Concept**
 - a. **Aim of FP.** The overall aim of FP is to adopt measures and procedures that are appropriate to the threats and risks inside the AOO. Although national and Alliance concerns may differ, FP and the preservation of FOM must not be degraded. FP measures are not meant to portray the image of an occupation force; rather, the population should perceive FP measures as sensible military precautions undertaken by a professional, disciplined, well-trained and confident force.
 - b. **Delegation of Authority.** The theatre commander has the overall responsibility for FP and is the only authority to decide on theatre-wide FP measures. Authority is granted to subordinate commanders to increase the FP measures as required by their specific requirements. The base FP Command Element has extracted direction and guidance from References A-H to conduct an estimate of the FP mission. This has been used to complete this Base FP Plan and the resulting base SOIs (Reference I).

EXECUTION

7. **General Outline.** FP must be a comprehensive and coordinated effort in order to protect personnel, facilities, equipment, operations and information. The following tasks have been identified from the FP Estimate.
8. **Specified Tasks**
 - a. **Establish a Tactical Area of Responsibility (TOAR)** to the limit of weapon range and that is under the command of the Base Commander in order

AD 80-25

to ensure FOM around the base / location and ultimately provide stand-off against efforts to inhibit primary operations.

b. **Command, Control, Communication, Intelligence & Integration.**

(1) **Establish a C2 element** that is able to conduct a full FP estimate, develop and amend FP plans as the situation develops, and can integrate with all elements of the Alliance / HN operational networks. Additionally, the FP plans must be based on a documented, objective threat assessment. Where FP measures are considered at risk to failure, the FP C2 is to prepare risk statements for the higher commander to accept (or for whoever is responsible for providing FP resources and manpower).

(2) **Develop daily working relationships with the local HN forces, IOs and NGOs¹**, in order to develop a coordinated and de-conflicted approach to operations in the TAOR.

(3) **Develop intelligence integration** with higher intelligence elements such as CI and intelligence fusion cells in order to benefit from and contribute to wider Situational Awareness.

(4) **Integrate with the theatre Air Operations Planning Group (AOPG)** in order to seek air mobility support for patrolling units / CASEVAC, and from ISTAR assets to provide surveillance / C-IED within the TAOR.

(5) **Liase with CIMIC², HUMINT and Information Operations teams** to raise the priority of such operations in the TAOR in order to gather intelligence on and focus efforts against opposing forces around the unit being defended.

(6) **Establish an FP C2 CIS plan**, or Information Exchange Requirements (IER), that can at least enable communication with the following:

- (a) All FP sub-unit elements at the location, cutting out unnecessary reporting nodes so information passes as quickly as possible.
- (b) Is able to fuse all surveillance system data in one location.
- (c) The location's main operations centre.

¹ The consideration of HN forces, IOs and NGOs as keen to collaborate with NATO forces is a sensitive issue. Those IOs, NGOs which have a neutral status and others whose ideology differs from that of NATO may be reluctant to collaborate. The issue of coordination and de-confliction with these organizations must be implemented in such a way that relationships are maintained.

² The use of CIMIC information to produce intelligence might be counter productive to the confidence of the civil population, IOs and NGOs. Those using this information must have this in mind and use it only in critical situations.

AD 80-25

- (d) Sector Commanders, if the base has been sub-divided into sectors.
- (e) Adjacent HN sy forces, IOs, NGOs and other Component Commands.
- (f) The operational / theatre FP officer.
- (g) The higher level NBC Warning & Reporting networks.
- (h) Operations elements that can support such as CI, CJ2, CIMIC, HUMINT, and the Joint / Air Operations Planning Group.

c. **Security**

- (1) **Implement off-base, high-visibility patrolling** in order to deter, disrupt, detect, delay and ultimately prevent or destroy potential hostile attacks from MANPADS, IEDs, mortars, rockets, and snipers. Patrols must have the mobility and firepower to dominate the TAOR as well as the ability to build relationships with the local population and thereby deny opposing forces practical and moral FOM.
- (2) **Develop a Fire Support plan** for Support Weapons in the event illumination or high explosives are required during a contact situation.
- (3) **Clarify details in the SOFA and MOUs** so that the police elements fully understand their powers of stop, search, arrest and detention.
- (4) **Check the physical security and INFOSEC** such as fences, doors, and security furniture to ensure it is good working order and available where it needs to be. Ensure document handling and IT procedures are in place to protect information.
- (5) **To ensure the security, safety and protection of food, water and energy / fuel sources at all stages of introduction / consumption at the location.** This means the fuel transfer points and convoys are protected where necessary. Food and water sources must also be vetted and monitored.
- (6) **Develop COE procedures** that ensures the unit has complete control and oversight of access to the following areas:
 - (a) Through the main and stand-by / alternate / trade base access points.
 - (b) For the fuel transfer point to the BFIs.

AD 80-25

- (c) Vital buildings such as Base Operations, etc.
- (d) Identified Vital Ground such as the vital working locations, aircraft operating surfaces, etc.
- (e) Internal and external VCPs at areas where personnel movement can be monitored and controlled as required.

d. **FP Engineering / Infrastructure Protection**

(1) **Develop an integrated approach to UXO, EOD and Mine Awareness issues.**

(2) **Ensure Fire Protection** has been considered for all areas of the locations and that fire evacuation orders are prepared; and there is a system to warn the Fire Crash Rescue Services (FCRS) in the event of a fire. Also, ensure fire appliances and alarms are routinely checked for serviceability.

(3) **Develop SOPs for maintaining a safe operating environment**, that includes safe working practices and healthy environment.

(4) **Develop FP engineering** projects in accordance with the Project Submission Request (PSR) process to ensure essential services / buildings are protected from blast / fragmentation and weather. Such areas include:

- (a) COE points;
- (b) ROLE / medical facilities;
- (c) Fences, barriers and boundaries;
- (d) Bulk Fuel Installations;
- (e) Gas, electric, and water storage / distribution networks;
- (f) CIS networks;
- (g) Sewerage / waste disposal / refuse disposal networks; and
- (h) Dining Facilities (DFAC).

(5) **Develop a Camouflage, Concealment, Dispersal and Deception (CCDD) plan** that is in harmony with main operations.

AD 80-25

e. **Health Protection**

- (1) **Develop a Mass Casualty plan** with the ROLE facility, and ensure arrangements are in place for either CASEVAC within the TAOR to the location for from the TAOR to an overflow, higher level ROLE facility.
- (2) **Develop a Health & Hygiene plan** that is supported by sufficient capacity of ablutions and medical support.

f. **Emergency Management**

- (1) **Develop Emergency Management plans to enable** recovery from any incident or accident that would demand a coordinated response. Such plans must be able to cope with IED / Indirect Fire / CBRN attacks as well as mass casualty situations and a range of unpredictable incidents. Plans should be based on common principles and kept as simple as possible so troops can learn them quickly and they are easy to implement under pressure. Training of local non-FP personnel will be required so individuals are able to act as First Responders or Incident Commanders.
- (2) **Identify specific manpower or train personnel to undertake Post Attack Recover (PAR)**, and who can search for UXOs or damaged infrastructure. A reporting network is required to support this effort and need implements as part of the CIS requirements.
- (3) **Identify personnel and resources that can repair damaged services** or facilities in order to restore main operations as quickly as possible.

g. **CBRN**

- (1) **Identify latent threats or dangerous infrastructure** that may eventually lead to an attack or release from a Toxic Industrial Material (TIM).
- (2) **Implement NBC and TIM detection, warning and monitoring capabilities.**
- (3) **Provide a suitable shelter posture** and relevant manning to provide protection against a sustained CBRN attack or TIM release.
- (4) **Identify personnel and resources** to support the shelter posture and who can undertake recces and surveys of CBRN TIM threats.

AD 80-25

COORDINATING INSTRUCTIONS

9. **Electronic Counter Measures (ECM).** The provision of ECM equipment is a national responsibility and nations are strongly encouraged to provide their troops with this capability. In order to prevent mutual interference between other ECM equipment and communications systems, coordination between TCNs and other agencies is required for Spectrum Management control.

10. **FP measures.** FP measures are issued by Theatre FP based on the prevailing threat, which differs from region to region.

11. **Risk.** The FP posture should be based on risk management, not risk elimination. Deliberate or accidental casualties are a reality of military operations, as are material and equipment losses and an overemphasis in avoiding them may impact adversely on the achievement of the mission. The commander therefore must balance risk within the context of mission accomplishment.

12. **Delivering FP.** All personnel must realise that whilst some elements of FP are delivered by specialists, everybody has a role to play in delivering an integrated FP effect.

SERVICE SUPPORT

13. No change to References A-C.

COMMAND AND SIGNAL

14. **Command.** As per the individual base's requirement.

15. **Signal.** As per the individual base's requirement.

16. Appendices (to be included in the real document):

1. Specific Threat Analysis.
2. Plans for Base's FP Capability Areas
3. SOIs.

FORCE ESCALATION

INTRODUCTION

- Purpose.** The purpose of this Annex is to provide guidance and procedures to attain a standardised approach to Force Escalation (FE). Considered and properly trained FE processes will help to mitigate against the risk of unnecessary civilian casualties. Best practice, properly adapted to local conditions, will help to prevent needless civilian casualties without impacting on the inherent right to self-defence. It must be made clear that good procedures can be followed that prevent needless civilian casualties as well as guarantee no impact on the inherent right to self-defence.
- Background.** Between Aug 06 and Jan 07 there were 73 Suicide-IED attacks reported across Afghanistan against ISAF, ANA and ANP. FE statistics for this same period show that 19 innocent civilians were shot dead and 26 were injured, but only one suicide bomber was shot. There have been incidents of 'blue on blue' engagements by ISAF forces, when overt and covert units have not recognised each other, and civilian road-users from outside of Afghanistan have been unable to comply with ISAF FE procedures because they were unaware of them.
- The Afghan government and population are understandably concerned with the manner in which FE are applied. Unfortunately, no matter how well applied, FE measures may result in unintended civilian casualties. Any civilian casualty is one too many and can only serve to undermine ISAF's mission in Afghanistan. It is for this reason that FE measures must be properly trained and understood, regularly reviewed and, where necessary amended. The local civilian population must be made aware of what is expected from them in order that the risk of them becoming an unintended victim of a civilian casualty incident is minimised.
- Threat and Operational Context.** Other future non-coalition forces can be expected to mount attacks of a deliberate or opportunistic nature against coalition forces employed in their full range of operational duties. Suicide attacks, in all their forms, leave forces particularly vulnerable and require soldiers to act decisively and, if necessary, with lethal force. A challenging operational environment and requirement to make split second decisions may result in coalition personnel resorting to lethal force when, in other circumstances, they may not have done so. A proper (not necessarily Police led) investigation of a civilian casualty incident must take the operational context into account when analysing the appropriateness of the person's reaction.
- Operational End State and Guiding Principles.** The operational end state is to enable individual soldiers to respond proportionately, in a discriminatory manner

AD 80-25

and against targets of necessity, thus preserving the legitimacy of the NATO operational concept, protecting fielded forces and the safety of innocent civilians. From the outset, 3 important guiding principles must be stressed:

- a. First, that any FE process must not create hesitancy or uncertainty in the minds of soldiers, nor introduce a culture of second-guessing by those who have the benefit of perfect, post-incident clarity. It is for the Commanders and soldiers on the ground to decide what is necessary and proportionate by way of self-defence and to act responsibly.
- b. Second, that maximum use of non-kinetic and non-lethal kinetic warning equipment must, where possible, be used to minimise the use of lethal options.
- c. Third, that NATO must promote greater compliance by the civilian population with regard to the instructions given to them by NATO forces. This must be achieved through clear messages and commonality of approach by soldiers using the FE process, supported by a robust, national IO campaign to explain to the Afghan people what is required of them to avoid unnecessary casualties.

PROCEDURES

6. **General.** The purpose of FE is to make the targeted individual or vehicle aware that they are behaving in a manner that is likely to result in the use of lethal force. Therefore, for consistency of understanding by ISAF personnel and civilians, the FE procedures across the whole of the AO must comprise the following common steps and thereby desist from such behaviour:

- a. **Step 1 - Initial Warnings.** Provide unambiguous initial warnings of a VCP, cordon or convoy so that those civilians who are aware of the IO campaign and are willing to comply with its requirements have an early opportunity to do so. Such warnings will include the use of ground and vehicle mounted signs of a standard design approved by NATO, and hand signals by uniformed (and therefore clearly identifiable) personnel.
- b. **Step 2 - Enhanced Warnings.** Use enhanced, targeted warnings and non-lethal force to ensure compliance of civilians who:
 - (1) Are aware of NATO requirements and are willing to comply, but missed the initial warnings for some reason.
 - (2) Are aware of NATO requirements and are unwilling to comply initially, but will comply once shown clear willingness to escalate.
 - (3) Are unaware of NATO requirements and need simple, unambiguous warning of what behaviour is required of them.

Such warnings could include use of pin-flares (proven as the most effective measure before lethal force is employed), high-power air horns, strobe lights,

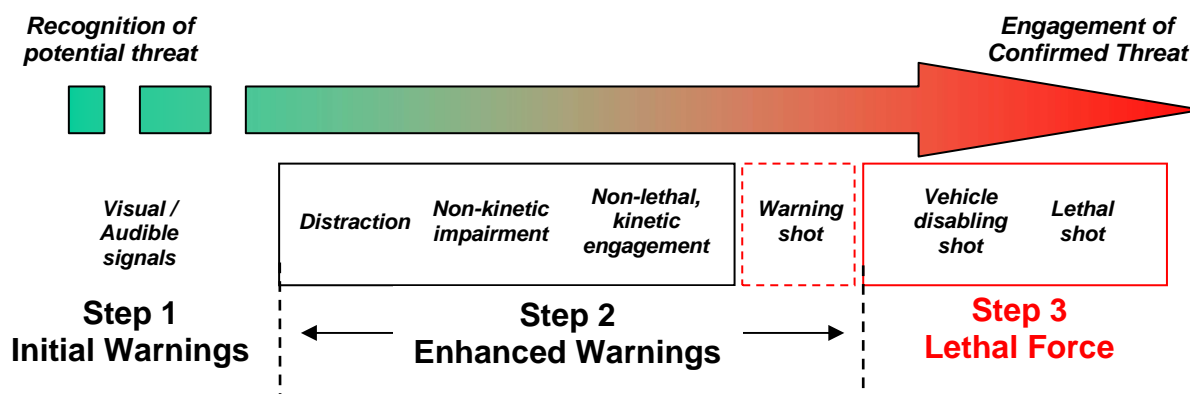
AD 80-25

dazzling lasers, tyre spikes, bean bag guns, paint guns, warning shots with live ammunition, etc.

