MINISTRY OF DEFENCE

Joint Doctrine Publication 3-64
Joint Force Protection

Development, Concepts and Doctrine Centre

MINISTRY OF DEFENCE

Joint Doctrine Publication 3-64

Joint Force Protection

Development, Concepts and Doctrine Centre

JOINT DOCTRINE PUBLICATION 3-64
JOINT FORCE PROTECTION

Joint Doctrine Publication 3-64 (JDP 3-64), April 2010,
is promulgated
as directed by the Chiefs of Staff

Assistant Chief of the Defence Staff (Development, Concepts and Doctrine)

AUTHORISATION

The Development, Concepts and Doctrine Centre (DCDC) is responsible for publishing Joint Doctrine Publications (JDPs) within a hierarchy of similar publications. Readers wishing to quote JDPs as reference material in other work should confirm with the DCDC Doctrine Editor whether the particular publication and amendment state remains authoritative. Comments on factual accuracy or proposals for amendment are welcomed by the Doctrine Editor at:

The Development, Concepts and Doctrine Centre
Ministry of Defence
Shrivenham
SWINDON, Wiltshire, SN6 8RF

Telephone number: 01793 314216/7
Military Network: 96161 4216/4217
Facsimile number: 01793 314232
Military Network: 96161 4232
E-mail: publications@dcdc.org.uk

DISTRIBUTION

Distribution of JDPs is managed by the Forms and Publications Section, DSDA Operations Centre, C16 Site, Ploughley Road, Arncott, Bicester, OX25 1LP. Requests for issue of this publication, or amendments to its distribution, should be referred to the DSDA Operations Centre. All other DCDC publications, including a regularly updated CD *Joint Doctrine Disk* (containing both JDPs and Allied Joint Publications (AJPs)), can also be demanded from the DSDA Operations Centre.

DSDA Help Desk: 01869 256052
Military Network: 94240 2052

All publications (including drafts) are available to view and download on the Defence Intranet (RLI) at: www.dcdc.dii.r.mil.uk

This publication is available on the Internet at: www.mod.uk/dcdc

JOINT DOCTRINE PUBLICATIONS

The successful conduct of military operations requires an intellectually rigorous, clearly articulated and empirically-based framework of understanding that gives advantage to a country's Armed Forces, and its likely partners, in the management of conflict. This common basis of understanding is provided by doctrine.

UK doctrine is, as far as practicable and sensible, consistent with that of the North Atlantic Treaty Organization (NATO). The development of national doctrine addresses those areas not covered adequately by NATO; it also influences the evolution of NATO doctrine in accordance with national thinking and experience.

Endorsed national doctrine is promulgated formally in JDPs.[1] From time to time, Interim JDPs (IJDPs) are published, caveated to indicate the need for their subsequent revision in light of anticipated changes in relevant policy or legislation, or lessons arising out of operations.

Urgent requirements for doctrine are addressed through Joint Doctrine Notes (JDNs). To ensure timeliness, they are not subject to the rigorous staffing processes applied to JDPs, particularly in terms of formal external approval. Raised by the DCDC, they seek to capture and disseminate best practice or articulate doctrinal solutions from which this can be developed for operations and training.

Details of the joint doctrine development process and the associated hierarchy of JDPs are to be found in JDP 0-00 *Joint Doctrine Development Handbook*.

[1] Formerly named Joint Warfare Publications (JWPs).

RECORD OF AMENDMENTS

Amendment Number	Date of Insertion	Initials

PREFACE

1. **Purpose**. JDP 3-64 *Joint Force Protection* is the principal publication for UK Joint force protection at the operational level and replaces JDP 1/99 *Force Protection in Joint Operations* in the UK Joint Doctrine Hierarchy. It draws together the overarching principles for a range of Joint operational doctrine publications that contribute to force protection, including Chemical, Biological, Radiological and Nuclear Defence, Force Protection Engineering, Explosive Ordnance Disposal, Joint Search, Ground-based Air Defence and Joint Personnel Recovery. This publication describes the coordinated measures by which threats and hazards to the Joint Force are countered and mitigated in order to maintain an operating environment that enables the Joint Commander the freedom to employ Joint Action. JDP 3-64 flows from other keystone doctrine, JDP 01 *Campaigning* and JDP 3-00 *Campaign Execution*, and provides considerations for the Commander's planning process described in JDP 5-00 *Campaign Planning*. It is aimed primarily at those responsible for the protection of the Joint Force on deployed operations,[2] specifically staff in the Permanent Joint Headquarters (PJHQ), Joint Force Headquarters (JFHQ) and their counterparts in subordinate headquarters.

2. **Structure**. JDP 3-64 comprises 4 chapters:

   a. **Chapter 1 – The UK Approach to Joint Force Protection** describes the strategic context in which the Joint Force operates and highlights the requirement for UK doctrine. It introduces the definition, enduring principles and explains the relationship between the UK approach to operations and force protection. It also describes the different approaches taken to force protection in each environment and acknowledges the wider dimensions of force protection which are required by multi-agency and multinational operations, and the implications of the media.

   b. **Chapter 2 – Joint Force Protection Policy and Planning** describes the generic roles, responsibilities and outputs of those staff within the MOD, PJHQ, JFHQ and Component headquarters responsible for force protection. It highlights the requirement for coordination within the Joint, multinational and multi-agency environments and the key factors to be considered in the planning process and during operations.

   c. **Chapter 3 – Joint Force Protection Risk** outlines the UK approach to risk levels and risk ownership as well as describing a

[2] Operations in the UK are covered in detail in JDP 02 *Operations in the UK: The Defence Contribution to Resilience*.

method of managing and prioritising force protection risk at the operational level.

d. **Chapter 4 – Joint Force Protection Execution** introduces a framework within which force protection measures can be applied.

LINKAGES

3. JDP 3-64 is linked with:

a. JDP 0-01 *British Defence Doctrine.*

b. JDP 01 *Campaigning*.

c. JDP 2-00 *Intelligence*.

d. JDP 3-00 *Campaign Execution*.

e. JDP 4-00 *Logistics for Joint Operations.*

f. JDP 5-00 *Campaign Planning*.

g. JDP 6-00 *CIS Support to Joint Operations*.

4. **Allied Doctrine**. NATO doctrine for force protection is contained within Allied Joint Publication (AJP)-3.14 *Allied Joint Doctrine for Force Protection* and Allied Tactical Publication(ATP) 80-25 *NATO Force Protection Directive*.

5. **Further Reference**. A detailed list of Allied and UK publications related to force protection is provided at Chapter 4 to this publication.

JOINT FORCE PROTECTION

CONTENTS

(INTENTIONALLY BLANK)

CHAPTER 1 – THE UK APPROACH TO JOINT FORCE PROTECTION

101. The spectrum of hazards and threats which confront the Joint force varies widely depending on the environment, mission type and intensity of conflict. In a deteriorating security situation, an increasing threat of violence against the force may also be accompanied by an increase in hazards. A breakdown in law and order will lead to criminality, public health and sanitation measures may fail, and potentially dangerous industrial, agricultural or medical facilities become neglected. As operations increase in intensity, the number of hazards and threats multiply, requiring more significant force protection measures to deal with them. Natural or man-made hazards may well present the most likely threat to the Joint force even if the actions of adversaries are the most dangerous. In common with other aspects of military operations, force protection is ultimately a balance between risk (sometimes poorly quantified) and finite resources. The successful weighing and judgement of this balance by commanders, and early consideration of force protection issues are key to maintaining freedom of action for the Joint force.

102. The UK approach to force protection is based on a set of principles focusing on iterative risk management and a framework of measures that provide a balance of proactive and reactive capability. While a commander is free to use any process which aids his thinking, he should be wary of assuming too much certainty in their outputs, since force protection is fundamentally dealing with a spectrum of unknowns. In it, adversaries, actors and environmental factors interact at a level of complexity that is impossible to model accurately given the number of variables. Joint Doctrine Publication (JDP) 3-64 *Force Protection* offers a method for considering and managing operational risk. However, as in all aspects of campaigning, it should be a commander's skill and judgement that remains of primary importance when decision-making in relation to force protection.

103. This chapter highlights the strategic and operational context relating to force protection. It describes the requirement for bespoke UK force protection doctrine as well as providing the UK definition and principles of force protection.