- c. **Step 3 - Lethal Force.** Use lethal force to engage those civilians who ignore warnings and continue to present a threat.

These steps are summarised diagrammatically overleaf:

Diagram 7 – Force Escalation Process



DIFFICULTIES IN APPLYING THE 3 STEPS

7. **Limitations of Hand Signals in Step 1.** Effective use of Step 1 will reduce the requirement for escalation to Steps 2 and 3, increasing the safety of both NATO forces and civilians. However, NATO troops must be aware that research has shown that the distance at which civilians **can** see hand signals, particularly in poor lighting conditions, is significantly less than the distance at which NATO troops believe they **should** be able to see them.

8. **Problems Associated With Enhanced Warnings in Step 2.** Steps 1 and 3 are relatively easy to define and act on. Step 2 is the area most likely to cause difficulties for NATO troops because:

- a. There can be a very compressed timescale between Steps 1 and 3 when dealing with FE incidents.
- b. Troops lack suitable equipment to take meaningful action at Step 2 (either because it does not attract the civilians' attention effectively or because it delays the soldier taking control of his weapon and moving to Step 3 quickly enough if the situation deteriorates).

9. **Repercussions of Lack of Suitable Equipment for Step 2.** If NATO Forces lack non-kinetic or non-lethal kinetic warning equipment they are unable to take action at the left-hand end and middle of the spectrum of Step 2. They are therefore forced immediately to act kinetically at the right hand end of the spectrum by using warning shots, which can inadvertently stray into Step 3 if, for instance, the soldier's aim is inaccurate or the rounds ricochet and hit an individual. **Again, research shows that because of weapons' flash suppressors and the ambient**

AD 80-25

noise that might be present in the vehicle being warned, these warning shots are not always as obvious to the recipient as ISAF soldiers expect.

Furthermore, there is a high risk of collateral damage from warning shots, and the disabling and killing shots that follow if warning shots are not heeded. The lack of suitable non-kinetic and non-lethal kinetic weapons within NATO forces does not provide the graduated response outlined in the diagram above and therefore increases the risk of early use of lethal force and the unintended collateral damage, injuries and deaths that follow from this.

10. **Main Effort of Force Escalation.** The Main Effort of FE procedures must be focused on Step 1 and the early stages of Step 2, so that the later stages of Step 2 (including warning shots) and Step 3 can be avoided whenever possible.

STANDARDISATION OF FORCE ESCALATION PROCEDURES AND EQUIPMENT

11. NATO cannot mandate FE TTPs or equipment to TCNs because of nations' different equipment, priorities and laws. However, consistency of FE behaviour can be maximised by following the 3-step process, using the approved warning signs, and procuring non-kinetic and non-lethal kinetic equipment that is:

- a. Compatible with existing equipment.
- b. Simple to train on.
- c. Readily available.
- d. Compliant with any national restrictions.
- e. Acceptable to the e.g. Afghan government and population.

12. **Acceptability by e.g. Afghan people.** Lights, strobes, wide-angle lasers, air-horns, etc. are acceptable to the e.g. Afghan people. Paint balls, pin-flares, baton rounds...etc are less so; however, in the absence of non-kinetic options and in preference to the use of warning shots they should be considered by individual nations.

FORCE ESCALATION SIGNS

13. **VCP / Cordon & Convoy Sign.** Signs that comprise a mixture of written and pictorial instructions can be effective, particularly when combined with an effective information campaign. For example, the ISAF-approved sign for use at VCPs and cordons is shown below left. The sign reads "STOP, DO NOT PASS THIS POINT UNTIL INSTRUCTED TO DO SO" in e.g. Pashtu and Dari, and is to be deployed in the direction of the anticipated threat. The ISAF-approved warning sign for vehicles is shown below right. It is mounted prominently on the rear of all overt ISAF military

AD 80-25

vehicles when they leave ISAF compounds and base areas. The sign reads “KEEP BACK” in e.g. Pashtu and Dari.



COMPLIANCE WITH THE LAW IN FORCE ESCALATION INCIDENTS

14. Situations will arise where, because of the imminence of a threat, not all of the graduated levels of FE can be applied. However, in all cases, levels applied must be reasonable and proportionate to the perceived threat, and consistent with the Laws of Armed Conflict and national rules governing the use of force in self-defence. Non-lethal weapons must always remain consistent with applicable treaties, conventions and international law, particularly the Law of Armed Conflict, as well as national and approved Rules of Engagement.

INFORMATION OPERATIONS TO SUPPORT FORCE ESCALATION AWARENESS

15. **General.** In order to ensure the compliance of the civilian population with NATO instructions, it is essential not only that they be informed of coalition intentions, but also that NATO forces employ standardized procedures that are consistently applied. Thereafter, where soldiers witness non-compliance, they will be alerted to possible hostile intent.

16. **IO Campaign.** It is vital that the requirement to obey instructions in the vicinity of NATO forces is clearly understood by the civilian population. This message must be reinforced through the medium of PI and PSYOPS both locally by RCs and theatre-wide by HQ ISAF. The key actions required and messages that must be stressed are as follows:

a. **Key Actions:**

- (1) Inform local leaders and civilians of coalition procedures (hand signals, signs, and verbal warnings) and the impact of not obeying them.

AD 80-25

- (2) Explain to local leaders and civilians the requirement for convoy signs and standardized procedures.
- (3) Promote amongst local leaders and civilians acceptance that NATO FE procedures are there to protect them as well as our own personnel.
- (4) Mitigate the impact of innocent civilian deaths by properly investigating, recording, reporting and dealing with the aftermath of a CivCas incident.

b. **Key Messages:**

- (1) NATO's FE Procedures are in place to protect both civilians and our own personnel from attack, and all coalition soldiers have an inherent right to self-defence.
- (2) Civilians must comply with the instructions of NATO forces and the signs that they display. Time and conditions permitting, hand signals, signs and verbal warnings will be employed before any shots are fired.
- (3) The NATO FE procedures are in accordance with the Law of Armed Conflict and seek to minimize the risk of civilian casualties - these efforts will be more successful with the co-operation of the civilian population.

COMMANDERS' RESPONSIBILITIES

17. **Applicability.** FE procedures will be used in the following situations:

- a. VCPs.
- b. Cordons.
- c. 5m and 20m Checks.
- d. Convoys.

18. **Commander's Approach.** This SOP is to be applied with military judgment appropriate to the prevailing tactical situation. Therefore all local commanders have to establish TTPs for FE by day, night and bad weather conditions. VCPs, cordon positions and patrol routes should be planned with great care so as to gain maximum protection from available terrain and infrastructure. Commanders must guard against routinely using the same routes or positions for cordons and VCPs: 5m and 20m checks should always be conducted. The local Commander should make efforts to engage with civilian cultural advisors and security forces in order to confirm that local TTPs will deliver the required warning messages to the local population.

AD 80-25

19. **Training.** The procedures contained within this SOP will protect both deployed forces and the NATO mandate, and are to be practised by all personnel as part of pre-deployment and in-theatre training.

20. **Reporting.** If a FE Incident occurs then local commanders are to report it up the chain of command.

CONCLUSION

21. This SOP provides direction on the procedures to be employed in order to reduce the number of incidents in which coalition personnel shoot innocent civilians in the mistaken belief that they present a genuine threat. It provides commanders with training and operating framework for reducing the likelihood of unnecessary FE incidents, but is not prescriptive and stresses that it is for local commanders and soldiers on the ground to act responsibly and within the law at all times. It also acknowledges the inherent right to exercise lethal force in self-defence.

TACTICAL LANDING ZONES

1. **Introduction.** To maximize the rapid concentration of forces and capabilities offered by air assets a commander might wish to use aircraft independent of forward operating bases. To achieve this he can establish a Tactical Landing Zones (TLZ) that can be located anywhere within an AO and activated only when and for as long as necessary.
2. Air operations at and around TLZs face the threats of Surface-To-Air Fire (SAFIRE), Man Portable Air Defence Systems (MANPADS), Small Arms Fire (SAF), Anti Aircraft Artillery (AAA), IEDs, mines and physical assault. This Annex has been included to outline FP measures that can ensure the integrity of TLZs against all threats.
3. **Definitions.** The following definitions will be used in TLZ security procedures:
 - a. **Aircraft Close Defence** is the securing of the aircraft and its parking ramp against physical incursion.
 - b. **Ground Defence Area** is an area established around an installation IOT prevent and / or disrupt both direct and indirect attacks by non-coalition forces against facilities, equipment and personnel. It will begin at the perimeter of the installation (if one exists) and extend to the maximum effective range of any ground-launched weapon system that J2 staff assess might be a threat to that facility or mission.
 - c. **Outer Security** is the provision of patrols and / or observation posts to maintain the integrity of the approach and departure routes and aircraft operating surfaces prior to aircraft arrivals or departures.
 - d. **TLZ** is a landing area with a natural surface or an existing airfield with poor infrastructure.
 - e. **TLZ Ground Protection Force** is any coalition sub-unit trained in basic infantry skills, with weapons and communications equipment that are capable of mounting patrols, observation posts and search operations. The ground protection force should receive TLZ security training prior to the performance of such duties.
 - f. **TLZ Search** is a physical search on foot of the runway and aircraft operating surfaces by personnel trained to detect and react to IEDs and / or non-coalition activity. A TLZ search must also include buildings and facilities within 50m of where aircraft will pass or be parked.

AD 80-25

g. **TLZ Secure** is when the runway, operating surfaces and any facilities within 50m of the runway and operating surfaces have been physically searched and then secured against incursion, and a ground protection force is in place to provide close defence (when required) and external security.

4. **Preparation.** The following need considering during the TLZ prep phase:

a. **TLZ Selection.** The selection of a TLZ will be conducted by air operations personnel based on whether the runway is long enough and firm enough for the aircraft to be operated. FP personnel should be involved in any planning and reces because if there should be a choice of TLZ the deciding factor might be FP capability versus risk.

b. **Frequency of Use and Associated Threats.** The frequency with which a TLZ may be used will drive the threats it faces. If the runway is rarely used, non-coalition forces may employ mines rather than wait to use MANPADS.

c. **Balance of Risk.** A TLZ might be activated without prior ground clearance if the mission and level of risk acceptable dictate. However, the integrity of aircraft operating surfaces could not be guaranteed, so the element of surprise might need to be traded off by the arrival of ground troops to clear the area prior to the arrival of aircraft. This risk decision is owned by the commander of the air mission.

d. **Specialist Equipment.** If any specialist aircraft handling equipment is required, consideration must be given to providing FP of it and its operating personnel whilst in transit to the TLZ.

5. **Establishing FP at a TLZ.** TLZ security operations are considered in 3 distinct phases and if local Air Traffic Control (ATC) is present the procedures must be coordinated with them.

a. **Prior to aircraft arrival:**¹

(1) Contact ATC to determine aircraft arrival time, approach direction and time-on-ground² information. Factors that might affect the FP footprint are:

(a) **Approach.** This will be driven by crew proficiency, load carried, weather and familiarity with the TLZ. The aircraft's captain will also seek to minimise his exposure to ground-based threats by adopting a profile that maximises the performance of any defensive aids system carried by the aircraft. Knowledge of

¹ If there are no communications with the aircraft, Prior Permission Required (PPR) procedures must have been applied for.

² Affected by whether this is an engine running off-load or shutdown.

AD 80-25

the aircraft's approach direction is important if the FP forces need to counter the MANPADS or SAFIRE threat. Furthermore, if the aircraft captain changes a pre-arranged approach without notice he must understand that the FP force might not be able to re-establish the necessary protection in time.

(b) **Taxiing.** Ideally, the aircraft should land, drop or pick up its cargo, turn around and take off in the opposite direction, or take off using the remaining runway length. However, runway size, the wind speed or need for specialist aircraft handling equipment might preclude this and the aircraft could spend significant periods of time taxiing around the aircraft operating surfaces. Careful positioning of loads and handling equipment should minimise this exposure.

(c) **Departure.** As with the approach, the aircraft captain will seek to minimise his exposure to any threats from the ground, and a generic departure will aim to gain height as quickly as possible to escape the SAFIRE envelope coupled with manoeuvre. The same considerations for mitigating MANPADS / SAFIRE threats apply as for the approach.

(2) Determine time phasing requirements to ensure "TLZ secure" is achieved prior to aircraft arrival.

(3) Conduct a TLZ Search iaw Appendix 1. This must be accomplished in sufficient time to ensure that an aircraft can be diverted should an incident occur or a threat be found.

(4) Deploy sufficient assets to ensure that areas that have been searched cannot be re-entered or interfered with.

(5) Deploy "outer security" elements and if conducting specific counter-SAFIRE / MANPAD operations deploy an area protection force.

(6) If required pre-position (but don't deploy) "aircraft close defence" elements³.

(7) Inform ATC when "TLZ Secure".

(8) Maintain communications with ATC IOT "wave-off" the aircraft in the event of an incident.

b. **Aircraft on the ground:**

³ Aircraft Close Defence Element personnel must be in possession of hearing protection, eye protection (goggles) and have no accoutrements liable to be sucked into aircraft engines. In addition they must have practised sending and receiving applicable aircraft close defence hand signals.

AD 80-25

- (1) Immediately prior to the aircraft's arrival at its off-load location deploy aircraft close defence elements, unless the area is already secure or ramp protection is not required⁴. Co-ordinate activities with any on-board aircraft security element and establish responsibilities (on-board security personnel should be TACON the local FP commander).
- (2) Confirm with ATC that the aircraft has no technical problems.
- (3) Confirm with patrols and observation posts that the TLZ remains secure.
- (4) Be prepared to "wave-off" the aircraft in the event of an incident.⁵
- (5) Maintain communications with the aircraft (through ATC if necessary).
- (6) Permit only authorized personnel to approach the aircraft.
- (7) Prepare for aircraft departure particularly if an 'engines running off-load' is being completed.
- (8) Ensure the aircraft is guarded and properly secured if remaining on the ground.
- (9) Maintain security within the close defence area and local area.

c. **Actions prior to aircraft departure:**

- (1) Contact ATC to confirm aircraft departure time and direction.
- (2) Determine time phasing requirements to ensure "TLZ secure" is achieved prior to aircraft departure, unless already secure.
- (3) If there is any suspicion that the defensive perimeter has been penetrated conduct a "TLZ search" iaw Annex A (this must be accomplished in sufficient time to ensure the aircraft's departure is not delayed).
- (4) Deploy sufficient assets to ensure areas searched cannot be re-entered or interfered with.

⁴ The requirement for Ramp security will need to be pre-determined with ATC, if available, and/or the arrival aircraft.

⁵ "Wave-Off" should be conducted through ATC. However, in the event of a communication failure a backup and pre-notified signal must be available: flares could be used but need to be pre-coordinated with ATC and the arriving aircraft.

NATO RESTRICTED
Releasable to PfP

AD 80-25

- (5) Inform ATC when "TLZ Secure".
- (6) Maintain communications with ATC until the aircraft has cleared the TLZ and secured areas.
- (7) Re-deploy forces as appropriate.

APPENDIX:

1. Search Consideration for TLZs

SEARCH CONSIDERATIONS FOR TLZs

INSURGENT WEAPONS AND TTPs

1. **Threat.** The following threats exist on TLZs and need considering as they will help troops undertake a better directed search.
 - a. **CWIED (Command Wire IED).** This type of threat is time consuming to set up effectively because of the need to dig-in or otherwise hide the command wire if it is not to be easily spotted, and is therefore most likely to be used at a location that is known to be used by ISAF aircraft but not guarded routinely. If the device has been put in place days or weeks before it is intended for use, the camouflaging of the command wire might have blended into the background extremely effectively and it is therefore critical that searches of aircraft operating surfaces and the ground to the sides of them are conducted on foot. The insurgent needs to have line of sight to the device to decide when to detonate it, so likely positions of observation need to be checked and cleared.
 - b. **RCIED (Radio Controlled IED).** The use of RCIEDs is common in Afghanistan due to the control that it offers non-coalition forces. Again, line of sight between the firing point and the TLZ is needed to ensure detonation at the correct time. Therefore, likely firing points need to be checked and cleared.
 - c. **LCIED (Light Command IED).** This would be impractical on an open TLZ but could possibly be used inside surrounding buildings or fuel / water tankers.
 - d. **Time Delay.** A time delay device offers a good opportunity to attack as it can be placed and left so that no one is at the scene. However, unless non-coalition forces have precise intelligence on aircraft movements the limitation of this tactic is that the insurgent will rely on luck that there are troops or an aircraft in the area when the device explodes.
 - e. **VOIED (Victim Operated IED).** A VOIED is an easy option for the insurgent as he will be away from the scene at the time of detonation and because this technique relies on positive action for initiation, if the device detonates it will have an effect. The limitation of this technique is that the device might be activated inadvertently by local nationals unless they are warned of its existence. VOIEDs could be initiated by tripwire, pressure or pressure release depending on the target, terrain and intent and could be

AD 80-25

improvised or purpose built (e.g. mines). Such devices could easily be buried under gravel or dirt runways.

f. **SIED (Suicide IED).** The threat from person- or vehicle-borne suicide bombers must be countered by effective control of access to aircraft and personnel and use of stand-off and robust force escalation procedures.

2. Search troops must have an awareness of the environment that they are operating in and what could have been achieved by non-coalition forces, e.g. if the TLZ surface is asphalt or concrete rather than matting or compact gravel it would be more difficult time and time-consuming to dig-in a device near the runway, so some other tactic might be more likely.

3. **Search Procedures and Aids.** The procedures for the search will depend on factors such as time and number of search personnel available, familiarity with the area, terrain, size of the area to be covered, and freedom of tactical movement.

4. Pre-search considerations should include:

a. A CJ2 intelligence update to ensure that all personnel are aware of non-coalition activity, capability and intent in the area.

b. A review of existing TLZ security measures.

c. Use of available technology to complement physical searches. The use of ECM (Electronic Counter Measures) should be considered whilst carrying out the search, but must be cleared through the ATC commander prior to use in case they interfere with airfield landing aids.

d. Use of other agencies to assist, e.g. search dogs, helicopters or specialist imaging units.

5. Considerations when conducting the search should include:

a. A check of all established boundaries to confirm there are no obvious security breaches.

b. In addition to the individual searchers' eyes there are various viewing devices that can be used to assist the search such as binoculars, NVGs and thermal cameras. Digital cameras or video can also be used to take pictures for comparison following subsequent checks and searches.

c. Areas must be searched **on foot**, as soldiers cannot clear an area to the required standard by driving through or along it. *(NB: a C-130 of the Royal Air Force was destroyed by an IED as it landed at a TLZ in Iraq in 2006. In this instance the large, daisy-chain device had not been spotted by searching troops, who conducted a pre-arrival visual check of the area by*

NATO RESTRICTED
Releasable to PfP

AD 80-25

driving their armoured patrol vehicles along the runway rather than dismounting and thoroughly searching the runway and its edges on foot).

d. Soldiers conducting searches should work in pairs to ensure that nothing is missed, talking to each other during the operation to ensure that any queries are aired and checked.

e. Due to the possible use of directional devices as much of the TLZ as possible must be searched. The tactical situation will dictate how much can be achieved (mines, etc).

f. Don't allow soldiers to set patterns whilst carrying out the search preparation as non-coalition forces may be watching.

g. Any buildings within the search area that are not used routinely can be secured and security-sealed to ensure that no one has entered since the last check.

h. The TLZ can be split down into a number of different search areas (a grid search), that is marked on the ground, mapping and aerial photography. Each area can then be made the responsibility of nominated personnel to ensure that:

(1) The whole area is searched.

(2) It is known when an area has been declared clear.

(3) Personnel can learn the peculiarities of that area so that they can notice the smallest change in subsequent checks.

i. Check for signs of disturbed ground, particularly on gravel runways, or look for repairs to tarmac surfaces that might indicate buried IEDs or mines.

6. If a device is found, EOD need to be on hand to dispose of the device.

1. **FORCE HEALTH PROTECTION - OCCUPATIONAL HEALTH & SAFETY**

a. **Overview.** Occupational health and safety is an integral part of FHP and FP overall. It is also an inherent responsibility of commanders. The military operating environment typically creates an environment that is conducive to the occurrence of accidents and injuries. A wide range of tasks, some of which might not be typical of those normally undertaken by military personnel, will require commanders at all levels to place increased responsibilities and duties on their subordinates. It is essential that combat power is conserved and not degraded by accidents and injuries.

b. This Annex provides an example of possible minimum standards required of commanders at all echelons for establishing their safety programmes. The key concepts to observe are:

- (1) Accidents are an impediment to the mission.
- (2) Risk decisions must be made at the appropriate level.
- (3) Risk Management must be continuous.
- (4) Performance to the correct standard is mandatory.
- (5) Corrective action must be swift and appropriate.
- (6) Safety success must be recognised immediately.

c. There are many significant non-battle injury threats within the theatre such as road traffic accidents, weather-related injuries, casualties from mines and UXOs, etc. It is therefore imperative that units exercise appropriate countermeasures to these threats wherever possible and educate their soldiers about them and their mitigation. Other procedures that require defining include:

- (1) Unsafe working procedures.
- (2) Proper use and wear of personal protective device.
- (3) Driving techniques and convoy procedures.
- (4) Health awareness, weather-related injuries.
- (5) Sports injury and prevention.

AD 80-25

- (6) Mine Awareness.
- (7) Fire Safety.
- (8) Weapons and Ammunition Safety.
- (9) Hazardous Material Concerns.
- (10) Accident Reporting.
- (11) Newcomers' Safety Briefing.

d. **Workplaces & Equipment.** Occupational Health and Safety Programmes are to meet the Standards laid down by EU Directives as implemented by the National Contingents' Governments. Although these standards will inevitably conflict with certain activities conducted by Armed Forces, the health and safety of soldiers and civilian employees must be protected as far as possible in accordance with the objectives of these directives. In this case an increased level of supervision based on a firm risk assessment will compensate for any necessary derivation. When a conflict arises between this SOP and national safety policies, the most restrictive measure will apply.

- (1) **Workplaces.** Workplaces should so far as is practicable meet the following criteria:
 - (a) Provide safe means of access and exit.
 - (b) Be free from risk of fire.
 - (c) Be adequately ventilated to provide fresh air and remove any fumes, dust and fibres. Ventilation may be natural (e.g. via windows or vents) or mechanical (e.g. via air conditioning machinery or extractor fans).
 - (d) Have all hazards identified and effectively controlled.
 - (e) Be adequately illuminated for the tasks being undertaken (e.g. appropriate general lighting for safe movement around the workplace and where necessary additional localised lighting of desks, work benches and computer stations.
 - (f) Be equipped with blinds or shutters to protect occupants against weapon splinters and shrapnel, and to prevent the interior from being viewed from the exterior during the hours of darkness.

AD 80-25

- (g) Be adequately heated or cooled for the tasks being undertaken. Where temperature control is not possible, such as outdoor vehicle parks, there should be a refuge nearby where personnel can warm or cool themselves at periods specified by their supervisors.
- (h) Have all required signs in place, i.e. areas of restricted access, fire exits, hazardous material stores, etc.
- (i) Provide personnel with protective clothing, safety eyewear, hazardous noise exposure prevention and respiratory equipment where appropriate.

e. **Equipment.** All equipment brought into or procured for use in-theatre must comply with the general criteria detailed above. In addition all equipment should be:

- (1) Operated only by qualified personnel (i.e. formally trained and current in the operation of that piece of equipment).
- (2) Stored, maintained and used in accordance with manufacturers' instructions.
- (3) Repaired only by personnel qualified and competent to do so.
- (4) Correctly wired with an undamaged power cable (in the case of electrical items).
- (5) Fitted with hand/eye guards where appropriate and marked with directions that personnel are to use them.
- (6) Checked prior to use in accordance with any specified users' checks in order to ensure that they are in good order.

f. **Accident and Injury Reporting.** Reporting of occupational injuries (i.e. injuries that occur while performing a duty) to the troop contributing nation is a national responsibility and should follow national rules. However, the tracking of the incidence and type of injuries occurring among NATO operational forces is an important component of overall operational and deployment health surveillance. This data is used to better implement force health protection recommendations and injury prevention measures. It is therefore imperative that injuries and injury statistics be reported to the cognizant NATO operational Commander Medical Advisor via the established EPINATO reporting process. It is also suggested that each Role 1, 2 or 3 medical facility appoint a representative to assist in the timely and proper reporting of occupational injuries.

AD 80-25

g. **Safety Programme.** The following elements form the pillars of FHP – Occupational Health & Safety:

(1) **Education.** All military and deployed NATO civilian personnel are to be provided with basic and refresher courses in Occupational Health & Safety as it pertains to living and working in the operational environment.

(2) **Information Campaign.** Safety issues will be publicised at regular and frequent intervals using all media sources.

(3) **Accurate Accident Reporting.** Accident reports must be honest and comprehensive and should be used to focus on what happened for the purpose of subsequent accident prevention, rather than to support disciplinary procedures.

(4) **Host Nation Activities.** Personnel should be briefed on specific HN activities so that their impact can be taken into consideration when planning.

h. **Hazardous Material (HAZMAT) and Hazardous Waste HAZMAT** is any fuel, oil, lubricant, solvent, paint, etc. that could be harmful to personnel or the environment if not properly handled, used and disposed of. This does not include ammo. Hazardous Waste is any substance or material intended for disposal, no longer in use, or abandoned, that represents a potential risk to health upon exposure.

(1) **Concept.** The prevailing concept for dealing with HAZMAT and Hazardous Waste must be one of proper shipment, transport, storage, use, and waste disposal rather than emergency clear-up operations. Prevention of unhealthy exposure or damage to the environment is cheaper and easier than cure. Also, thought is needed about the returning of equipment and land to the HN, as well as maintaining a healthy operating environment.

2. **FIRE PREVENTION AND FIRE SAFETY.** While Fire Safety in regards to Burn injury prevention does fall under the auspices of FHP-Occupational Health and Safety, prevention of fire does not. When it comes to fire prevention equal concern regarding this effort is also directed towards the protection of valuable property, supplies, and other material assets.

a. **Fire Marshalls.** Fire marshals will support base camp commandants, as applicable, by conducting periodic fire inspections in bivouac areas, maintenance areas, and buildings. Inspection results will be kept on file,

AD 80-25

including the results of immediate corrective actions taken (such as replacing smoke detectors, counselling soldiers caught smoking in the billets, etc).

b. **Causes of Fire.** The main causes for concern with regard to Fire Prevention are given below and need specific rules to govern the risk they may pose, especially in austere, hastily build camps because of number of tents and temporary wooden buildings that may be present.

- (1) Cooking devices.
- (2) Electrical devices.
- (3) Fuels and other flammable liquids.
- (4) Smoking.
- (5) Privacy screens in private rooms.
- (6) Open flame devices, such as candles.

c. Areas in need of special attention to ensure continued fire prevention are:

- (1) **Fire Lanes.** Fire Lanes throughout the billeting and administrative areas are to be kept clear at all times.
- (2) **Fire Extinguishers and Fire Alarms.** Fire marshals are to ensure that all fire extinguishers and fire alarms are maintained in a serviceable condition.
- (3) **POL and ammo storage areas** need signing to order: 'No Smoking within 15 m (50 feet)' in red letters on a white background.
- (4) **POL Vehicles.** POL vehicles will be bonded and grounded at field locations.
- (5) **Bonding and Grounding.** Bonding is accomplished by connecting two or more electrically conductive objects so that their electrical charges equalize. Grounding (earthing) is accomplished by connecting an object to the ground so that the object's electrical charge can be dissipated. Bonding and grounding reduce the chances of sparking (arcing).
- (6) **Fire Extinguishers.** Fire extinguishers must be located next to all POL points and storage locations.

AD 80-25

(7) **Fuelling.** Vehicle operators must turn off vehicle engines when being refuelled.

(8) **Smoking.** Smoking cannot be allowed within 15m (50 feet) of vehicles carrying explosives or flammable fuels.

(9) **Gasoline Storage.** Gasoline in portable containers will be stored in stacks. Each stack will not exceed 4,000 litres (1,000 gallons) and will be at least 1.5 meters (5 feet) from the next stack. Stacks will not be closer than 15 meters (50 feet) to occupied tents, buildings, warehouses, or combustible storage areas, and when possible will be located at lower elevations than bivouac areas. Gasoline and other flammable fuels with a flash point of 100°F/35°C or less will not be stored in tents, buildings, or other structures with closed sides. Gasoline and other flammable liquids will not be used to start solid fuel fires or used as a cleaning solvent unless specified for this purpose. Other fuel considerations include:

(a) **All fuel cans** to have serviceable gaskets.

(b) **Field stoves and ranges** with attached fuel tanks are to be allowed to cool off for at least 30 minutes before being refuelled.

(c) **Vehicles, trailers, and temporary storage areas** containing packed or bulk flammable and combustible liquids are to be located at least 15 meters (50 feet) from vehicles loaded with explosives and ammunition and structures.

(d) **Incendiary Devices.** Incendiary devices for destroying classified material are to be stored so that any accidental ignition will not be hazardous. Installing explosives and pyrotechnics for additional security of classified material is prohibited.