Strategic Context

104. For reasons of national interest, the UK will continue to conduct military operations overseas, most probably as part of a multi-agency response aimed at tackling security issues early. Such operations are likely to be conducted within a coalition framework, although the UK may still operate alone where necessary. In addition to Defence, Other Government Departments (OGDs),

Non-governmental Organisations (NGOs) and International Organisations will also play a significant role in some operations, particularly those conducted in support of the Military Assistance to Stabilisation and Development (MASD) Military Task. In future conflict, smart adversaries will continue to present us with a mix of threats that combine conventional, irregular and high-end asymmetry. Conflict could involve a range of trans-national, state, group and individual participants who will concentrate and operate globally and locally, and come together for mutual benefit. Conflict may involve concurrent inter-communal violence, terrorism, insurgency, pervasive criminality and widespread disorder. Such operations are likely to be characterised by a blurring of the tactical, operational and strategic levels of war and increased media attention.[1] This is because as part of the multi-agency response, the requirement to coordinate national instruments of power at the tactical level, drags down some characteristics of the operational level into the tactical. Joint force protection is a fundamental enabling activity within campaigning and must be considered from the outset of the planning process.

SECTION I – UK JOINT FORCE PROTECTION DOCTRINE

105. North Atlantic Treaty Organization (NATO) doctrine describes a predominantly passive approach to force protection with an emphasis on minimising vulnerabilities.[2] This approach has evolved from the Cold War survive to fight mantra that remained prevalent in the 1990s. The UK pursues a more proactive approach, centred on an iterative risk management process. In contrast to NATO doctrine, the UK considers that force protection is applicable across the spectrum of military activities and includes capabilities that can directly counter action by adversaries rather than simply mitigating its effects. To that end, there is a requirement to articulate the UK approach to Joint force protection and highlight how it is considered within the campaigning process. Where there are variations, UK doctrine has primacy for UK national and UK-led operations.

[1] The Future Character of Conflict: The Ministry of Defence (MOD) Position by DCDC, September 2009.
[2] Allied Joint Publication (AJP)-3.14 *Allied Joint Doctrine for Force Protection*, defines force protection as '*measures and means to minimise the vulnerability of personnel, facilities, materiel, operations and activities from threats and hazards in order to preserve freedom of action and operational effectiveness thereby contributing to mission success*.'

UK Definition

106. The UK definition of Joint force protection is:

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

The UK definition is derived from the requirement for force protection within the context of the UK approach to operations. The definition draws the distinction between Joint force protection and Joint Action and highlights that force protection is an enabling activity.

Principles of Joint Force Protection

107. **Hazard and Threat Assessment**. A comprehensive hazard and threat assessment based on accurate and timely Intelligence is the basis for risk analysis and management activity and the selection of force protection measures. Building on the initial Joint Intelligence Preparation of the Environment (JIPE), this continuous process is informed by all sources. Where dedicated force protection assets are deployed, they will require access to these sources and potentially the ability to task assets to provide the requisite level of situational awareness. More detail on the type and range of hazards and threats is provided in Chapter 4.

108. **Risk Analysis and Management**. Together, risk analysis and management are the tools that enable the development of a plan to counter and mitigate the problems identified in the hazard and threat assessment. Having identified all potential hazards and threats, consideration must be given to the likelihood of occurrence and, in the case of adversaries, their most likely and most dangerous potential courses of action. Consideration must be given to the vulnerability of critical assets and the significance of their loss. A plan is then developed to counter and mitigate hazards and threats. As a general principle, risk management responsibility must be delegated to the lowest appropriate level of command. However, some force protection risks are of such strategic significance that this is not appropriate; in such cases ownership and management will remain at the Joint Force Commander (JFC) level or higher. Inevitably, a balance has to be struck between other activities, force protection and the finite resources available in theatre. The UK approach to force protection risk is detailed at Chapter 3.

109. **Coordination and Integration**. Force protection activity must be fully coordinated across components and multinational elements for effective

battlespace management, provide a degree of standardisation across the Joint Operations Area and make best use of finite resources. It is essential to coordinate and integrate force protection planning at the strategic, operational and tactical levels in order to ensure a unified approach and mitigate vulnerabilities that an adversary might otherwise exploit.

110. **Flexibility**. Force protection measures should have the flexibility and agility to respond rapidly to new circumstances, providing contingency options and, where possible, redundancy. Flexible force protection measures provide the commander with the resilience to meet unforeseen circumstances.

111. These principles are shown within Figure 1.1 to illustrate the UK approach to Joint force protection.

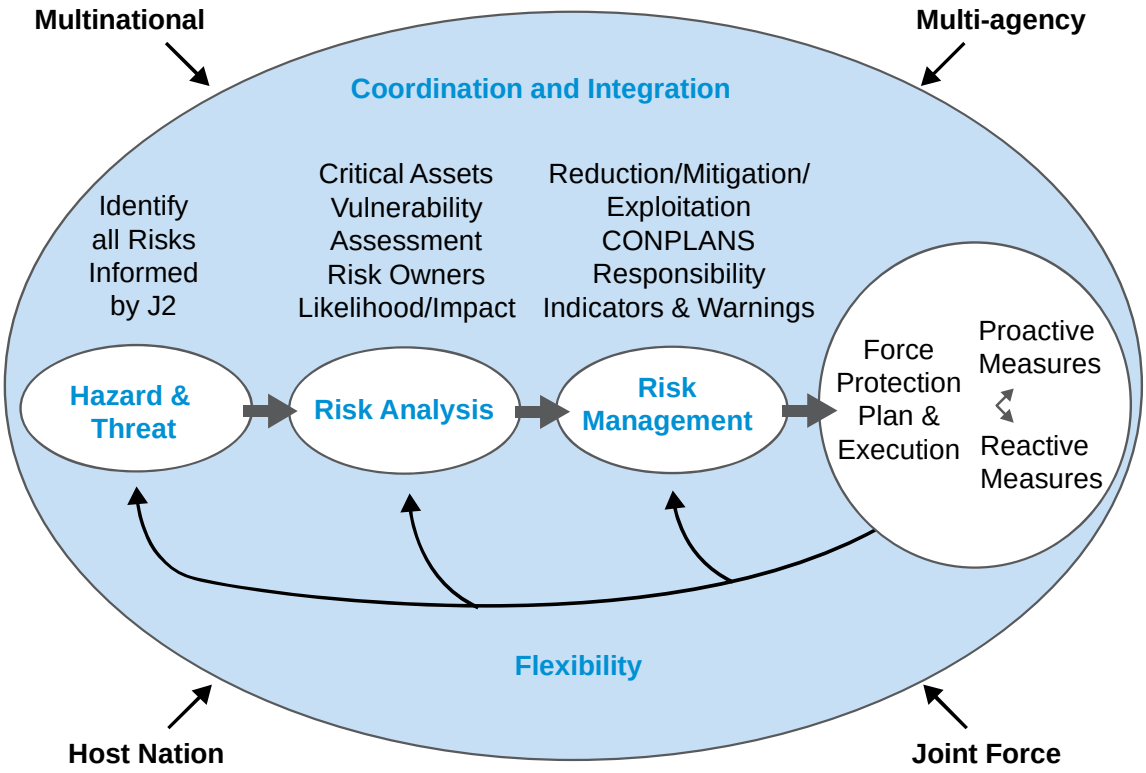

Figure 1.1 – Joint Force Protection Principles

Operational Context

112. **The UK Approach to Operations and Force Protection**. The UK pursues a manoeuvrist approach to operations that places a premium on shattering an enemy's overall cohesion and will to fight, rather than simply depleting his materiel or gaining territory for its own sake.[3] Joint action is the

[3] Joint Doctrine Publication (JDP) 01 *Campaigning*, page 3-12.

means used to achieve this effect and is defined as the deliberate use and orchestration of military capabilities and activities to realise effects on other actors' will, understanding and capability, and the cohesion between them.[4] Joint action is implemented through the coordination and synchronisation of fires, influence activities and manoeuvre. The UK's proactive approach to force protection means that the boundaries between force protection and Joint Action frequently overlap; it is often difficult to discern where one activity ends and the other begins. For example, at the operational level, deliberate activity undertaken to remove a potential threat to the Joint force might include anti-submarine warfare, counter-fires or offensive counter-air operations. While these activities will inevitably enhance the protection of the force, they are considered as deliberate combat operations in their own right and hence Joint action rather than force protection. Conversely, at the tactical level, the use of fires against an adversary using or attempting to use force against static locations such as a logistics site or a Sea/Air Point of Disembarkation would be considered as force protection activity rather than a deliberate use of Joint action. Fundamentally, force protection activity should enable the Joint force's freedom to operate in spite of the presence of hazards or threats in the area of operations. A contemporary example at the operational level is the proactive approach to countering the improvised explosive device threat in Afghanistan, which seeks to predict, prevent, detect, exploit, neutralise and mitigate the threat in order to enable operations to continue.