(e) **Pyrotechnics.**

(f) **Electrical Installations.** Only trained personnel can be allowed to install electrical wiring and equipment.

COUNTER SAM OPERATIONS

OUTLINE

1. **Introduction.** Successful Airfield Operations are key to achieving rapid concentration of forces in response to changing threats, but aircraft are particularly vulnerable to non-coalition activity when on the ground and during landing and take-off. The loss of a large transport aircraft with an attendant mass casualty event could have catastrophic political impact on the coalition mission and remains a very real risk. This Annex details proven measures to protect aircraft when approaching and departing airfields.

2. **Threat.** The most potent surface to air threat comes from first and second generation man portable air defence systems (MANPADS) such as SA-7 and HN-5, which remain serviceable long after components such as battery packs might have been expected to fail, but which have had little impact on recent operations because of poor operator skills and the defensive aids suites fitted to many aircraft. The most likely threat comes from small arms, crew served medium and heavy machine guns, and rocket propelled grenades, either used separately or grouped together in well-planned ambushes, a tactic that has been used with considerable success against rotary wing aircraft and could be used against slow-moving fixed wing aircraft on predictable flight paths, for example during approach and departure.

3. TTPs need to be developed with air traffic control to account for the volume of air movements, the purpose of particular movements and the strategic value to the insurgents' IO campaign if they were destroyed, as well as the FP resources available (there will be other conflicting priorities).

4. **Tactical Area of Responsibility (TAOR).** A TAOR is needed to define the ground around an installation established IOT prevent and / or disrupt both direct and indirect attacks against coalition facilities, equipment and personnel. It will begin at the perimeter of the installation (if one exists) and extend to the maximum effective range of any ground-launched weapon system that J2 staff assess might be a threat to that facility or mission. The TAOR may require political-level authorisation so TCNs can deploy their troops into and have HN permission to carry out operations on this land.

5. **Planning Considerations.** The local FP commander has the responsibility for devising detailed plans following liaison with a range of agencies to ensure coherence (e.g. ATC, flanking units, air ops, etc.) although ultimately the airfield commander will own the risk. The effectiveness of counter SAFIRE plans rely on established and practised TTPs to guarantee effective operations by GDA FP assets, ATC and aircrew, and a thorough understanding of the enemy's weapons and operators capabilities, such as:

AD 80-25

- a. Acquisition criteria (e.g. optical/thermal/radar).
- b. Horizontal and vertical range.
- c. Launch parameters (day/night/ability to engage a crossing target or limited to tail chase only).
- d. Launch signature (first and second stage motors, smoke, and dust).
- e. Guidance mechanism: unguided (such as guns or RPG), passive (heat seeker such as SAM-7), or active (on-board laser or radar system, or operator controlled guidance such as Blowpipe).

6. **Generic Threat Data.** Specific threat data should be obtained from CJ2 staff, but the following table offers generic guidance on common threat systems.

THREAT	MIN RANGE	MAX RANGE	MAX ALT	VISUAL FEATURES
SA-7b	0.7 km	4.5 km	12 500 ft	Grey/white corkscrewing plume
SA-14	0.7 km	4.5 km	12 500 ft	Grey/white shallow corkscrewing plume
SA-16	0.3 km	7.0 km	16 500 ft	Grey/white straight plume
SA-18	0.3 km	7.25 km	21 300 ft	Grey/white straight plume
STINGER BASIC	0.3 km	5.0 km	15 100 ft	Grey/white straight plume
SMALL ARMS/RPG	-	1.0 km	3 000 ft	Nil
MED CALIBRE	-			Perhaps dust plume from recoil

Note: An elevated firing position will increase the range of a MANPADS by about 500 metres for every 1000 ft of height gain due to decreased air resistance for the missile to penetrate.

7. **Launch Sites/Firing Points.** Effective launch sites will be defined by weapon characteristics in accordance with the following generic criteria:

- a. Within weapon range and altitude boundaries.
- b. Offering covered or high speed access/egress routes as weapon systems and trained operators are high value assets to the enemy and he will not wish to expose them to risk for longer than necessary.
- c. Offering a good view of the flight path to allow target identification and time to ready the weapon for firing (*Note: some weapons have a finite and relatively short battery life once the system is activated for firing, though operators have been known to overcome this limitation by adapting car batteries for use*).
- d. Offering protection to the firer from recoil or reflected back-blast from rocket motors (ideally a flat, open area).
- e. Minimising launch signature from dust or other loose material (*Note: some MANPADS firers have wetted the launch area prior to firing to minimise*

AD 80-25

dust, or used tarmac/concrete surfaces).

8. **MANPADS Tactics.** The most common type of MANPADS is a heat-seeker, which is ideally sited for a side-on moving to rear hemisphere engagement. This maximises the potential of the seeker head to pick up an aircraft's exhaust plume and minimises the chance of visual warning by the aircraft crew. The best times for a heat-seeker MANPADS engagement are dawn and dusk because the target aircraft stands out better against the cooler ambient temperatures for the seeker head to find, and the firer can move into or out of position during darkness. A visually-acquired MANPADS engagement typically needs 10-15 seconds to complete the acquisition / seeker activation / firing sequence.

9. **Small Arms Tactics.** Small arms are best sited directly on the flight-path to allow a head-on / overhead / tail-on engagement. This minimises the calculation of deflection (lead angle) and offers the best opportunity for hits. The advantage of waiting until the aircraft is overhead is that more rounds can be fired before the aircrew are likely to realise they are being engaged and can take avoiding action.

10. **Identification of Hotspots.** A combination of a thorough map appreciation, on-site recce and understanding of SAFIRE weapon characteristics will allow the FP commander to identify the best possible launch sites / firing points, known colloquially as 'hotspots'. Likely hotspots might include:

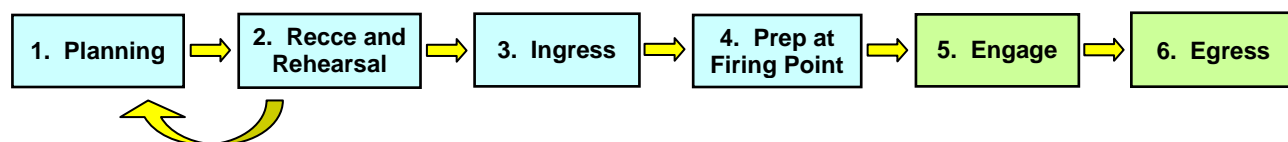
- a. **Roads:** for ease of access/egress and minimising of launch signature.
- b. **Built-up Areas:** offer good visibility and firing points from flat-topped buildings, and good ingress/egress if there is a compliant local population.
- c. **Waterways:** rivers and lakes can be used for ingress/egress, as barriers to pursuit (particularly if crossing points are booby-trapped), and in the case of shallow water can be used as a firing point to minimise launch signature.
- d. **High Ground:** offers good visibility and can increase the weapon system's engagement envelope.

11. **Threat Period.** The threat to air activity is bounded by space and time as the threat exists only when aircraft are present on arrival and departure, but the time necessary for FP assets to adopt a secure posture must always be factored into the planning cycle.

COUNTERING THE THREAT

12. **Adversary Attack Cycle.** For planning purposes a potential adversary attack cycle might be as follows:

AD 80-25



Disruption of any of the first 4 stages is likely to either negate the attack or force the operator to move to a less effective firing position.

13. **Plotting the Firer and Weapon Trail.** It is very difficult to stop an unexpected and well-planned attack from taking place and the best chance of success is to combine the use of intelligence with selected FP assets in order to break the attack cycle in the early stages. SAFIRE weapons systems and their firers are high value assets to an enemy and will often be brought independently to the firing point immediately prior to firing. Both will leave a trail, which if detected could provide an opportunity for interception.

a. **Firer Trail.** Tracking the firer means building up the profiles of known players with particular skills who have links to known insurgents or previous attacks. These players should then be monitored for unexpected movement patterns. Unless strong relations are built-up within local communities to provide such information, progress in this area will be very difficult. The distant training camps that provide such specialist training will normally be monitored through national and theatre-level assets.

b. **Weapon Trail.** Because of their symbolism and tactical value, SAFIRE weapons might be stored under some form of quartermaster system and might need to be serviced at regular intervals. The weapon might be moved from storage and moved to a temporary holding area shortly before use, and might be moved by the trained operator or a more expendable member of a firing team. Again, good links with the local community might generate information on SAFIRE weapon locations and movements.

14. **Interdiction of Approach Routes.** Because of their size many SAFIRE weapons are moved by vehicle for speed and concealment. This gives a limited opportunity to interdict the weapons as they are moved along a pre-determined movement corridor, so routes to and from hotspots should be pre-determined, and any choke points or common ground identified. FP assets would then be in a position to interdict such points by observation, overt and covert patrolling, VCPs and heli-borne assault.

15. **FP Commander's Mitigation Strategies.** The FP commander is faced with 2 options to mitigate the SAFIRE threat: firing point denial or Counter Insurgency (COIN).

a. **Denial.** The general principle of counter SAFIRE ops is to deny the competent operator the terrain from which an engagement can be made within the threat weapon system's parameters, and with MANPADS this area can be extended to many square kilometres. The key terrain should be identified through close liaison with CJ2 staff and the production of an Intelligence

AD 80-25

Preparation of the Battle-space (IPB). The disadvantages of this approach are that over time patterns will inevitably be set that the enemy might exploit, it can be resource intensive, and FP troops would need to deploy many times without knowledge of success, whilst the enemy would need to penetrate successfully only once. Launch sites can be dominated either by FP forces occupying them, or by observation linked to direct/indirect fire effect. This latter course of action allows a relatively small force to dominate a number of potential launch sites, but depends for success on effective surveillance, communications and fire control.

b. **COIN.** In the COIN approach the FP commander seeks to create a more strategic effect by information gathering in the local area in order to interdict SAFIRE weapons and firers early in the adversary attack cycle. He will need to reward the compliant (e.g. through CIMIC and other aid) whilst at the same time attacking the minds of the non-compliant and their supporters through more aggressive tactics. The disadvantages of this approach is that it can take considerable time to achieve, must be consistent, needs a constant source of reliable intelligence, requires subtlety of thought, and needs a viable reward / punishment mechanism.

In practice the FP commander is likely to use a combination of these methods: an initially aggressive domination of the hotspots coupled with a robust, intelligence-led TAOR-wide COIN campaign, leading eventually to an environment where the trust and goodwill of the local population has been gained and the support for insurgents undermined.

16. **ATC, Air Ops, Air Crew and FP Coordination.** Detailed coordination is required on a routine basis between Air Ops, ATC, Air Crew and FP IOT design, rehearse and implement local procedural countermeasures as required. Coordinated communication between ground and air assets will facilitate the efficient collective response of the GDA FP assets, ATC, the subject aircraft and other aircraft airborne in the vicinity.

17. **Air Threat States.** The Theatre Air Threat States, their definitions (owned by CJ2) and FP mitigation measures are defined as follows:

Air Threat	Threat to Air Ops (as defined by CJ2)	FP Mitigation Required
HIGH	Air operations are severely threatened. Enemy forces are actively targeting air operations. Air operations in the area should be reconsidered or significantly mitigated.	General mitigation procedures to be adopted and all firing points (from the IPB) are to be denied the operator during specified aircraft movements. The coalition would need to provide additional guidance and manage any intended air movement on a case-by-case basis.
SIGNIFICANT	Air operations are threatened and preventative measures must be adopted to protect air assets.	General mitigation procedures to be adopted and the most likely firing points (from the IPB) are to be denied the operator.

NATO RESTRICTED
Releasable to PfP

AD 80-25

MODERATE	Minor threats to air operations exist and some preventative measures may need to be taken to mitigate the threat.	General mitigation procedures to be adopted.
LOW	Threats to air operations are minimal and very limited in nature. Very little mitigation required.	General mitigation procedures to be adopted.
NEGLIGIBLE	There is no threat	No requirement.

BASIC PROCEDURES

18. Detailed TTPs for the arrival and departure of aircraft are required, and they should consider the following points:

- a. Establish the local SAFIRE threat.
- b. Establish at what point (height and distance from the runway) a particular aircraft type enters/departs the engagement envelope of a particular threat type.
- c. Define general mitigation procedures such as:
 - (1) Routine checking of likely firing points.
 - (2) Varying aircraft approach/departure timings and headings – the majority of in-theatre threats rely on visual acquisition and aiming so one of the best countermeasures is to fly by night with all lights extinguished.
 - (3) Routine engagement with local nationals to gain information on hostile activity and potentially recovery of cached SAFIRE weapons.
- d. Understand the effects of weather on MANPADS engagements and use them to advantage: rain and low cloud can inhibit acquisition and seeker lock-on, and sunlight around the edges of broken cloud may generate sufficient IR energy to distract a missile seeker head.
- e. Deploy to counter SAFIRE positions in time to deter/disrupt enemy activity.
- f. Ensure TAOR FP assets have direct communications with ATC throughout the operation to confirm when the area is secure and any changes to aircraft movements (time or direction).
- g. Establish aircraft wave-off procedures in case of communication failure.
- h. Establish 'actions on' if aircraft is engaged by SAFIRE.
- i. Define debriefing requirements post any attack.

AD 80-25

APPENDIX:

1. Plotting the Safire Trace

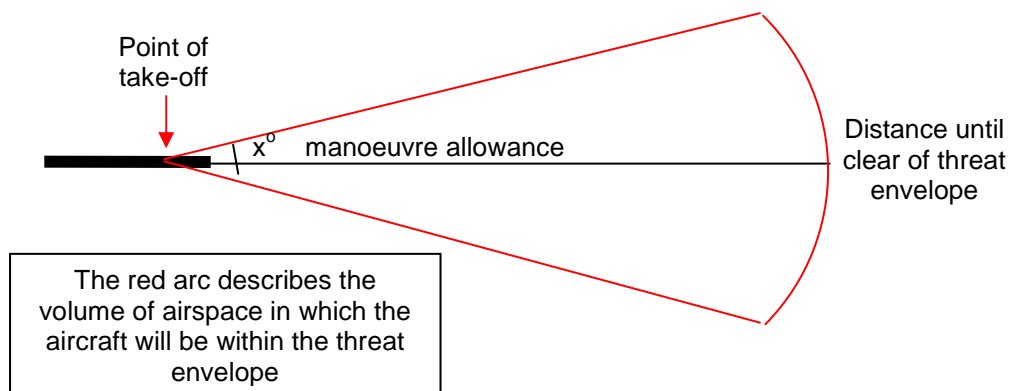
PLOTTING THE SAFIRE TRACE

1. This guide is designed to enable the FP Commander to determine the area of ground that must be dominated in order to minimise the risk of a SAFIRE event during aircraft arrivals and departures. It is a generic guide and specific CJ2 support will be required to cater for specific aircraft profiles and threat weapon systems.

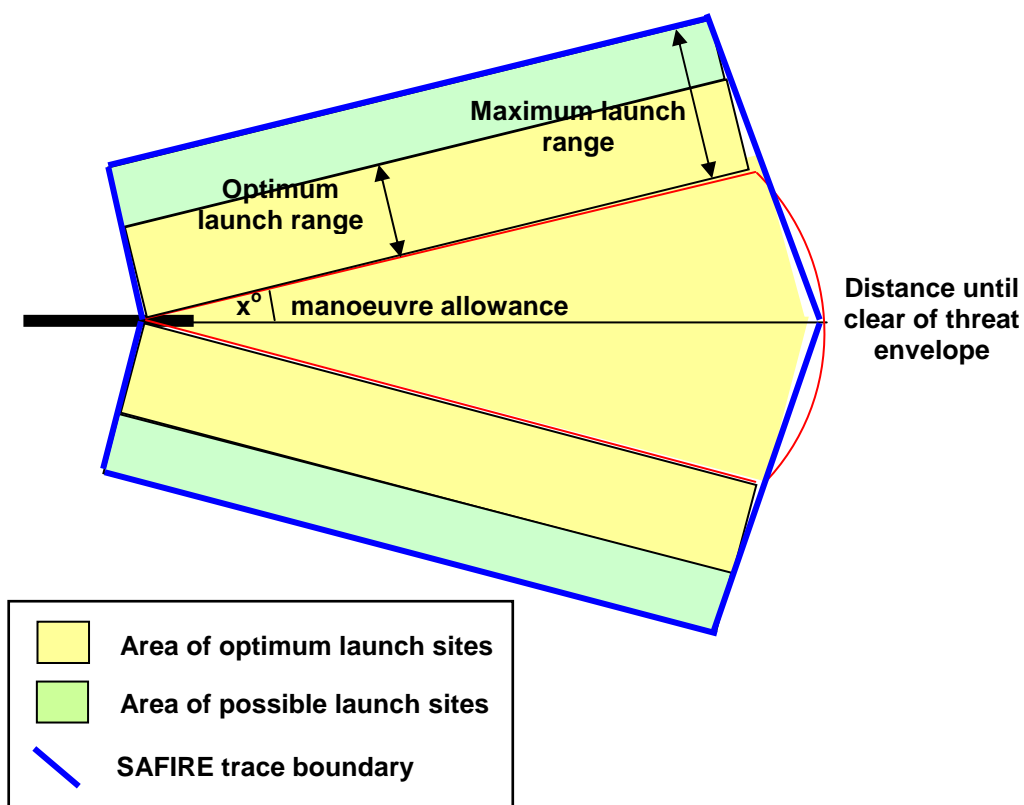
SAFIRE TRACE

2. **Take-off.** To determine the SAFIRE trace for take-off:
- a. Determine the point at which aircraft is expected to lift off the runway (this could be a significant way before the end of the runway on a long strip).
 - b. Establish the engagement envelope of the anticipated threat system.
 - c. Establish how far (in km) the aircraft must travel horizontally from lift off to climb out of the threat envelope.
 - d. Confirm if the aircraft will continue along the extended centre-line or whether it will turn after takeoff: the latter will produce a kinked SAFIRE trace.
 - e. Using the above information draw a diagram to the scale of the map to be used for planning as follows:
 - (1) Mark the point of aircraft lift-off.
 - (2) Draw a line along the intended route of departure to the point at which it clears the threat envelope.
 - (3) If the aircrew wish the option of turning left/right and manoeuvring after take-off add these arcs either side of the centreline. (Note: the more room the aircrew want to manoeuvre, the greater the area the FP troops need to dominate and the more assets required).

AD 80-25



- (4) Obtain the optimum/maximum/minimum engagement ranges for the threat system. For first/second generation heat seeker missiles the shots with the highest kill probability are fired from the beam and moving into a rear aspect profile.
- (5) Add these threat figures to the trace of the volume of airspace in which the aircraft will be within the threat height.



- (6) Once this trace is drawn to scale, lay it on the map and identify the location of any ideal launch sites within the area of optimum launch

AD 80-25

sites, placing them in priority order for surveillance, but bearing in mind that the operator may fire from anywhere within the envelope.

3. **Landing.** The SAFIRE trace for landing is constructed using a similar logic, but plots where the aircraft enters the threat zone and where it touches down.

DEFENCE PLAN DIAGRAM

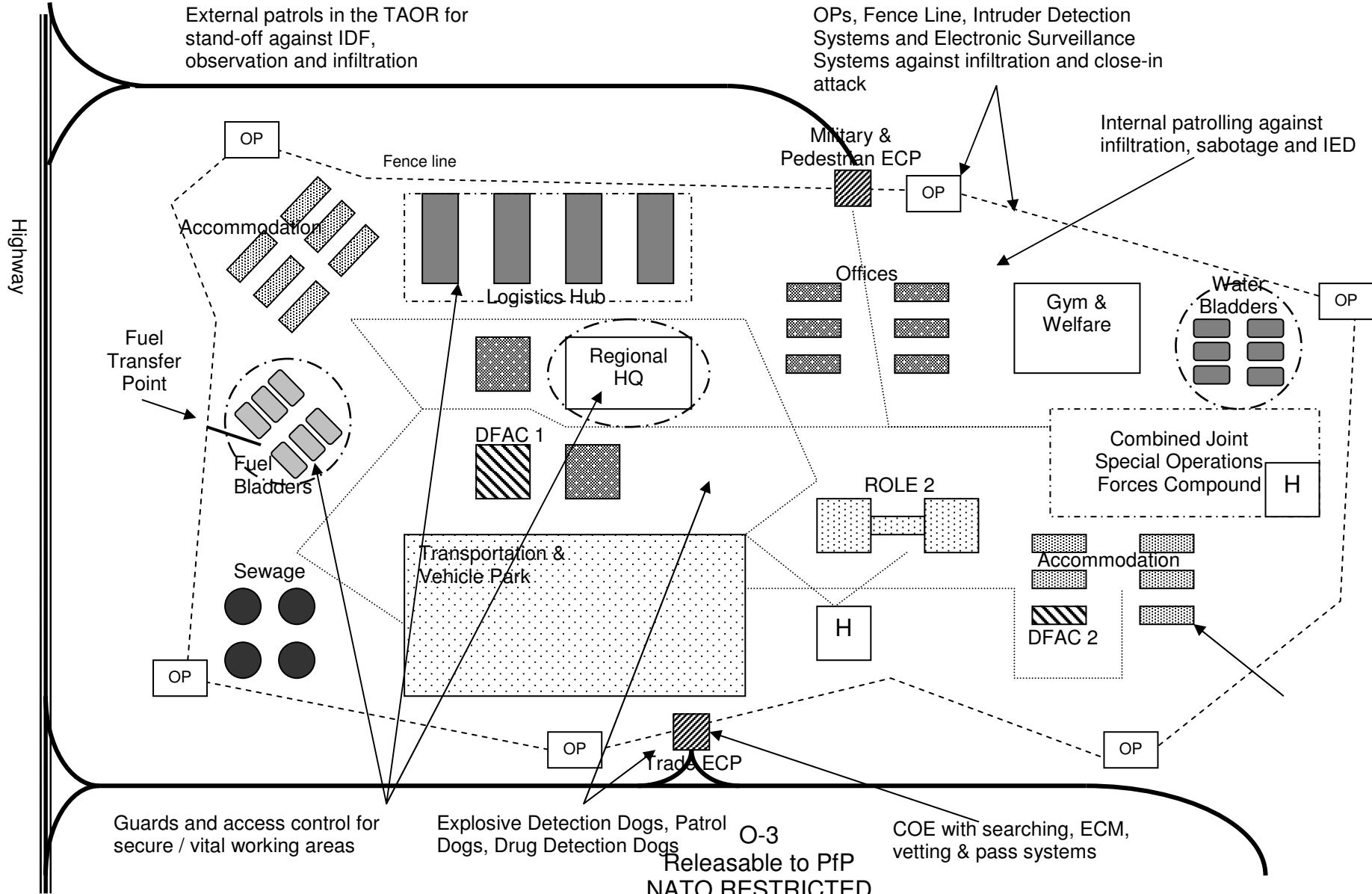
1. **Introduction.** The diagram overleaf illustrates how a layered defence plan could be implemented. Naturally, bases can be colossal in size and hugely complex given the variety of tenants, so the simplistic representation has been made to put examples into pictures. The following principle should be kept in mind when planning how FP assets will be allocated to specific roles in the defence plan.

- a. **Layering & Depth.** Security forces or physical security measures should be placed around the identified vulnerable areas / critical assets starting from inside the location and working outwards. This method ensures layers of defence are built up and can act as a filter deny threats an influence over coalition operations in as many different ways as possible.
- b. **Mutual Support.** Mutual support is about pre-planning where additional assets can be obtained from in the event of consuming too much manpower / resources during a sustained period of escalation.
- c. **All-Round Defence.** Locations should be physically defended around 360 degrees; this aspect also means ensuring that all vulnerabilities are afforded the necessary measures to defend against the identified threat.
- d. **Flexibility.** Security forces must be able to work outside of their prescribed duties in times of emergencies. This can be covered by orders such as 'in addition to the primary tasks, be prepared to...'.
- e. **Reserve.** History continues to teach that a reserve force / reserve capacity is essential to success to regain control after an emergency and defeat the threats that tend to impose themselves suddenly and unexpectedly.
- f. **Aggressive Defence.** Aggressive defence is about the **will** to engage non-coalition forces in kinetic and non-kinetic ways. Rapid decision making based on well understood ROE is required for kinetic options. For some instances, such as pre-emptive strikes, the FP C2 must quickly inform higher-level C2 who can then authorise certain measures. For non-kinetic operations, there is a need for a proactive (rather than aggressive approach) to build relationships with the threat audience.
- g. **Avoidance of Surprise.** The more possibilities for observation, the better security forces will avoid being surprised. This aspect is also greatly supported by integrating into the intelligence network through HUMINT and CIMIC teams as well as HN liaison.

AD 80-25

h. **Key Terrain.** Key Terrain are the areas that non-coalition forces can dominate in order to influence our primary operations. This may be high ground, factories overlooking a dock, or the land under the flight path at an airhead.

AD 80-25



FP VULNERABILITY ASSESSMENT

1. A key component of providing effective FP is a Vulnerability Assessment (VA). The VA process will be applied to all NATO operational installations and can be extended to outside agencies upon request. A VA must focus on the probable threats to an activity and the appropriate countermeasures to those threats. In cases where no threat exists, activities will be assessed on their ability to implement FP measures under increasing Alert States in response to an increased threat.

2. The planning template at Annex D, although seemingly complicated, takes staff through the complete start-to-finish FP process to ensure plans and measures are in place to meet the objectives of FP, i.e. conserve the fighting potential of a force. More explicit questionnaires may be useful for small units but following Annex D will uncover root problems and highlight possible solutions. Working through this process would take 2-3 days, but the end result would be a clear plan to address vulnerabilities whilst fully appreciating the threat and available resources.

3. **VA Team Composition.** A good VA team would need to consist of the specialists listed below, but may also include additional members depending on the location or threat. The following team composition and their associated commitments are a proven way to maximise the efficiency of the VA team:

a. **Team Chief (FPO).** Provides overall management of the VA team, to include individual performance evaluation. Presents the in and out-briefings, and performs other duties based on their experience and training. The Team Chief is responsible for the preparation of the VA in cooperation with the other team members and for evaluating installation, facility, and personnel security and safety. If vulnerabilities are discovered they will formulate and suggest mitigating measures and assist in their implementation. They will assess the following specific points:

- (1) Security forces composition & capabilities.
- (2) Emergency / Contingency Management.
- (3) Advising on the effectiveness of FP plans and SOPs.
- (4) Liaison mechanism between adjacent / supporting forces and HN.
- (5) Fire protection and safety issues.
- (6) Integration into the Air Defence plan.

AD 80-25

(7) CBRN concerns and the unit's ability to survive and operate under CBRN conditions, as well as integrate into CBRN Warning & Reporting.

b. **Intelligence / Security Officer.** Responsible for evaluating the security policy to ensure full coordination with policy matters and compliance with unit security directives and procedures. He will assess the following specific points:

- (1) Current information related to conventional and non-conventional threats such as Terrorism, Espionage, Sabotage, Subversion, Organized Crime, Civil Unrest, and Information Warfare, and coordinated security measures to negate and counter these threats.
- (2) Security Directives.
- (3) Security and education awareness programs.
- (4) Security reporting and the processing of security investigations.
- (5) Security posture, including procedural, operational, and technical security requirements, in order to enhance security and future missions.
- (6) Policy and procedures for Local Civilian Hire (LCH) and Contractor access to facility.
- (7) Protection measures for personnel and VIPS.
- (8) Operational security requirements and measures for control of access to restricted areas.
- (9) The processing of security clearances for facility personnel.
- (10) Liaison with local national security/police authorities.
- (11) Physical/personal security measures at the facility.
- (12) Administrative procedures regarding personal and physical security standards, to include physical security of technical equipment.
- (13) Collection, analysis, and dissemination of threat information.
- (14) Intelligence estimates and products in FP plans and orders.
- (15) Links with host nation and higher headquarters' intelligence assets.

c. **Engineer.** Responsible for evaluating threat and damage assessments. He will assess the following specific points:

AD 80-25

- (1) Damage mechanisms including blast, shock, and fragmentation.
- (2) Building and barrier resistance or mitigation of threat weapons effects.
- (3) Appropriate stand-off distance, potential hardening, or other mitigating measures.
- (4) Systems related to physical security and personnel protection.
- (5) Safe havens.
- (6) Mechanical, electrical, and other service systems for vulnerability to weapons effects and suggest mitigating measures.
- (7) If structural vulnerabilities are found, suggest measures to correct problems and assist in their implementation.

C-IED. Responsible for evaluating threat and damage assessments. He will assess C-IED preparedness and training.

d. **Communications.** Responsible for evaluating communication facilities, INFOSEC and OPSEC procedures. He will assess the following specific points:

- (1) Does the Unit possess a central Command Post with appropriate communications and adequate redundancy?
- (2) Communications provision.
- (3) COMSEC and INFOSEC arrangements and procedures.
- (4) Alarm procedures.
- (5) Arrangements for provision of crypto and maintenance of classified systems.

e. **Medical.** Responsible for evaluating medical and environmental health procedures and facilities. He will assess the following specific points:

- (1) Emergency medical cover in relation to the threat.
- (2) Level of medical cover and determine any changes required.
- (3) Procedures for environmental health and hygiene.
- (4) Vector control and general pest control procedures.