113. The Operational Framework is derived from the manoeuvrist approach and provides a JFC with a way to visualise effects and activities and, potentially to articulate his intent. It comprises 5 broad functions: Shape; Engage; Exploit; Protect and Sustain. Within this framework, protect preserves the capabilities of a Joint force so that they can be applied as planned. The same components against which a JFC seeks to engage an opponent (will, understanding and capability) are also those in his own force that must be protected, as it is these upon which an opponent is likely to focus his actions. Since sustain operations ensure the means by which a JFC can shape, engage, exploit and protect, they represent an obvious target for any opponent. A JFC will identify his own critical vulnerabilities and seek to protect them. Force protection provides the means to achieve this, but its success in execution rests upon sound risk management, and a holistic approach to countering and mitigating threats and hazards.

114. Force protection becomes of particular concern to the JFC whenever elements of the force are in static locations, pinned down by time or space constraints, by adversary action, terrain, weather, operating characteristics or other circumstances. In such situations, for example a deployed (and

[4] JDP 01.

immobile) operating base near to a populated area, the commander's ability to use fires, manoeuvre or influence in order to prevent attacks on the Joint force may be constrained and hence force protection becomes a major consideration. The degree to which force elements are likely to be static varies between environments, and this has led to noticeable differences in the approach taken to force protection in each (this is explored in greater detail later in this chapter). While static operating locations represent an important focus for force protection, due to their ease of targeting, force protection measures also apply to manoeuvre elements, for example, individual and platform protective measures.

115. To be effective, routine force protection measures executed at the tactical level such as dress states, personnel and vehicle equipment fits and robust tactics, techniques and procedures, must be coordinated at the operational level. As the resources available to the deployed force will be finite, and the range of possible hazards and threats very large, a rigorous and dynamic process of risk assessment, resource allocation and risk reduction is required at the operational level to ensure that the tactical measures taken are sufficient, agile and coherent; to be effective against the threat. This process is described in detail in Chapter 3.

116. Force protection also contributes directly to the physical and moral components of fighting power. The timely provision of demonstrably effective force protection capability in the face of an escalating threat will enhance the perception of worth held by those on operations and help maintain or improve confidence in political and military leadership.

117. **The Relationship between Security and Force Protection**. The term security has many definitions depending on the context in which it is used. In its broadest sense, security can relate to societal conflict or human security, but this publication does not address these issues. The wider aspects of security are described in detail in the National Security Strategy, JDP 0-01 *British Defence Doctrine* (BDD) and JDP 3-40 *Security and Stabilisation: The Military Contribution*. BDD also describes security as a principle of war '*the provision and maintenance of an operating environment that affords the necessary freedom of action, when and where required, to achieve objectives*'.[5] Security in this sense is also broader than force protection as it may include activity such as flank protection for manoeuvre forces. Force protection may therefore be considered as subsidiary to security as a principle of war.

[5] JDP 0-01 *British Defence Doctrine* (3rd Edition).

118. At the tactical level, JDP 03 *Security in the Contemporary Operating Environment*[6] defines security as '*the condition achieved when designated personnel, information, materiel, activities and installations are protected against espionage, sabotage, subversion, terrorism and other threats, such as organised crime, as well as against loss or unauthorised disclosure*'. In this context, there are 2 categories of security: Protective Security, the organised system of defensive measures instituted and maintained at all levels, which encompasses the totality of security measures across defence; and Operations Security (OPSEC), measures that preserve the secrecy of current operations and future plans. Protective Security is considered as a subordinate function of force protection while OPSEC is an enduring command responsibility which is of particular importance in supporting force protection measures. Protective Security is a directed activity regulated by Joint Service Publication (JSP) 440 *The Defence Manual of Security*.

119. **The Joint Force**. The Joint force is defined as '*a force comprised of significant elements of 2 or more Services operating under a single commander authorised to exercise operational command or control*'.[7] The JFC is explicitly responsible for the force protection of the Joint force including civilians directly employed by the Ministry of Defence; this includes contractors. As civilians accompanying the force, Contractor Support to Operations are to be included when planning for force protection. The extent to which contractors' personnel are able to self protect and are able to contribute to collective defence will depend on the nature of their contractual engagement. Detailed guidance on the provision of force protection to contractors and the contribution that they can provide should be sought from Permanent Joint Headquarters (PJHQ) and Assistant Chief of the Defence Staff (Log Ops) staff. JSP 567 *Contractor Support to Operations* provides a policy overview covering Sponsored Reserves, Contractors on Deployed Operations and Private Military and Security Companies (PMSCs). In contemporary operations, the JFC may also have responsibility either formally or informally for the protection of personnel from OGDs, NGOs and International Organisations and may need to consider the implications of embedded partnering with local security forces for force protection. Although force protection is predominantly the responsibility of National Contingent Commanders (discussed further in Chapter 2), in multinational operations situations may occur where one nation's personnel are reliant on the force protection measures provided by another. For a Joint force and in multi-agency and multinational operations, coordination of force protection activity across nations is a key planning consideration.

[6] JDP 03 *Security in the Contemporary Operating Environment*.
[7] JDP 0-01.1 *United Kingdom Glossary of Joint and Multinational Terms and Definitions* (7th Edition).

SECTION II – THE ENVIRONMENTS AND FORCE PROTECTION

120. Each Service has developed a different approach to force protection as a consequence of the vulnerability of force elements in the environments in which they operate. In the land environment, force protection is seen as part of everyone's job and it is not considered as a discrete activity. Conversely, in the air environment, the vulnerability of air platforms based on the ground has led to the development of dedicated force protection force elements. At the operational level, understanding the different approaches and requirements of each environment is crucial to achieving coordinated and coherent force protection planning and execution. Moreover, in addition to the traditional environments, modern operations rely on the Electromagnetic Spectrum (EMS) and the information environments, including cyberspace. Commanders and staff must have an understanding of the unique force protection requirements in each environment and the contribution that each component can provide to Joint force protection.

121. **The Maritime Environment**. British Maritime Doctrine[8] considers force protection in its widest sense, noting that '*a maritime force…will not only require self protection but will inevitably contribute to the overall protection of the Joint force itself*.'[9] Where manoeuvre may be exploited and fires are relatively unrestricted, the Navy will provide force protection as an integral part of its role. Force protection becomes a prominent factor where maritime forces are required to transit maritime choke points, enter or leave harbour, or manoeuvre in restricted waters[10] for operational, maintenance or other reasons. Where maritime manoeuvre is restricted, maritime forces become increasingly vulnerable to asymmetric attack in addition to the conventional threat from enemy forces; for this reason much of the UK maritime focus on force protection is devoted to countering the asymmetric threat. A congested littoral environment challenges the production of a recognised maritime picture and as a consequence, warning and reaction time is likely to be significantly reduced, determining the intent of numerous, unidentified small craft operating in close proximity to maritime units is a particular challenge. Asymmetric threats range from suicide craft, unmanned vehicles and semi-submerged vessels to multi-axis swarm attacks by fast attack craft. It also includes low, slow flying aircraft, such as microlights or small private aircraft. Maritime forces may also be restricted in time and space by certain operations, such as mine clearance and amphibious operations or when supporting forces ashore with aviation, Naval Fire Support or critical command and control capabilities.

[8] BR1806 *British Maritime Doctrine* (3rd Edition).
[9] BR1806, page 152.
[10] For example, where maritime units are constrained by the available depth or width of navigable water or other navigational hazards.

122. **The Land Environment**. Land forces consider force protection to be an intrinsic part of operations, and force protection is not considered separately in the list of tactical activities in Army Doctrine Publication (ADP) *Operations in the Land Environment*. Nevertheless, the land commander is encouraged to scale the effort and resources devoted to force protection according to the risk so as not to detract from those required for shaping, engaging and exploiting operations. Therefore, the underlying philosophy and considerations surrounding force protection in the land environment are similar to that at the joint level, albeit force protection is not generally considered as a discrete activity.

123. **The Air Environment**. Aircraft are scarce, expensive and relatively fragile. The operating bases that they depend on are large, static areas whose locations will become well-known to an adversary (except those operating from an underway maritime platform). Air operating locations are difficult to disguise or relocate and they have limited redundancy; there will be few suitable bases in theatre and they are likely to be crucial to the success of the joint campaign. The strategic consequences which could arise from the loss of air freedom of manoeuvre, or loss of a key air platform, mean that air force protection must be highly proactive, requiring the employment and coordination of a wide range of capabilities. Force protection is therefore a particular characteristic of air and space power and a critical enabler for achieving control of the air.[11] The vulnerability of air operating locations, including both operating bases and Tactical Landing Sites, necessitates protection in depth through a layered approach. This should include the establishment of a Ground Defence Area (GDA), extending well beyond the perimeter of the base, in order to prevent direct and indirect attacks being targeted against aircraft (both on the ground and in the air), facilities or personnel. Furthermore, the linkage between countering and mitigating adversary action, and the immediacy of air operations requires that the GDA is placed under the control of the air base commander. Where aircraft operate from land locations, the RAF has developed specialist organic force protection assets with specialised doctrine, structures, equipment scales and training[12] tailored to the particular context of air operations.

[11] Air Publication (AP) 3000 *British Air and Space Power Doctrine* (4th Edition), page 38.
[12] AP 3241 *RAF Force Protection Doctrine for Air Operations*; AP 3241A *Force Protection for Air Operations CONOPs;* AP 3241B *RAF Force Protection Operations Manual*; AP 3241C *RAF Force Protection TTPs*.

124. **Cyberspace and the Information Environment**. Cyberspace,[13] as part of the information environment, is as much a part of the contemporary operating environment as the land, sea or air. However, outside of specialist organisations, it is a domain which is poorly understood. Its advantages are already exploited on a daily basis but equally, it is not possible to avoid the range of threats inherent within it. Military applications include: command and control; logistics; unmanned operations; and, increasingly, onboard monitoring systems. Cyberspace is both ubiquitous and indispensable. This makes it something that must be understood, secured and, if an advantage is sought within it, ultimately controlled; it is no different from the land, sea and air in this respect.

125. UK military forces are already so dependent upon cyberspace that they cannot afford to operate in a way which would subsequently deny it to them. This reinforces the need for robust Computer Network Defence (CND) which must be comprehensive; a computer cannot be partially defended as an adversary will exploit any weakness in either software, firmware,[14] connectivity or through physical access to the machine itself. CND is a non-discretionary element of force protection and will play an increasingly prominent role in future operations. Commanders and staff should seek detailed guidance on CND from PJHQ J6 Information Assurance.

126. **The Electromagnetic Spectrum Environment**. The EMS environment covers different types of electromagnetic radiation from radio waves (at low frequency/long wavelength) through visible light to gamma rays (at high frequency/short wavelength). It supports a wide range of military activity including communications, navigation and surveillance. The effective understanding, protection and exploitation of the EMS should be the product of a robust Battlespace Spectrum Management policy, and is fundamental to the successful conduct of military operations.

127. Electromagnetic energy can be used directly to generate physical effects. For example, an electromagnetic pulse can disrupt the EMS and electronic equipment, while directed energy weapons can achieve similar but more targeted effects on personnel and equipment. Radiation of electromagnetic energy can also disrupt use of the EMS. Electronic defence covers active and passive measures and includes protection of forces, platforms, equipment and information. It also includes measures to safeguard our own use of the EMS.

[13] A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. A working definition in general use within Ministry of Defence (MOD), and under consideration by the Joint Doctrine Steering Committee.
[14] Permanent software programmed into read-only memory (Concise Oxford English Dictionary).

SECTION III – MULTI-AGENCY, MULITNATIONAL AND HOST NATION CONSIDERATIONS

Multi-agency

128. The contemporary battlespace is further complicated by the presence of other elements who may be providers or recipients of force protection. Multi-agency operations may be limited or constrained by the level of force protection which the military are able to provide. Civilian organisations are almost certainly unable to accept the same level of risk as military forces. If the mission is reliant on effects which only civilian actors can provide, then success may hinge on force protection issues. This situation can be further complicated when certain elements of force protection are provided by PMSCs. While the capability these offer may be a valuable addition to the overall effort, freeing up military assets that would otherwise be required for force protection tasks, their use must be carefully monitored and, where possible, coordinated by the joint staff if a coherent approach to influence activity and perhaps campaign legitimacy is to be maintained at the operational level. Key command considerations for interaction with PMSCs include legal, interoperability, OPSEC and Protective Security and support. Guidance for operational commanders is contained in JDN 1/08 *Military Interaction with Private Military and Security Companies* and detailed legal guidance should be sought from a legal advisor or via reachback, through PJHQ J9 Legal. As with multinational operations, force protection in a multi-agency environment can be a force multiplier or a constraint. It requires early consideration by joint planning staffs, in concert with other agencies.

Multinational

129. National contingents within an alliance or coalition can be expected to have a different appetite for risk and hence may have varying outlooks and approaches to force protection. Furthermore, NATO doctrine[15] states that force protection provision is a national responsibility. National contingents will have their own equipments, tactics and procedures for force protection tasks which must be harmonised if the force is to operate together. The JFC should ensure that a coherent force protection policy is developed that takes account of the varying approaches taken by other national contingents.

[15] AJP-3.14 *Allied Joint Doctrine for Force Protection.*

Host Nation Considerations

130. Similar considerations apply where the Joint force is operating with the consent of a host nation, usually under a Status of Forces Agreement. The host nation may be responsible for elements of force protection, such as guarding fixed installations, and may have a role protecting lines of communication. The commander must be confident that the capabilities the host nation deploys are appropriate to the perceived hazards and threats. Equally, the posture adopted by the host nation and any constraints it may impose must not be allowed to erode the legitimacy of the Joint force.

The Media, Reputation and Force Protection

131. Modern communications and media mean that politicians can be called to account, almost in real time, for the loss of life, perceived lack of resources and campaign design. This can pull politicians down below the strategic level and involve them in operational and even tactical matters. Equally, tactical activity played in the presence of the international media can also have a strategic effect, particularly in stabilisation and peace enforcement operations. Modern information and communication technologies allow journalists, members of the civilian population, or indeed members of the participating combatants, to record and publish material to a potentially worldwide audience. In a society which is increasingly risk-averse and litigious, the effect of the media is to magnify any error in the risk management process inherent in force protection. Negative comment, whether via the media or in public discourse, ultimately affects the reputation and the credibility of the UK Armed Forces. This can have a particular impact on force protection as the reputation of a force provides a deterrent effect; if this is sufficiently eroded, it is more likely that further attacks will be launched. Guidance for commanders on media operations is provided in JDP 3-45.1 *Media Operations*.

CHAPTER 2 – JOINT FORCE PROTECTION POLICY AND PLANNING

201. This chapter describes the force protection roles and responsibilities of Ministry of Defence (MOD), Permanent Joint Headquarters (PJHQ), Joint Force Headquarters (JFHQ) and Component headquarters staff. The Chapter highlights the process for force protection planning from the initial planning stages within the MOD to the conduct of force protection at the component level. Force protection is not considered as a separate or discrete function during the formal estimate process within either the MOD or PJHQ and consequently many of the hazards and threats will be identified as the planning process evolves. To that end, every staff officer within the planning process must have an understanding of the principles of force protection highlighted in this publication and knowledge of where to seek specialist advice.

SECTION I – FORCE PROTECTION WITHIN CAMPAIGN PLANNING

202. **Defence Crisis Management Organisation**. The UK's approach to crisis management, and the MOD's role within the Defence Crisis Management Organisation (DCMO) as the Strategic Military Headquarters, is described in detail in Joint Doctrine Publication (JDP) 0-01 *British Defence Doctrine*, JDP 01 *Campaigning* and JDP 5-00 *Campaign Planning*. In short, the DCMO provides the MOD focus for crisis management, both as a Strategic headquarters and a Department of State. The DCMO translates political intent into military activity and issues direction to and monitors reporting from, deployed commands. At the outset of a crisis, the DCMO, in liaison with Other Government Departments (OGDs), other national governments and international organisations as part of a comprehensive approach, will produce a Political-Military Estimate. The central aim of the Political-Military Estimate is to consider any potential crisis and to assess political implications against military feasibility and sustainability. The aim is to give politicians informed choices as to the ends and ways. This high-level estimate is then used as the basis to initiate a Chief of the Defence Staff (CDS) Planning Directive. Force protection is only considered in the most general terms at this stage.

203. **Military Strategic Estimate**. Once Initial Planning Guidance or a CDS Planning Directive has been produced by the MOD, a Military Strategic Estimate will be completed. The Military Strategic Estimate is the Joint Commander's Estimate which is normally conducted by PJHQ under a J5 lead, to:

a. Analyse the UK's political and military intentions.

b. Identify the military mission and scope the military tasks and forces required, in order to achieve the specified end state.

c. Identify and assess military courses of action.

204. J5 will form a pan-divisional team to produce this estimate, ensuring that specialists from all areas are represented, including OGDs where appropriate. J5 staff may consult force protection specialists as necessary or seek an input to the estimate from the PJHQ J3 Force Protection Team.