AD 80-25

- (5) Food and water preparation and provision.
- (6) Reserves of essential supplies for medical and food preparation facilities.
- (7) Infrastructure and facilities for medical and environmental health support, including procedures for disposal of clinical, human and routine waste.

FORCE PROTECTION – MINIMUM STANDARDS AND ESSENTIAL TASKS FOR CRISIS RESPONSE OPERATIONS (CRO)

References:

- A. MC 327/2 NATO Military Policies for Non-Article 5 Crisis Response Operations.
- B. AJP-3.14 Allied Joint Doctrine for Force Protection.
- C. AJP-5.0 Allied Joint Doctrine for Operational Planning. (MC 133/2)
- D. NATO STANAG 7132 (Edition 1) Nov 07, Aircraft, Rescue and Fire-Fighting - Minimum levels of crash fire rescue (CFR) equipment.
- E. ATP 3.4.1.1 Chapter 6 Force Protection.
- F. ACO Forces Standards Volumes I – XI.
- G. JFOB Handbook - US Force Protection Handbook for Joint Operational Bases (Dec 06).
- H. Air Pamphlet 3241 (AP 3241) RAF Force Protection Doctrine for Air Operations (Jan 06).

INTRODUCTION

1. Force Protection (FP) represents an essential element of the operational environment that a NATO expeditionary force must provide to secure itself once deployed. All FP measures are a means to minimize the vulnerability of personnel, facilities, equipment, and operations to any threat and in all situations, to preserve the freedom of action and the operational effectiveness of the force. There are six core FP capabilities which, if employed through a layered approach, can be effective against a wide spectrum of threats. Other functional areas such as training, manpower, intelligence, C2 relationships, and equipment are important FP enablers and should be incorporated into FP processes and plans. This Annex combines capabilities, principles and concepts outline in previous chapters and annexes with lessons learned and minimum requirements stated in other NATO publications in order establish a baseline of FP standards and essential tasks.

AIM

2. Commanders are responsible for all aspects of FP for their assigned forces. Therefore, the aim of this Annex is ensure contributing nations, who provide NATO Commanders with FP forces, a baseline minimum standard of competence and ability to perform essential FP tasks.

PROCEDURES

3. The following procedures must be applied as a minimum when delivering robust FP at the operational and tactical level:

AD 80-25

- a. Publish a plan/SOP which clearly defines roles and responsibilities of FP forces assigned.
- b. Ensure an effective and functional C2 structure for FP forces assigned.
- c. Conduct periodic exercises to ensure familiarity with plan/SOP.

MANPOWER

4. The following manpower requirements must be addressed as a minimum when delivering robust FP at the operational and tactical level:
 - a. Establish a staff element which can coordinate/synchronize current FP operations with HHQs, subordinate elements and other base or tactical units.
 - b. Establish a staff element which can integrate future FP plans and requirements with HHQs and Commanders who are responsible for a specific base or area of operations.
 - c. Operational and tactical manpower requirements should be identified through the FP process outlined in AJP-3.14. Manpower requirements should appropriately reflect a comprehensive mitigation plan designed to reduce against assessed threats. Manpower should be accounted for through Crisis Establishment (CE), Combined Joint Statement of Requirements (CJSOR/TCN), or voluntary national contributions (VNC). Generation of manpower through Crisis Establishment should meet the requirements of AAP16 (D).

AREA OF RESPONSIBILITY (AOR) SPECIFIC TRAINING

5. FP personnel deployed as part of a CJSOR, CE or under VNC arrangements should complete AOR specific training prior to assuming assigned duties. All FP personnel assigned to a specific AOR will coordinate closely with the Operational Commander's FP representatives in order to develop training materials that address AOR-specific issues whether it is for their unit or a specific position. The following training requirements should be addresses as a minimum:
 - a. Train FP specialists to implement the controls and measures within their specialty.
 - b. Understand the enemy force capability and intent for specific AOR (including historical data, TTPs, and methods of operation).
 - c. Understand operational constraints (terrain, political, etc).

NATO RESTRICTED
Releasable to PfP

AD 80-25

- d. Recognize specific weapons and their effect in the operational environment (IEDs, mines, rockets, and mortars).
- e. Be familiar with AOR specific FP measures. At a minimum all forces shall be familiar with Force Escalation procedures and Rules for the Use of Force/ Rules of Engagement (RUF/ROE).
- f. Be familiar with FP measures for the specific NATO base, port, or installation to which deployment is expected.

THEATER SPECIFIC LEADER TRAINING

6. All FP Officers assigned to a specific theatre should have a basic understanding of the NATO FP Chain of command, the FP process, and should be capable of directing their forces having achieved the following training competencies as a minimum:

- a. Complete one of the NATO FP Courses (P5-40 or P5-44).
- b. Conduct a situational awareness visit with JFC and Theatre FP personnel prior to deployment.
- c. Conduct Operational Planning IAW OPP (Ref C).
- d. Supervise the application of the RUF/ROE IAW Ref A.
- e. Conduct Vulnerability and Risk Assessments IAW AJP 3.14.
- f. Conduct Risk Management IAW with AJP 3.14 and supports mission objectives.
- g. Understand and/or develop local SOPs that address FP postures, graduated response matrix, weapon readiness levels and security postures IAW specified operation.
- h. Understand the NATO Procurement Process (CUR process, outlined in Bi-SC 85-1).
- i. Establish quality control over FP procedures, measures, and periodic exercises.
- j. Understand the responsibilities, restrictions and the role of contractors.
- k. Understand your role, responsibility and impact as the FP officer within the mission.

AD 80-25

ESTABLISHING THE BASE

7. All FP Officers and subordinate personnel to a specific theatre should have an understanding of how to set up or maintain the basic FP framework for a static location. Guidelines for designing access control points, infrastructure, and perimeters of the base are located in Annex I. The following are additional essential tasks to perform in establishing a base:

- a. Create a defence in depth approach to FP Tactical Area of Responsibility. At a minimum this should include establishing an area outside the perimeter for stand-off/surveillance or patrols, the perimeter itself, and internal areas of responsibility.
- b. Provide FP Mutual Support. Ensure capabilities from organic and non-organic assets are networked appropriately to provide adequate detection, tracking, warning, and reaction to assessed threats (examples: ISTAR, Weapon Location Radar (WLR), Public Address (PA) System e.g. Giant Voice, and Communications).
- c. Prepare the site using layered concepts that integrates the six FP capabilities (Ref B) and FP measures from several functional categories. (Other categories can include Personnel, Equipment, Infrastructure, and Procedures.)
- d. Locate or prepare the site that provides adequate stand-off to known threats (IED, IDF small arms, direct attack, or underwater mines).
- e. Determine or understand effects of known threats and ensure adequate infrastructure protection (this will require close coordination with combat/civil engineers).
- f. Establish control of the roads, water ways, piers, access control points, and other vulnerable approaches to the site. Where the C2 structure permits, establish a tactical area of responsibility (TAOR) around the base monitored and secured by base FP troops. The exact size of the TAOR should be dictated by the nature of the threat.
- g. Construct the base with a main gate and a reserve (alternate) gate.
- h. Build gates to work effectively against demonstrations and riots.
- i. Ensure the perimeter is adequate to protect against known threats (vehicle/human intrusion, view from sniper fire, IED detonation, floating mines).
- j. Where the threat dictates, construct the perimeter wall to reduce the effects of an IED blast (for example, the elimination of fragmentation or providing for blast venting).

AD 80-25

- k. Locate and erect towers that provide mutual support along the perimeter.
- l. Ensure towers have unobstructed line of sight all around the perimeter.
- m. Provide guard towers with detection equipment (night vision devices, cameras, etc).
- n. Set up and operate an alarm system that covers the whole base.

PROTECTING THE BASE

8. All FP Officers and subordinate personnel to a specific theatre should have an understanding of how to implement or maintain FP measures to protect a static location. The following is a baseline of essential tasks to perform in protecting the base:

In terms of Physical Security:

- a. Set up a plan for the defence of the base should it come under attack.
- b. Establish a QRF specifically assigned for the protection of the base.
- c. Assign all units in the base a sector of responsibility for which they are responsible for the security of in the event of an enemy attack.
- d. Plan for the defence of the base that incorporates all available weapon systems.
- e. Establish a system that distinguishes the personnel that have access to the base.
- f. Establish a system that records the personnel that enter or leave the base.
- g. Establish a system for body search of visitors including search of females, locally employed personnel, clerical personnel and VIPs.
- h. Establish a system for search of cars including search of POVs and delivery trucks.
- i. Establish a combination of technical and manual detection capabilities to mitigate against contraband, explosive devices, and weapons entering at access control points.

NATO RESTRICTED
Releasable to PfP

AD 80-25

- j. Establish a varied pattern of the timings and methods of patrolling, changing of guards and detachments and other routine activities.
- k. Create a system to establish how and when to leave and enter the base in order not to create a pattern that is traceable for any enemy of subversive parties.
- l. Provide the guards with written instructions giving orders when to use force, provide the necessary equipment to carry out those orders, and how to call for assistance.
- m. Divide the base into areas with higher protection and therefore restrictions of access.
- n. Establish a combination of technical and manual passive/active detection capabilities to mitigate against direct, indirect, or asymmetric attacks.

In terms of Force Protection Engineering:

- o. Protect areas of congregation, critical equipment and functions. This includes C2 facilities, accommodation, ammunition compounds, dining facilities (DFAC), logistic (RSOI) areas, medical facilities, MWA buildings, and operations centres. Guidance and standards are included in Annex I.

In terms of Protection of Force Health Protection and Life Support:

- p. Provide a designated place to take shelter for every person in the base.
- q. Protect the base water supply.
- r. Protect the Electrical infrastructure in, and leading to, the base.
- s. Protect personnel through effective protective equipment (EPE) measures against hostile or friendly weapon systems (includes CBRN).
- t. Ensure adequate Force Health Protection through effective medical, industrial, environmental, and disease preventive measures (AJP-4.10A).

In terms of Consequence Management:

- u. Develop Contingency Plans, Incident Response and Damage Control Measures.
- v. Provide essential Aircraft and Fire Fighting rescue services IAW Ref D.
- w. Set up a plan for actions on post attack recovery operations.

NATO RESTRICTED
Releasable to PfP

AD 80-25

In terms of Intelligence, Counter-Intelligence (CI) Human Intelligence (HUMINT):

- x. FP Staff shall liaison with J2 Staff to ensure a standard Threat Assessment (TA) in accordance with AJP-2.0 Chapter 4. At a minimum TA should provide necessary data on threats, establishes probability of occurrence, likelihood, and impact on personnel/mission.
- y. Ensure FP Intelligence Requests are incorporated with local collection effort.
- z. Establish organic CI and HUMINT assets within the FP C2 structure.

In terms of Community or Civil Relations (CIMIC):

- aa. Create a routine to establish good relations with the neighbouring community in order to increase the overall level of force protection.
- bb. Set up a UXO box outside the base where local people can deliver their findings of UXO for safe destruction.

SUMMARY

9. All FP measures are a means to minimize the vulnerability of personnel, facilities, equipment, and operations to any threat and in all situations, to preserve the freedom of action and the operational effectiveness of the force. Nations familiar with NATO standards will be an essential enabler to the delivery of the overall FP plan during NATO Crisis Response Operations. This Annex provides a framework in which successful protection of NATO forces can be achieved. However, in some cases the baseline may have to be adjusted in order to respond to changing/emerging threats and should be conducted through continuous assessments.

IDENTITY MANGEMENT FOR FP

REFERENCES:

- A. SHAPE's OPLAN.
- B. CP 0A0155 INFOSEC CP.
- C. CM (2002)49 – NATO SECURITY POLICY

SITUATION

1. **Introduction.** Identity Management (IdM) is a key global enabler for FP, e.g. by managing identities, establishing trust, protecting personal information, operating networks including controlling access to facilities, networks or services, performing online e-transactions, and complying with local legal and regulatory requirements. IdM is a core, constantly evolving and expanding cyber security and Force Protection capability.

This annex describes a common, structured Identity Management Model and Identity Management Plane to be used within and across NATO FP plans and its coalition member nations.

2. **Situation.** The identification of an entity materializes its/his/her uniqueness of that entity in a specific context. Entity has to be taken in its broader sense and represents a physical person (human), a moral or legal person (command, company), an object (information, system, and device) or a group of these individual entities. The identification process is an integral part of Identity Management during which an entity may be authenticated, and be associated with information representing the entity within some context e.g. a mission. Different attributes of an entity form its identity in different contexts. Thus, an entity can have different identities in different contexts. The important point here is that all these different identities go back to the same entity, i.e. uniquely identify it. For example, a human entity may have the following context dependent identities: a biological Identity (DNA fingerprint) relevant when dealing with entities associated with a person's passport, a virtual identity relevant when a person is dealing with one or more on-line web-service providers, a social Identity relevant in the context of membership of a social community, a legal Identity relevant when a person is dealing with government agencies or with entities with an interest in meeting the requirements of a particular legal jurisdiction.

3. **Generic Threats.** NATO personnel, civilian employees, equipment and facilities face a wide range of identity threats in-theatre, within the operational realm and within static locations brought on by the increasing pace of IT support to the current C2 process. Hostile and criminal non-coalition forces are trying to infiltrate compounds, systems and elements of the NATO missions. The most likely cyber threats include identity theft, identity impersonation or masquerading and a highly

AD 80-25

dangerous threat exists from Cyber Identity abuse given the lack of trust mechanisms within that environment.

Lack of formal and global NATO identity mechanisms will result in increased fratricide (e.g. failing IFF), infiltration and subversion.

4. **General Threat Analysis.** No change to Reference A-C.
5. **Specific Threat Analysis.** Specific threat levels relevant to the facility / location are given in detail in this section or at an Appendix.
 - a. **CBRN/ROTA.** As per guidance given in para 5.
 - b. **Friendly Forces.** As per guidance given in para 5.
 - c. **Non-Coalition Forces.** As per guidance given in para 5.
6. **FP Concept**
 - a. **Aim of FP.** The overall aim of FP is to adopt measures and procedures that are appropriate to identity threats and risks inside the AOO. Although national and coalition concerns may differ, identity supporting FP and the preservation of identity FOM must not be degraded. FP measures are not meant to portray the image of an occupation force; rather, the population should perceive FP measures as sensible military precautions undertaken by a professional, disciplined, well-trained and confident force.
 - b. **Delegation of Authority.** The theatre commander has the overall responsibility for FP and is the only authority to decide on theatre-wide FP measures. Authority is granted to subordinate commanders to increase the FP measures as required by their specific requirements. The base FP Command Element has extracted direction and guidance from References A-H to conduct an estimate of the FP mission. This has been used to complete this Base FP Plan and the resulting base SOIs (Reference I).