205. **The Permanent Joint Headquarters J3 Force Protection Team**. The PJHQ J3 Force Protection Team is an integral part of many of the MOD's various working groups and ensures that MOD force protection policy is converted into pragmatic and workable direction to deployed commanders. The primary aims of the Force Protection Team are:

a. Provide specialist advice over the full range of force protection areas and for all environments.

b. Ensure that force protection coherency across all operational theatres is maintained.

c. Ensure that force protection risks that may have operational or strategic impact are identified, understood and, where required, mitigated to acceptable levels.

d. Assist in the conduct of the Military Strategic Estimate in order to determine constraints, opportunities and Requests for Information (RFI).

e. Contribute specialist force protection inputs to all other PJHQ J5 and JFHQ planning processes as required.

f. Dependent on the type of operation, conduct a force protection reconnaissance. A list of considerations that may be used by the PJHQ J3 Force Protection Team during the estimate and reconnaissance process is detailed at Annex 2A.

206. **Chief of Defence Staff's Operational Directive**. If a crisis develops into an operation, the Military Strategic Estimate provides the basis for CDS' Operational Directive to the Joint Commander. The directive articulates the military strategic objectives, the desired strategic and military end-states and constraints to be applied to operational planning. Additionally details of forces and resources to be assigned, designation of the Joint Operations Area (JOA),

the anticipated duration of the campaign with guidance on sustainability, the legal position and Rules of Engagement (ROE) will be included. Force protection is an integral part of CDS' Operational Directive to the Joint Commander and the PJHQ J3 Force Protection Team works alongside J5 staff to produce a force protection paragraph within the directive. The force protection paragraph will provide specific force protection direction on the security of personnel, mission essential assets and campaign infrastructure. CDS' Operational Directive also tasks the Joint Commander to provide force protection guidance to the theatre commanders within the Joint Commander's Mission Directive.

207. **Joint Commander's Mission Directive**. The Joint Commander will exercise Operational Command (OPCOM) of assigned forces. He is responsible for: giving further direction and advising the theatre commander as necessary; through the Operational Teams, deploying sustaining and recovering the force; and monitoring and reporting to CDS on the progress of the campaign. As such the Joint Commander will issue a mission directive, coordinated by J5, to the Joint Task Force Commander (JTFC) that expands, where necessary, on the direction given in CDS' Operational Directive and will include his own personal direction. The Joint Commander's Directive will also include a short paragraph that details the operational force protection direction. Moreover, it will refer to the Force Protection Annex of the Theatre Reference Document for detailed force protection guidance. The Theatre Reference Document is an overarching document that provides J1-J9 staff direction to deployed commanders, components and front line commands. The Theatre Reference Document collates the myriad of operational directives and issues them under cover of a frontispiece. The following direction is contained within the Theatre Reference Document:

a. Forces assigned.

b. ROE authorisation.

c. Intelligence and Security Plan.

d. Targeting Directive.

e. Information Campaign.

f. Finance.

g. Logistics, including the Joint Mounting Order.

h. Personnel.

i. Medical.

j. Communications and Information Systems.

k. Information exploitation.

l. Force protection.

The Force Protection Annex to the Theatre Reference Document will include direction on risk assessment, risk management, specific force protection priorities that are to be addressed and multinational force protection issues. Importantly, the annex tasks component commanders with producing a force protection directive that sets out the baseline force protection posture to be applied to all force elements under command.

208. **Operational Estimate**. The Operational Estimate is normally conducted by the JFHQ/Joint Task Force Headquarters (JTFHQ) staff, to analyse the military mission, confirm or adjust the forces required and to prepare the campaign plan. Once again, this process does not specifically include dedicated force protection specialists and JFHQ/JTFHQ staff seek input or guidance as required.

209. **Outputs of the Planning Process**. Further to the estimate process, there are a number of plans and guides maintained by PJHQ:

a. **Joint Planning Guides**. Joint Planning Guides comprise generic planning data for a particular region or theatre. Joint Planning Guides may also provide generic advice for a particular type of operation, such as Disaster Relief or a Non-combatant Evacuation Operation. They are produced by J5 on the authority of the Chief of Joint Operations. The periodic review of Joint Planning Guides is initiated by J5 staff and occurs as required (roughly every 2 years). Force protection advice is included within the Joint Planning Guides and is provided by the PJHQ J3 Force Protection Team and JFHQ.

b. **Joint Contingency Plans**. Joint Contingency Plans are prepared by J5 for situations where there is a particular likelihood of an operation being mounted or the anticipated warning time is reduced. In addition to the planning data contained in Joint Planning Guides, Joint Contingency Plans contain specific information on the military capabilities that may be required and their deployment options, including readiness states where appropriate. They are written in response to specific planning direction issued by the MOD and approved by Deputy Chief of Defence Staff (Operations). Force

protection advice is included within the Joint Contingency Plans and is provided by the PJHQ J3 Force Protection Team and JFHQ.

c. **Campaign Plans**. Once the Joint Commander's mission directive is issued, the JTFC can conduct his Operational Estimate and develop the Campaign Plan. Campaign Plans are written by the staff of the JTFC appointed for a specific operation, assisted by other divisions within the PJHQ and the supporting commands. These plans are maintained by JFHQ. Force protection specialists will form part of JFHQ's staff.

d. **Civil Contingency Plans**. Civil Contingency Plans are produced by the British Embassy/High Commission. They establish the Warden System and provide a procedure for orderly evacuation if required. Civil Contingency Plans are held centrally by the Foreign and Commonwealth Office and some are held by J5 on the advice of the relevant J5 Desk Officers.

SECTION II – JOINT FORCE HEADQUARTERS, JOINT TASK FORCE HEADQUARTERS AND COMPONENT HEADQUARTERS

Joint Force Headquarters and Joint Task Force Headquarters

210. JFHQ/JTFHQ is responsible for the operational estimate. Within the JFHQ, force protection is coordinated by J3/J7 in order to ensure it is considered across all branches. The JFHQ/JTFHQ conducts its campaign planning in accordance with Joint Doctrine Publication (JDP) 5-00 and, to ensure an integrated planning effort, utilises the Operational Planning Team (OPT) concept to bring specialists together. To support the force protection element of the planning effort JFHQ/JTFHQ assembles 3 specific OPTs. The first, during mission analysis, identifies and quantifies threats and hazards. The second, as the decisive conditions and supporting effects are identified, looks at mitigation. The third, held as required, concerns the implementation of mitigation and checks effectiveness.

211. The Force Protection OPTs employed by the JFHQ/JTFHQ utilise the risk analysis and risk management process described in Chapter 3. The output of the process is recorded in a risk register and used to support analysis of the commander's collective risks. The Force Protection OPTs will, as a minimum, include specialists from J2, Joint Force Engineering, J4 Medical, J33 and representatives from the components. They may also include other specialists as necessary, such as a Chemical, Biological, Radiological and Nuclear (CBRN) Adviser, J3 Influence or a specialist in Computer Network Defence.

212. The outputs of the operational estimate are:

a. **Campaign Directive**. As Joint force protection is an enabler of Joint action, it will only appear in the campaign plan where its absence would prevent the achievement of a decisive condition.

b. **Operation Plan and Operation Order**. The JFHQ/JTFHQ will produce Operation Plans and Operation Orders to support the Campaign Directive. These documents often delegate responsibility for force protection to component commanders according to environment, location or task.

c. **Force Instruction Document**. The Force Instruction Document provides enduring details and procedure for working on an operation with the JFHQ/JTFHQ. It is written specifically for the operation and contains specific force protection direction. The force protection section provides overarching policy and JTFC's force protection intent and priorities. It will also include annexes on security, CBRN, Ballistic Missile Defence, personal protection, force protection engineering, combat identification, counter indirect fire and Counter-Improvised Explosive Device (C-IED).

213. **Operational Level Approach to Force Protection**. It is recognised that force protection measures can be dictated by threat (maximising on risk) or they may be dictated by task (maximising on opportunity). The JFHQ/JTFHQ will identify the approach for Joint force protection for the operation. The operational level approach to force protection will be stated in the Force Instruction Document, but does not constrain the component commanders from applying the most appropriate approach at the tactical level.

Maritime Component Headquarters

214. Within a JOA, the Maritime Component Commander (MCC) has responsibility for the force protection of all maritime assets and coordinates the measures required while ships are at sea. While the majority of these will be implemented by commanding officers from their own ships' capabilities as a routine part of maritime warfare, some platforms, such as Royal Fleet Auxiliaries, Strategic RO-ROs or Minor War Vessels, may require additional maritime resources, and this will be coordinated within theatre by the MCC. Where the threat is sufficient that a joint approach is necessary, the MCC will liaise with the staff responsible for J3 Organisation and Deployment and J3 Force Protection in the JTFHQ to obtain the necessary capabilities. The MCC is unlikely to include a dedicated force protection staff and the function will be

coordinated across the N3 warfare staff, drawing on expertise from the Navy Command Headquarters force protection staff as required.

215. As maritime units routinely transit in and out of the JOA during deployed periods, and may call into ports that lie both within and outside it, a different approach is taken to the coordination of force protection alongside. In order to provide a consistent approach from the point of view of the ships, the 'Maple Matrix' system is used regardless of whether the port concerned is in a JOA or not. The system consists of a periodic signal from the Navy Command N3 staff, which, read in conjunction with a matrix of force protection capabilities, details the measures to be taken in ports around the world. These will include some which may be partly or wholly provided by the host nation and will be arranged via the normal liaison process between the ship, UK diplomatic staff and the host nation authorities.

Land Component Headquarters

216. Within the Land Component Command Headquarters, the staff branches will interpret the Joint Commander's Directive and the Joint Force Headquarters Operational Estimate to ensure that all planning is coherent with the JFC's intent; this includes the force protection posture. Clear direction will be issued on force protection measures, constraints and the authority for decisions that are delegated to subordinate commanders. The headquarters may not include any dedicated force protection staff with the function coordinated by G3/5 staff or by specific counter threat staff such as C-IED. The intent must ensure that the force protection measures embrace all force elements within the land component, including entitled civilians, and addresses all aspects of the threat while considering the policies, doctrine and procedures of any allies, coalition partners and the host nation.

Air Component Headquarters

217. The Joint Force Air Component Headquarters (JFACHQ) may provide a national air headquarters, the framework and lead elements of a coalition air headquarters or provide representation within a headquarters led by another nation. The Joint Force Air Component Commander (JFACC) is responsible for planning, executing and assessing the air aspects of the JTFC's expeditionary campaign. The JFACHQ contains organic force protection staff who ensure the JFACC's intent, priorities, concerns and issues across the deployed force are understood so that force protection effort can be correctly coordinated and prioritised within the air component. The JTFC will usually delegate to the air component responsibility for Theatre Missile Defence (TMD) and air defence warning and with it, the responsibility for the timely dissemination of warnings within the air component and to other component

headquarters. In order to provide a timely response to theatre missile attacks, the TMD Warning Cell maintains continuous surveillance of the JOA using links to other national assets.

Joint Force Logistics Component Headquarters

218. A deployed Joint Force Logistics Component (JFLogC) headquarters requires its own J2/3/5/6/7 staff to plan and execute its core functions, including force protection. The lack of integral force protection, including firepower and mobility, make logistic force elements particularly vulnerable, which must be taken into account during planning in order that the JTFC understands the potential impact on operations. Close liaison with force protection staff in other component headquarters will be required to ensure the security of logistics personnel, materiel, equipment and infrastructure. Detail of the factors to be considered is expanded further in JDP 4-00 *Logistics for Joint Operations*, and includes: force protection during deployment; a criticality assessment of the contribution of logistics capabilities to operational success; a threat assessment against specific critical logistics assets; a vulnerability assessment, risk management and appropriate incident response. During the course of an operation command of the logistics component may pass to a Joint Force Support headquarters or a National Support Element particularly in a multinational environment. The nature of force protection is also likely to change, with increasing reliance on civilianisation, contractorisation and multinational support changing the vulnerability of the support network to attack.

Special Forces Component Headquarters

219. Special Forces (SF) operate across the range of Military Tasks set out in Defence Strategic Guidance, and are held at appropriate readiness for Standing Strategic Tasks, Standing Home Commitments, Standing Overseas Commitments and Contingency Operations. SF operations are inherently high risk and therefore a careful balance of force protection measures is required. Too many may reduce the risk, but hinder the freedom of action or movement, which is often vital to success. Conversely, too few protection measures may increase the risks to SF operators and could jeopardise the operation.[1] The key thread common to all SF tasks is access to the highest level intelligence, thereby allowing effective planning to counter and mitigate against identified risks. On expeditionary operations, there are 2 key considerations, protection of extended lines of communication and effective combat identification and battlespace management, to prevent fratricide of SF operating behind enemy lines and/or in areas targeted by deep strike assets.

[1] JDP 3-05 *Special Forces Operations*.

ANNEX 2A – FORCE PROTECTION PLANNING FACTORS FOR THE ESTIMATE PROCESS

2A1. Potential planning factors that may need to be considered during the estimate and reconnaissance process are listed below. The list is intended as a handrail and is neither prescriptive nor exhaustive; each factor should be analysed according to its interrelationship with others.

2A2. Operational Environment:

a. Background to Conflict/Situation.

(1) Historical drivers.

(2) Reasons for UK involvement.

(3) Lessons from previous conflicts/operations.

b. Current Situation.

(1) Diplomatic/Political.

(2) Military.

(3) Economic.

(4) Humanitarian.

(5) Information/media.

(6) Likelihood of escalation/de-escalation.

c. Rules of Engagement (ROE)

(1) UK ROE Profile.

(2) UK Political Position Indicator.

(3) Theatre-Specific ROE Profile, if relevant.

(4) Tactical Engagement Directive.

(5) Dormant or situation-dependent ROE.

(6) Escalation of Force procedures.

d. Legal.

(1) Status of Forces Agreement, Memorandum of Understanding and Technical Agreements.

(2) Host Nation limitations on Freedom of Action.

2A3. Ground/Battlespace (supported by and developed alongside Joint Intelligence Preparation of the Environment):

a. Impact of weather.

b. Vital Ground.

(1) Nature of the Operating Base. For example, austere, bare-base, well-found.

(2) Critical infrastructure.

(3) Physical protection/resilience.

(4) Entry Control Points.

(5) Prioritised Defended Asset List.

(6) Sectorisation.

(7) Mapping, imagery.

c. Key Terrain.

(1) Ground of tactical use to the adversary.

(2) Ground of tactical use to defenders.

(3) Ground that must be denied to the adversary.

d. Environmental.

(1) Climate.

(2) Altitude.

(3) Health – diseases, flora, fauna, endemic disease.

(4) Mines/Unexploded Ordnance.

(5) Road safety.

(6) Criminality.

(7) Internally Displaced Persons.

(8) Toxic Industrial Materials/Hazards.

(9) Cultural.

e. Lines of Communication.

(1) Location(s).

(2) Flow rates.

(3) Responsibility for protection.

2A4. Enemy Forces:

a. Adversary/Factions Centre(s) of Gravity.

(1) Critical Capabilities.

(2) Critical Requirements.

(3) Critical Vulnerabilities.

b. Dispositions.

c. Organisation.

(1) Physical structure.

(2) Levels of capability/commitment within organisation(s).

d. Intent.

(1) Doctrine/philosophy.

(2) Assessed short and long-term plans.

(3) Likely objectives.

(4) Previous actions.

e. Capability.

(1) Direct ground attack – including Special Forces.

(2) Ground-to-Air – Small arms fire and Man Portable Air Defence Systems (MANPADS)

(3) Air Attack – capability, unmanned aerial systems, theatre ballistic missiles.

(4) Maritime Attack – capability.

(5) Improvised Explosive Devices.

(6) Chemical, Biological, Radiological and Nuclear.

(7) Suicide attack.

(8) Intelligence gathering and targeting.

(9) Sabotage.

(10) Electronic Warfare.

(11) Computer Network Attack.

(12) Subversion.

(13) Theft.

(14) Intimidation.

(15) Mobility.

(16) Communications Security (COMSEC) and surveillance awareness.

(17) ROE.

(18) Media and Information Operations.

(19) Relationship with local population(s).

f. Adversary Potential Courses of Action.

(1) Most likely.

(2) Most dangerous.

2A5. Civilian Population/Neutral Groups:

a. Locations.

b. Demographics.

c. Cultural, religious and social dynamics.

(1) Key leaders and opinion formers.

(2) Cultural ‘red lines’.

(3) Language.

(4) External influences.

d. Attitude and opinions.

e. Impact of international, national and local news media.

f. Human Security.

(1) Physical security.

(2) Access to food and water.

(3) Access to healthcare.

(4) Employment.

(5) Ability to move unhindered.

g. Level of consent.

(1) Adversary/faction activity.

(2) Friendly activity.

h. Likely response to Support and Influence activity.

i. Pattern of life.

j. Employment in support of Friendly Forces.

k. Presence of Refugees/Internally Displaced Persons.

l. Presence and role of Non-governmental Organisations (NGOs).

(1) Attitude to adversary/factions.

(2) Attitude to friendly forces/coalition/host nation.