EXECUTION

7. **General Outline.** FP must be a comprehensive and coordinated effort in order to protect personnel, facilities, equipment, operations and information. The following tasks have been identified from the FP Estimate.

8. Specified Tasks

a. Establishing an Identity

The process of establishing an identity in a mission includes:

- (1) Collecting and / or allocating sufficient identity attributes on the entity (following the mission structure of the domain) to distinguish the entity

AD 80-25

from any other in the domain, and allocating as part of these attributes a unique identity reference to the entity in this domain.

(2) Validating the identity, checking that the attribute values are correct (with a degree of assurance proportional to the mission and specified in an associated mission policy) and, legitimately associated with the entity in question.

(3) Establishing some relationships with one or more other entities in the mission that allows future interactions

(4) Proceeding with the identity registration, storing the identity in an IdM record.

It is common to allocate one or more identity authentication credentials during this process (e.g. ID cards, passwords, authentication tokens) and to make them part of the identity. Identity authentication credentials may be allocated as part of the identification process, or at a later time. If identity authentication credentials are issued at a later time, such issuance must be immediately preceded by authentication of the entity's identity similarly to what can be provided during the identification process.

It is also common to allocate during this process some prerogatives and to make them part of the identity (e.g. how to get a new ID card for a user). These can then be used to manage future interactions between the entity and one or more other entities.

b. **Command, Control, Communication, Intelligence & Integration.**

(1) **Establish a C2 IdM plan**

Identity Activation. The process of establishing an identity in a mission involves systems management action within the mission context to allow an entity to interact with other entities according to the mission goals and prerogatives determined within the identification process.

Identity Suspension

A mission identity may be suspended if confidence is lost in the correctness or other assumed identity attribute properties. An identity may also be suspended if the associated entity ceases to have interactions in the mission according to a predefined pattern (e.g. a person doesn't use a service for a long period), or if there is period of time when no interactions will occur (e.g. when a person takes a holiday). The process of suspension commonly requires verification to ensure that the correct identity is subject to suspension. Identities are commonly suspended by changing an attribute such as the end of validity period or information on its state.

Identity Termination

AD 80-25

Termination of an identity occurs when there is no further need for an entity to engage in the mission activities or interactions with the mission. Commonly this is a consequence of changed circumstances (e.g. a person leaving an organization or killed or missing in action). Sometimes it is necessary to terminate identities to prevent unauthorized actions, fraud and other types of crime in a mission.

Termination is also required for privacy reasons. It may, however, be restricted by law and regulation. Termination of an identity involves removal of all records that an entity may have possessed in a domain. Termination of an identity involves also the notification of all systems and processes with which identity has established contacts.

Termination may be initiated by the entity (such as by resignation) or by the identity authority. It must be properly recorded for audit and review purposes. After an identity has been terminated, it is possible to reallocate the associated identity reference attribute to another entity unless the identity is archived. However, care must be given to this process and privacy requirements associated to the mission identification policy may limit that capability.

Identity Archiving

This is an optional lifecycle process. Identities may be archived when the associated entity is not longer active in the domain. This is required either:

- When a legal or regulatory requirement must be able to determine whether or not a particular entity has in the past had a given identity in a domain; and
- When the possibility exists that the associated entity may in future become active again in the domain.

Identity Reactivation

Reactivation from the suspended or archived state is sometimes required, e.g. when returning after a period of unavailability.

Prior to reactivation it is necessary to determine which archived identity can be legitimately associated with a particular entity in order to preserve privacy but not only.

This involves proofing the identity once again. Reactivated identities will usually have the same identity reference attribute that was used previously by an entity in the established state. When reactivating from the archived state it is common that new identity credentials are issued and to proceed with an identity authentication.

Other aspects of Identity life-cycle management **Identity Reference Choice**

Depending on the context an identity reference may be chosen by the entity, a parent/master of the entity or provisioned by an identity manager or generator through or not the identity authority. For example, entities may be given an

AD 80-25

incremental unique number, may choose their reference with analogy to a name of their choice provided the name does not already exist, or may again be given an email address as reference.

In all cases the identity reference is enrolled to the Identity Management system together with some attributes, such as authentication attributes (passwords or shared secrets) and the identity manager must guarantee the uniqueness of the identity of the entity in the domain.

Entity Identification

Entity identification occurs:

- During or after the initial identification process (as part of the process of recognizing an identity and establishment of relationships in a domain)
- As part of the process of entities interacting with each other once established in a domain; and
- During the reactivation process, similarly to the identification process.

In addition, entity identification can take place at the remaining stages of the identity life cycle. For example, when activating, deactivating, terminating and archiving an identity, authentication of the entity requesting these actions should take place as part of verifying the authority of that entity to make these requests.

Entity identification is the process of confirming a claimed identity to an acceptable level of confidence and establishing that the claimed identity is genuine. It may happen as part or just at the end of the identification process for the purpose of the creation of an initial credential or when renewing these credentials (after reactivation for instance).

Initial entity identification includes verifying the entity for being authorized to hold a credential of the organization.

Initial entity identification takes place prior to the issuing of any credentials and the consecutive provisioning of any privilege to the entity. The complexity of this process varies widely. Requirements are generally based on the sensitivities of the possible privileges to be later authorized to the entity. Consecutive verifications (for reissue or replacement of credentials) can be as strong as the initial one or less complex considering the presence of a first credential.

Once credentials based on a claimed identity are issued, whenever they are used, there is the requirement of determining that the claimed identity is used by the user to which the identity was assigned. This ongoing authentication process is needed to minimize the likelihood of fraud based on one entity pretending to be another, sometimes known as identity fraud.

Identity authentication controls the credential given to an entity and any related credentials with the objective to certify that the entity is authentic.

AD 80-25

In some cases, an on-going track record of successful interactions between entities in a mission (e.g., a token) can give rise to increased confidence that their identity are as claimed and that identity authentication credentials are not compromised. The processing of mutual authentication, also described as two-way authentication, where both parties involved in a recognition process must be authenticate between each other, is an improved authentication process where the likelihood of compromise is further reduced.

In some cases where the entity is not present (e.g. under silence condition) a unilateral authentication process may take the place of a bilateral authentication (because the person is not there to confirm). Such a unilateral authentication requires a robust auditable process, as it typically involves confirming identity by means other than knowledge of the entity, and may well be similar to the process used in identity establishment described in the initial authentication.

Identity Management within a Coalition environment

Following chapter 3.7, it is the sole responsibility of NATO and nations to create and maintain identities within their own domains. Therefore, identities will not be created within the federated domain.

Nevertheless, the handling of identities within and across a federated mission is the primary responsibility of the Identity Management within a coalition domain.

Therefore, the Identity states, which are described in chapters 4.2.2, 4.2.3, 4.2.5 and 4.2.6 (Activated, Deactivated, Archiving, Reactivation), are responsibilities of a federated IdM within this federated domain.

Identity Management Framework components

An Identity Management system must provide accurate and updated identity information on entities of resources of a mission or community of interest.

Information is originating from systems such as an HR system, a system managing contractors, other management systems for entities outside of the mission or COI, and object inventories such as the inventory of IS processes and resources. These sources are called Authoritative Sources since they control the life cycle of entities, from the identification process until they are terminated.

A repository, the Identity registry, collects information on users from the different authoritative sources, and makes this information available to any system that may need it. In the case of a federated Identity Management system, an Identity registry exists at least once per domain/community.

Personally identifiable information of the Identity Registry will be relevant and not excessive for the purposes for which they are collected. Any irrelevant data must not be collected and if it has being collected it must be discarded. Data is required to be kept accurate and up to date by the Identity Management system Additional

AD 80-25

techniques and procedures need to be developed to enforce quality of information maintained at Authoritative Sources level.

The Identity Management system maintains the synchronization between the providers (including cross-mission towards a federated domain) and the users of entity information. The Identity Management system also maintains synchronized links to other master references of user information such as the email system. With the help of authentic sources, the Identity Management system controls the validity period of legitimate actions of an entity in a domain. Security and control services linked to the Identity Management system are informed when a validity period ends and can act accordingly.

Identity Management System

The Identity Management system is the kernel of the Identity Management Framework. It ensures the objectives are obtained and the control criteria implemented. It provides tools for managing the identity registry and eases the delivery of identity information to systems of the mission that may need it. Because it is validating the existence of entities the Identity Management system represents the ultimate authority source of entity management. Other management systems rely on the contextual Identity Management system and the secure, reliable, and regulation compliant management of information associated with the identification of entities.

Identity Registry

The Identity Management system contains a registry where identity information is maintained, the list of attribute types and values, and a reference to the definitive authentic source of the values for these attributes. It represents the unique reference of entity' identity information to all information systems of the mission and it represents therefore for these systems the reference for entity's identity information in a particular domain. Users of the information (applications and systems) may keep a copy of the information (as far as this is not compromising the requirements for privacy) but the maintained information is kept in the identity registry of the domain.

Authoritative Sources of Entity Information

An authentic source is designated as the place where identity information is maintained. A number of referenced authentic sources must be authorized to validate new entities within one domain. The authentic sources may be located outside of the mission boundaries as entity information management may be delegated to external services under service level agreement.

The maintenance of the entity information is guaranteed by means of synchronization between entity authentic source and the identity registry. The recognition of the authentic sources is done through a separate identification and registration process similar to the registration of entities. A superior authority

AD 80-25

must (if needed) be designated per mission to guarantee a proper bootstrapping process.

An Identity Management system can also be seen as an additional authentic source that can act on behalf of any other authentic source within the same domain. For external Identity Management, a national Identity Management system has in addition the responsibility to act as an authoritative source for national entries within the federated domain.

(2) **Develop daily working relationships with the local HN forces, IOs and NGOs**, in order to develop a coordinated and de-conflicted the approach to operations in the TAOR.

(3) **Develop intelligence integration** with higher intelligence elements such as CI and intelligence fusion cells in order to benefit from and contribute to wider Situational Awareness.

(4) **Integrate with the theatre Air Operations Planning Group (AOPG)** in order to seek air mobility support for patrolling units / CASEVAC, and from ISTAR assets to provide surveillance / C-IED within the TAOR.

(5) **Liaise with CIMIC, HUMINT and Information Operations teams** to raise the priority of such operations in the TAOR in order to gather intelligence on and focus efforts against non-coalition forces around the unit being defended.

(6) **Establish an FP C2 CIS plan**, or Information Exchange Requirements (IER), that can at least enable communication with the following:

- All FP sub-unit elements at the location, cutting out unnecessary reporting nodes so information passes as quickly as possible.
- Is able to fuse all surveillance system data in one location.
- The location's main operations centre.
- Sector Commanders, if the base has been sub-divided into sectors.
- Adjacent HN security forces, IOs, NGOs and other Component Commands.
- The operational / theatre FP officer.
- The higher level NBC Warning & Reporting networks.
- Operations elements that can support such as CI, CJ2, CIMIC, HUMINT, and the Joint / Air Operations Planning Group.

c. **Security**

(1) **Implement off-base, high-visibility patrolling** in order to deter, disrupt, detect, delay and ultimately prevent or destroy potential hostile attacks from MANPADS, IEDs, mortars, rockets, and snipers. Patrols must have the mobility and firepower to dominate the TAOR as well as

AD 80-25

the ability to build relationships with the local population and thereby deny non-coalition forces practical and moral FOM.

(2) **Develop a Fire Support plan** for Support Weapons in the event illumination or high explosives are required during a contact situation.

(3) **Clarify details in the SOFA and MOUs** so that the police elements fully understand their powers of stop, search, arrest and detention.

(4) **Check the physical security and INFOSEC** such as fences, doors, and security furniture to ensure it is good working order and available where it needs to be. Ensure document handling and IT procedures are in place to protect information.

(5) **To ensure the security, safety and protection of food, water and energy / fuel sources at all stages of introduction / consumption at the location.** This means the fuel transfer points and convoys are protected where necessary. Food and water sources must also be vetted and monitored.

(6) **Develop COE procedures** that ensure the unit has complete control and oversight of access to the following areas:

- Through the main and stand-by / alternate / trade base access points.
- For the fuel transfer point to the Bulk Fuel Installations (BFI).
- Vital buildings such as Base Operations...etc.
- Identified Vital Ground such as the vital working locations, aircraft operating surfaces...etc.
- Internal and external VCPs at areas where personnel movement can be monitored and controlled as required.

d. **FP Engineering / Infrastructure Protection**

(1) **Develop an integrated approach to UXO, EOD and Mine Awareness issues.**

(2) **Ensure Fire Protection** has been considered for all areas of the locations and that fire evacuation orders are prepared; and there is a system to warn the Fire Crash Rescue Services (FCRS) in the event of a fire. Also, ensure fire appliances and alarms are routinely checked for serviceability.

(3) **Develop SOPs for maintaining a safe operating environment,** that includes safe working practices and healthy environment.

(4) **Develop Military engineering** projects in accordance with the CRO Urgent Requirement (CUR) process to ensure essential services / buildings are protected from blast / fragmentation and weather. Such areas include:

AD 80-25

- COE points;
- ROLE / medical facilities;
- Fences, barriers and boundaries;
- Bulk Fuel Installations;
- Gas, electric, and water storage / distribution networks;
- CIS networks;
- Sewerage / waste disposal / refuse disposal networks;
- Dining Facilities (DFAC).

(5) Develop a Camouflage, Concealment, Dispersal and Deception (CCDD) plan that is in harmony with main operations.

e. **Force Health Protection**

(1) Develop a Mass Casualty plan with the ROLE facility, and ensure arrangements are in place for either CASEVAC within the TAOR to the location for from the TAOR to an overflow, higher level ROLE facility.

(2) Develop a Health & Hygiene plan that is supported by sufficient capacity of ablutions and medical support.

f. **Emergency Management**

(1) Develop Emergency Management plans to enable recovery from any incident or accident that would demand a coordinated response. Such plans must be able to cope with IED / Indirect Fire / CBRN attacks as well as mass casualty situations and a range of unpredictable incidents. Plans should be based on common principles and kept as simple as possible so troops can learn them quickly and they are easy to implement under pressure. Training of local non-FP personnel will be required so individuals are able to act as First Responders or Incident Commanders.

(2) Identify specific manpower or train personnel to undertake Post Attack Recover (PAR), and who can search for UXOs or damaged infrastructure. A reporting network is required to support this effort and need implements as part of the CIS requirements.

(3) Identify personnel and resources that can repair damaged services or facilities in order to restore main operations as quickly as possible.

g. **CBRN**

(1) Identify latent threats or dangerous infrastructure that may eventually lead to an attack or release from a Toxic Industrial Material (TIM).