(3) Provision of security.

(4) Impact on local population.

(5) Underlying agendas.

2A6. Friendly Forces:

a. Military Strategic End-state.

(1) UK.

(2) Host Nation.

(3) Coalition.

b. Military Strategic Objectives.

(1) UK.

(2) Host Nation.

(3) Coalition.

c. Own/Host Nation/Coalition Centre(s) of Gravity.

(1) Critical Capabilities.

(2) Critical Requirements.

(3) Critical Vulnerabilities.

(4) Risk tolerance.

d. Burden-sharing requirements and responsibilities.

e. Command and Control Arrangements.

(1) Own.

(2) Task Organisation.

(3) Affiliated units.

(4) Potential for conflicts of interest between multinational elements.

f. Chain of Command’s Battle Rhythm and Reports and Returns requirements.

g. Disposition of flanking units and formations.

h. Other Government Departments.

(1) Role.

(2) Support requirements.

(3) Relationships with and between.

i. Liaison requirements.

(1) Up and Across.

(2) Inward.

j. Fratricide.

(1) Risks.

(2) Countermeasures and mitigation.

(3) Electronic fratricide.

k. Administration.

(1) Preparation requirements.

(2) In-theatre support

l. Logistics.

(1) Source of support.

(2) Host nation/Ally responsibilities.

(3) Ammunition storage and supply.

(4) Impact of explosive storage safety rules.

(5) Petrol, oil and lubricants (POL) storage and supply.

(6) Rations.

(7) Mechanical engineering.

(8) Transport.

(9) Convoy support/protection requirements.

(10) Stock dispersal and storage.

m. Medical.

(1) Support arrangements.

(2) Casualty Evacuation (CASEVAC) procedures.

(3) Environmental Health challenges and responsibilities.

(4) Theatre medical preparation requirements.

(5) Ability to assist Support and Influence activity.

n. Financial.

(1) Financial limitations or freedoms.

(2) Funding for Support and Influence activity.

(3) Availability of Commander's Compensation funding.

o. Media.

(1) Level of engagement.

(2) Impact on conduct of operations.

p. Training

(1) Training gaps and risks.

(2) Pre-deployment training requirements.

(3) Pre-deployment training equipment requirements.

(4) Reception, Staging, Onward Movement and Integration (RSOI) requirements.

(5) Own In-theatre training requirements.

(6) Facilities.

2A7. Own/Host Nation/Coalition Capability:

a. Air Battlespace Management.

b. Intelligence, Surveillance and Reconnaissance.

(1) Air – formal or *ad hoc* tasking.

(2) Electronic Intelligence.

(3) Space.

(4) Human Intelligence (HUMINT).

c. Counter Ground-to-Air.

(1) Aircraft Defensive Aid Suites and Tactical Techniques and Procedures.

(2) Information Management – warning and reporting.

(3) Extant ground activity.

d. Counter Indirect Fire.

(1) Command and Control.

(2) Battlespace Management.

(3) Intelligence and Exploitation.

(4) Sense.

(5) Prevent.

(6) Warn.

(7) Intercept.

(8) Respond.

(9) Protect.

e. Direct ground attack.

(1) Mitigation.

(2) Counter-attack.

f. Counter Improvised Explosive Device.

(1) Predict.

(2) Prevent.

(3) Detect.

(4) Neutralise.

(5) Mitigate.

(6) Exploit.

g. CBRN.

(1) Inform – sense, knowledge management.

(2) Protective Measures – physical protection, hazard management, medical countermeasures.

h. Control of Entry.

(1) Use of biometrics.

(2) Personnel inflow requirements (military and local nationals) and search.

(3) Vehicle requirements inflow and search.

i. Suicide attack.

(1) Detection.

(2) Mitigation.

(3) Escalation of force procedures.

j. Counter-intelligence and Communications Security.

k. Counter-sabotage – physical security and protection.

l. Electronic Warfare.

m. Computer Network Defence.

n. Policing.

(1) Jurisdiction.

(2) Special Investigations.

(3) Detention facilities.

o. Ground-Based Air Defence.

(1) All Arms Air Defence.

(2) Weapon Control Orders.

(3) Recognised Air Picture.

(4) Chain of Command and liaison.

p. Counter Adversary/Faction Mobility.

(1) Route denial.

(2) Canalisation.

q. Force Protection Engineering.

(1) Host nation/civilian support.

(2) Restoration of essential services.

r. Support and Influence Activity.

(1) Key Leadership Engagement.

(2) Security Sector Reform.

(3) Psychological Operations.

(4) Civil-Military Cooperation (CIMIC).

(5) Reconstruction.

(6) Veterinary and Medical Outreach.

(7) Position, Profile, Posture.

(8) Integration of non-kinetic and kinetic effects.

(9) Consent winning activity funding.

(10) Compensation.

s. Communication Information Systems.

(1) Availability.

(2) Interoperability.

(3) National security caveats.

(4) Battlespace Spectrum Management.

CHAPTER 3 – JOINT FORCE PROTECTION AND RISK

301. Military risk is defined '*as the probability and implications of an activity or event, of potentially substantive positive or negative consequences, taking place*'.[1] Force protection at the operational level is primarily about effective risk management. Moreover, from a moral, duty of care and legal perspective, it is necessary to demonstrate that in planning for operations, a comprehensive risk assessment has been undertaken. This is achieved by applying a standardised risk methodology to ensure that a consistent, auditable, strategic approach to force protection risk analysis and management is employed as part of planning processes. Joint Doctrine Publication (JDP) 5-00 *Campaign Planning* details an endorsed approach to military risk and this chapter builds on this approach in order to describe how risk analysis and risk management are applied to force protection planning. The model described can be used to help a commander to identify, analyse, prioritise and manage risks; it is simply an aid and does not replace the requirement for commanders' judgement.

SECTION I – UK APPROACH TO RISK LEVELS AND RISK OWNERSHIP

302. Defining the acceptable level of risk for any operation is an art not a science. The level of risk will change, sometimes rapidly, according to the strategic, operational and tactical circumstances, and may need to address multiple areas where risk levels differ markedly. Risk tolerance permits freedom of manoeuvre and enables mission success. Measures to manage risk at any level should not be constrained by an overly restrictive process.

303. **Political Level**. The Secretary of State (SofS) for Defence and the Chief of Defence Staff (CDS), in consultation with the Prime Minister, approve operational plans; thereby they implicitly accept ownership of the risks to the force associated with the operation on behalf of the Government. While SofS owns the risk, CDS is ultimately responsible for articulating that risk to the SofS for specific operations.

304. **Strategic Level**. CDS defines and regularly reviews the acceptable level of risk across the range of current operations, contingent tasks and departmental activity in consultation with his operational Chiefs of Staff, ensuring that Other Government Departments (OGD) are included as part of a comprehensive approach. He prioritises and directs the requisite force protection mitigation activity, in conjunction with the relevant operational commander(s), recognising the significance of accumulated risks and the

[1] Joint Doctrine Publication 01 *Campaigning* (2nd Edition).

strategic impact of the loss of scarce resources. CDS' directives provide the high level direction for operational risk management and describe how it is directed, coordinated and prioritised at the strategic level for each operation.

305. **Operational Level**. Operational-level risk is identified to CDS by Deputy Chief of the Defence Staff (DCDS) (Operations) and the appointed Joint Commander (normally Chief of Joint Operations (CJO)) through regular reviews as part of the operational planning process. As the owner of the operational-level risk, the Joint Commander is responsible for risk mitigation for those forces under his Operational Command. In addition, he has a responsibility to consult the front line commands to agree that appropriate measures are in place to minimise the risk to their personnel and equipment given that they retain full command.[2]

306. **Linkage between Levels of Risk**. In the same way that tactical events can have strategic repercussions, and strategic decisions can have tactical implications, so too, risks at the tactical level can have consequences at both the operational and strategic levels. Those managing risk should always be cognisant of this broader perspective, when assessing likelihood, impact and ownership in particular. In practice, risk will often percolate up the chain of command from the tactical commander to the operational and strategic levels.

307. **Multinational Operations**. Each nation determines how its personnel are employed, normally based upon its own acceptable levels of risk. Moreover, as the threat is unlikely to be uniform across the Joint Operations Area (JOA) and may be subject to frequent change, risk reduction and mitigation measures are unlikely to be uniform across a joint force. On multinational operations, risk mitigation should, in the first instance, be addressed through the multinational operational chain of command. However, a UK National Contingent Commander (NCC), usually either Commander British Forces (COMBRITFOR) or the Senior British Military Representative, will retain responsibility for force protection risk mitigation in respect of assigned UK forces through the national chain of command. Where the UK NCC is unable to mitigate risk to an acceptable level, CDS will engage with the multinational headquarters in order to implement an agreed mitigation process.