AD 80-25

(2) **Implement NBC and TIM detection, warning and monitoring capabilities.**

(3) **Provide a suitable shelter posture** and relevant manning to provide protection against a sustained CBRN attack or TIM release.

(4) **Identify personnel and resources** to support the shelter posture and who can undertake recces and surveys of CBRN TIM threats.

COORDINATING INSTRUCTIONS

9. **Electronic Counter Measures (ECM).** The provision of ECM equipment is a national responsibility and nations are strongly encouraged to provide their troops with this capability. In order to prevent mutual interference between other ECM equipment and communications systems, coordination between TCNs and other agencies is required for Spectrum Management control.

10. **FP measures.** FP measures are issued by Theatre FP based on the prevailing threat, which differs from region to region.

11. **Risk.** The FP posture should be based on risk management, not risk elimination. Deliberate or accidental casualties are a reality of military operations, as are material and equipment losses and an overemphasis in avoiding them may impact adversely on the achievement of the mission. The commander therefore must balance risk within the context of mission accomplishment.

12. **Delivering FP.** All personnel must realise that whilst some elements of FP are delivered by specialists, everybody has a role to play in delivering an integrated FP effect.

COMMAND AND SIGNAL

13. **Command.** As per the individual base's requirement.

14. **Signal.** As per the individual base's requirement.

EXAMPLE ANNEX U – Operations in a Chemical, Biological, Radiological, and Nuclear (CBRN) environment

REFERENCES:

- A. SHAPE's OPLAN.
- B. Joint Force Command's OPLAN.
- C. Theatre Commander's OPLAN.
- D. Current theatre SOP (if it exists).
- E. STANAGs.

SITUATION

1. **General.** The planning and conduct of CBRN defence operations must support theatre in the maintenance of security throughout the relevant Area of Operations (AOO). The CBRN threat assessment, CBRN defence planning and preparation, and CBRN Warning and Reporting (W&R) amongst coalition forces and HN must be considered and addressed as required. Specific CBRN defence operations and procedures will be planned and conducted at the operational and tactical levels as an integral part of operations to ensure overall FP is supported.

2. **CBRN Threat Assessment.** CBRN agents have not been used in Theatre and there is currently no indication of hostile intent to use CBRN substances in the immediate future. However, non-coalition forces operating in the AOO are assessed to be seeking a CBRN option and although unlikely, use of a natural or Toxic Industrial Materials (TIM) as an asymmetric weapon cannot be ruled out. A significant threat exists from natural and man-made environmental hazards and endemic diseases.

a. **Biological Agents as Asymmetric Threat.** Primary targets include high visibility political targets. The most probable means of delivery include letters or packages. The attack would have limited tactical effect but high psychological impact.

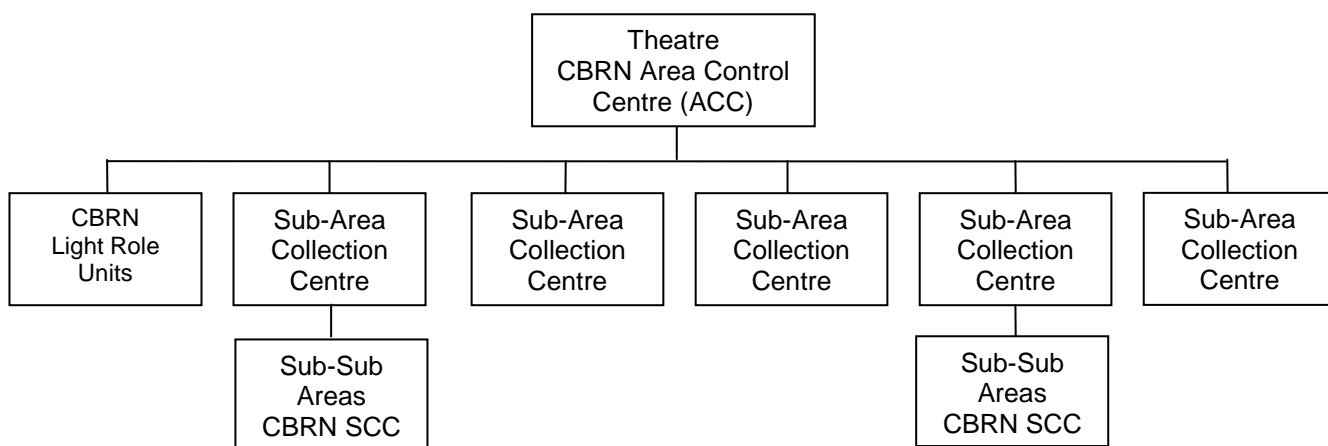
b. **Chemical Agents as Asymmetric Threat.** The most likely chemicals that could be used include narcotics production precursors or insecticides used in the farming industry. As large quantities of chemicals are required to produce significant effect, most probable means of delivery would be large transports (cargo truck, fuel truck, etc). The attack would have limited tactical effect.

AD 80-25

- c. **Radiological Sources as Asymmetric Threat.** The most likely threat includes the use of radioactive materials in conjunction with IEDs to produce contamination by spread of hazardous material.
- d. **TIM.** These are primarily found at the small laboratories spread throughout the AOO. They pose an immediate threat with localized effect.
- e. **Endemic Diseases.** Endemic diseases pose a CBRN-related threat. Proper medical force protection measures and treatment to reduce these specific threats are outlined in the medical annex.

3. Friendly Forces

- a. CBRN Defence Task Organization:



- b. **CBRN Forces & Capabilities.** As detailed in the CJSOR or listed here.

MISSION

- 4. Conduct CBRN defence operations in order to prevent or mitigate the effects of a CBRN attack or TIM release.

EXECUTION

- 5. **Concept of Operations.** CBRN elements will provide support primarily in their respective AOO while the theatre deployable CBRN unit will act when local capabilities are overloaded, restricted by national caveats, or unable to respond properly due to technical or tactical limitations. All sub regions will appoint a CBRN officer as an adviser to their local commander and will serve as a point of contact for all CBRN matters to ensure coordinate and cohesive theatre-wide CBRN operations. On order or on the increase of the CBRN Threat Level to MEDIUM or HIGH, all regions will operate a Collection Centre (CC), and sub-units will man a CBRN Sub Collection Centre (SCC), as described in the Task Org above. All units, bases and

NATO RESTRICTED
Releasable to PfP

AD 80-25

facilities are to be prepared to take appropriate FP measures and conduct self-decontamination as appropriate. On order, all commanders are to liaise with local authorities and respond to any CBRN event and be prepared to support the local population with assistance in the isolation and cordon of hazardous areas or material(s).

NATO RESTRICTED
Releasable to PfP

AD 80-25

6. **Tasks**

Organization	Tasks
Theatre HQ CBRN Defence Cell	<p>T1: Man the CBRN Area Control Centre (ACC) during CBRN threat levels MEDIUM and HIGH.</p> <p>T2: Coordinate preparation of CBRN defence reaction plans and establish warning and reporting procedures.</p> <p>T3: On order, coordinate CBRN defence priorities in conjunction with the United Nations and HN government.</p> <p>T4: Maintain the AOO CBRN threat assessment and CBRN vulnerability assessment.</p> <p>T5: Establish and maintain AOO CBRN Hazard Database, including Low Level Radiation (LLR) and TIM hazards.</p> <p>T6: Coordinate and conduct appropriate CBRN Warning and Reporting exercises, CBRN Defence reaction exercises, Consequence Management exercises and exercises to test the readiness of CBRN units within the AOO as required to validate the CBRN Defence readiness in each of the geographic areas.</p> <p>T7: BPT support CIMIC coordination centre with the coordination of CBRN Defence issues and priorities between all Theatre HQs and HN authorities as well as other civil defence authorities.</p> <p>T8: BPT support plans to implement Information Operations (INFO OPS) response to CBRN events across the AO and in support of NATO operations.</p>
Regional Commands	<p>T1: Appoint a CBRN officer as an adviser to the commander and as a point of contact on CBRN matters.</p> <p>T2: Maintain a CBRN threat assessment and CBRN vulnerability assessment for the respective AOO.</p> <p>T3: Establish and maintain a current list (database) of CBRN hazards in the respective AO. Develop contingency plans based on this list for minimizing the operational impact caused by CBRN hazards and/or ROTA within the region.</p> <p>T4: On order, establish a CBRN CC and conduct warning and reporting system IOT conduct continuous CBRN monitoring within assigned AOO to provide for early detection, identification, and warning of CBRN hazards.</p> <p>T5: On order, liaise with local authorities and establish procedures for timely and accurate CBRN warning to the local population.</p> <p>T6: BPT support Sensitive Sites Exploitation (SSE) operations on potential WMD / TIM facilities and or material(s).</p> <p>T7: BPT assist local authorities with the isolation, cordon, or transportation of hazardous materials.</p>
Sub-Units	<p>T1: Appoint a CBRN officer as an adviser to the commander and as a point of contact on CBRN matters.</p> <p>T2: Maintain a CBRN threat assessment and CBRN vulnerability assessment for the respective AOO.</p> <p>T3: Establish and maintain a current list (database) of CBRN hazards in the respective AOO. Develop contingency plans based on this list for minimizing the operational impact caused by CBRN hazards and/or ROTA within the region.</p> <p>T4: On order, establish a CBRN SCC and conduct warning and reporting</p>

U-4

Releasable to PfP
NATO RESTRICTED

NATO RESTRICTED
Releasable to PfP

AD 80-25

	system IOT conduct continuous CBRN monitoring within assigned AOO to provide for early detection, identification, and warning of CBRN hazards.
--	--

7. Specialized Tasks

a. Outline of Sub-Unit Tasks / Sub-Tasks for Specific Locations.

Completed here as required.

Organization	Sub-Tasks
Theatre-Wide Specific Unit	<p>ST1: BPT conduct operations within entire AOO in support of theatre or HN government authorities.</p> <p>ST2: On order conduct CBRN site surveys / CBRN reconnaissance to identify and mark any CBRN-related hazards (chemical, biological, radiological and/or related munitions requiring exploitation or removal) at potential hazardous sites to include waste dumps and hazardous material production facilities and assess potential threats to troops, civilian population, and the environment.</p> <p>ST3: On order collect samples and provide initial analysis for threat assessments. ON ORDER transport CBRN samples to additional reach-back laboratories for conclusive analysis. BPT conduct sampling in semi-permissive environments and support the removal of explosive ordnance and improvised explosive devices.</p> <p>ST4: BPT decontaminate a platoon size element IOT minimize the consequences of exposure of personnel and render contaminated critical material "CBRN safe".</p> <p>ST5: On order support reserve forces in the conduct of any CBRN (related) operation.</p> <p>ST6: BPT conduct two simultaneous light reconnaissance missions.</p>

8. Priority of Effort and Support. The priority of effort for all CBRN operations is to support the theatre commander in his political, strategic, and operational efforts in support of the HN government. Emphasis will remain on the following:

- a. Protection of key leadership.
- b. Industrial and hazardous chemicals / materials.
- c. EOD removal and identification.
- d. Identification and removal of unknown or suspected biological, chemical, or radiological materials.

9. Co-ordinating Instructions

a. CBRN W&R. CBRN W&R is to be conducted IAW Reference X. Commanders are to warn local populations of any chemical or radiological hazards. Biological reporting remains classified and reports are to be released to local authorities only when authorized to do so by theatre CBRN Officer.

b. Current CBRN Dress State. As detailed.

AD 80-25

- c. **Chemical Downwind Messages (CDMs).** The Theatre CBRN ACC will provide the CDMs on a twelve-hour basis during Threat level MEDIUM and HIGH. During lower threat levels these reports will be available on the Theatre web.
- d. **Operational Exposure Guidance.** Standard military protective equipment provides limited protection against most likely chemicals. It is of vital importance that all commanders strictly follow the guidance given in Reference B and which deal with personnel exposure to low level radiation and toxic industrial chemicals.
- e. **Riot Control Agents.** Use of riot control agents is authorised iaw ROE XYZ.
- f. **Reporting Requirements**
- (1) Report first use of CBRN weapon with CBRN 1 report.
 - (2) Report one correlated CBRN 2 and CBRN 3 report after each CBRN attack, until otherwise directed.
 - (3) Report ROTA with CBRN 4 report (preferred to CBRN 1 if possible).
 - (4) Report CBRN situation (CBRN SITREP) daily, once directed.
 - (5) Other reports (CBRN 4 – CBRN 6) on request only.
- g. **Strike Serial Number.** ALPHA XX1/100ACC/100ACC001/RC/-//
- (1) Field 1. XX1 for theatre (by ACC only, others leave blank).
 - (2) Field 2. Code of the originator (refer to SOP).
 - (3) Field 3. Sequence number (refer to SOP).
 - (4) Field 4. Type of incident (N, B, C, RN, RB, RC, RU).
 - (5) Field 5. Grading – used as necessary.

SERVICE SUPPORT

10. **Sustainment.** Commanders will ensure that all units in the AOO have complete sets of Individual Protective Equipment (IPE) and relevant unit CBRN defensive equipment IAW Reference X. Additional sets of IPE and replenishment of expendable items is in accordance with national policies and procedures and re-

AD 80-25

supply is to be available not later than 24 hours after an increase in the CBRN Threat Level.

11. **Medical.** CBRN threats to coalition forces are considered unlikely. However, should such a threat be indicated, the Medical Director will coordinate appropriate medical planning and preparation of additional CBRN protective / preventive measures and treatment. However, it is the responsibility of every TCN to provide protection for their personnel and therefore TCNs should provide adequate medical capabilities in the Theatre.

12. **Shortages.** Mission critical shortages of CBRN defence equipment and supplies should be reported through national logistic reporting and Theatre command chains immediately.

13. **Coordination of Evacuation Routes.** Formations will co-ordinate and designate contaminated evacuation routes with subordinate, adjacent, and follow-on units.

14. **CBRN Defence Support.** Requests for CBRN defence support to local populations will be forwarded through CJ9 channels to the appropriate staffs for action.

COMMAND AND SIGNAL

15. **Command.** The lead CBRN Officer is the Theatre CBRN Defence Officer. The HQ CBRN Officer will be located at HQ CJ3 TFP&CBRN Section.

16. Signal

a. CBRN Warning and reporting will be accomplished IAW Reference X which can be shared with non-NATO nations contributing forces in the AOO.

b. All CBRN information and messages will be sent via Theatre-wide classified communication information system. Alternate communication channels in order of priority are fax and phone.

c. Theatre CBRN ACC will pass reports of CBRN attacks / incidents to HQ JFCB Operations Centre via CRONOS.