308. **Multi-agency Operations**. While OGDs, Non-governmental Organisations (NGOs) and International Organisations can (and do) work in highly hazardous situations, they may withdraw their personnel if they judge that a lack of security is preventing them from working effectively. Accordingly, commanders should appreciate the risk appetite of civilian partners, determine

[2] Current MOD force protection policy, published as 2007DIN03-007 *Policy for the Protection of UK Forces*.

their commitment of resources and personnel, and address as an integral part of their planning the consequences of multi-agency support being periodically or conditionally unavailable.

SECTION II – FORCE PROTECTION RISK PROCESS

Force Protection Risk Identification

309. In simple terms, force protection risk identification aims to recognise what could go wrong, and how. It should begin from the outset of campaign planning. Force protection risks are identified during hazard and threat assessment. J2 lead the threat assessment using all-source Intelligence covering threats and some hazards, particularly those that are exploitable by opponents (see JDP 2-00 *Intelligence*[3] for details). Information on other hazards is provided by command-led analysis[4] that supports operational planning and provides the Joint Force Commander (JFC) with his situational understanding (see JDP 5-00 for details).

310. **Joint Intelligence Preparation of the Environment**. Joint Intelligence Preparation of the Environment (JIPE) provides an understanding of the operating environment and highlights future requirements for information and intelligence. JIPE relies upon the constant interaction of J2, J3 and J5 staffs to ensure that the current and future activities of friendly, neutral and hostile actors are properly represented, allowing force protection staff to understand how they interface and interact. At the same time, details such as downwind traces from toxic industrial hazards and areas covered by weapon systems can be plotted, assisting in the selection of force protection measures. As an operation proceeds, information on threats is updated, but force protection staff in conjunction with J2 should update information on hazards. A recognised force protection picture will need to draw on medical, Environmental Health and Civil-Military Cooperation (CIMIC) expertise as well as the intelligence on opponents. Force protection staff should coordinate with J2 to ensure that the changing threats and hazards are continuously updated to inform the ongoing risk analysis and management process. Staff should also check that force protection requirements are included in the Intelligence Requirements Management and Collection Management processes.

311. **Commanders' Collective Risk**. Force protection is only one of a range of issues where the JFC and his staff will need to consider risk; other risk areas might include political, plans, command and control, logistics and

[3] Due to be promulgated late 2010.
[4] The understanding of the constituent elements of a situation, and their interrelationships, in order to obtain a thorough understanding of the past, present and anticipated future operational context. (JDP 01 (2nd Edition)).

information. Risk should be considered for all possible areas and the JFC must understand the cumulative and collective risks associated with the operation.

Force Protection Risk Analysis

312. Having identified force protection risks, the next stage is to analyse them. Risk analysis seeks to understand the likelihood of the activity or event occurring, the potential severity of the outcome, and to ascertain who owns each risk. While risks should be analysed individually, in the context of force protection it is essential to understand their collective impact across all levels of command. For instance, an activity may be deemed to have minimal impact at the tactical level but to have significant implications at the strategic level. Even though the likelihood of its occurrence may be small, measures of mitigation should be put in place. This is an ongoing process, subject to continued review and adaptation in response to the constantly changing situation.

313. **Likelihood and Impact of Risk**. Any potential risk should be assessed, in terms of its *likelihood* and its *impact*, using all available objective and subjective methods and techniques. The importance or weighting attributed to each risk assists the prioritisation of measures to mitigate or reduce their impact, and aids the development of potential exploitation options. When analysing force protection risks, particular consideration must be given to critical and vulnerable assets.

314. **Risk Matrix**. The risk of any single event occurring may be plotted on a matrix, an illustrative example of which is at Figure 3.1, showing likelihood versus impact. An activity or event may, for example, be classified as high likelihood of occurrence, and high impact – overall, a high risk score. To aid his subsequent management, a commander may draw his own risk tolerance line, to provide broad guidance rather than a prescriptive ‘rule’ to be followed. In particular, the acceptable threshold may need to be adjusted to the political situation or context.

Impact	Likelihood[5]					
	Unavoidable	Extremely Likely	Highly Probable	Probable	Possible	Unlikely
9 Operational Failure	10	10	9	9	8	7
8	10	9	9	8	7	6
7 Decisive Condition Prevented	9	9	8	7	6	5
6	9	8	7	6	5	4
5 Supporting Effect Fails	8	7	6	5	4	3
4	7	6	5	4	3	2
3 Joint or Component Activity Unsuccessful	6	5	4	3	2	1
2	5	4	3	2	1	1
1 Negligible	3	3	2	1	1	1

Risk Tolerance Line (an example)

Figure 3.1 – Risk Assessment Matrix

Force Protection Risk Management

315. Having identified and assessed likely risks, the commander and his staff should develop measures to reduce their likelihood and impact, mitigate unfavourable outcomes, and exploit opportunities that may arise. Operational risks should be prioritised, so that attention can be focused on mitigating the most severe first.

316. **Force Protection Risk Table**. One method of prioritising force protection risk is to produce a Force Protection Risk Table. The table comprises 5 steps that mirror the process outlined at Figure 1.1:

a. **Step 1 – Risk Identification**. This is derived through the estimate process and led by the J2/3/4/5/6 and J9 staff.

b. **Step 2 – Risk Analysis**. Each risk is analysed to consider likelihood of occurrence and potential impact in order to produce an overall risk rating using a risk matrix such as the example at Figure 3.1.

c. **Step 3 – Risk Management**. Consideration is then given to how each risk may be mitigated through use of proactive and reactive

[5] These titles are descriptive and represent relative likelihood.

measures. The risk is then further analysed to consider the likelihood of occurrence and impact after the mitigation measures have been applied (again using a risk matrix table), in order to determine the residual risk. Having calculated the residual risk, the commander can then determine whether he can terminate, treat (further), tolerate or transfer each risk.[6] Use of a simple colour code can focus attention on the most prominent risks.

d. **Step 4 – Implementation**. A force protection plan is produced and measures employed to counter and mitigate the risks identified in steps 1-3. Chapter 4 gives more details on the range of measures that can be applied and considerations in their employment.

e. **Step 5 – Review**. The process is continually reviewed.

An example of how a Force Protection Risk Table might be completed is at Figure 3.2.

[6] Definitions for terminating, treating, tolerating and transferring risks are provided in JDP 5-00 *Campaign Planning*.

Step 1 Identification[7]	Step 2 Analysis			Step 3 Management				Residual Risk[8]	Remarks
	Likelihood	Impact	Overall Risk[9]	Proactive Measures	Reactive Measures	Likelihood	Impact		
Ground Attack									
MANPADS versus aircraft	Possible	7	7	DAS, TESSERAL	Air TTP	Unlikely	5	3	
Indirect fire	Probable	3	3	Off base patrolling	PAR	Possible	3	2	
Air Attack									
Adversary Air Attack	Unlikely	6	4	AEW, CAP, COLPRO	DCA, PAR	Unlikely	4	2	
Adversary air versus Maritime	Unlikely	7	5	AEW, Maritime Surveillance	Mar Strike, TTPs	Unlikely	4	2	
Maritime Attack									
Adversary Naval attack	Possible	7	6	Organic surface AEW, Surface disposal	TTPs	Unlikely	3	1	
Mining	Probable	6	6	MCM detection, Int	MCM Ops	Possible	3	2	
Asymmetric Attack									
IED	Extremely likely	7	9	ECM, FPE, Exploitation	IEDD TF	Extremely likely	6	8	
CBRN									
Anthrax delivery	Possible	8	7	Vaccination	CBRN W&R	Possible	5	4	
Chemical	Unlikely	8	6	Int	CBRN W&R, IPE	Unlikely	3	1	
Hostile Electronic Warfare									
Surveillance	Extremely likely	2	4	Active & Passive electronic defence measures	Active & Passive electronic defence measures	Probable	2	2	
Jamming	Possible	3	2	As above	As above	Possible	1	1	
Hostile Intelligence Surveillance and Reconnaissance									
HUMINT	Unavoidable	3	6			Unavoidable	3	6	
Environmental									
Vector-borne disease	Unavoidable	3	6	Education, EH Checks	Segregation	Probable	2	2	
Road traffic accidents	Unavoidable	2	5	Education, TTPs		Probable	2	2	
Fratricide									
Blue-on-Blue ground	Possible	4	3	Battlefield Mgt		Possible	4	3	

Figure 3.2 – Exemplar Force Protection Risk Table

[7] Topics in the first column are exemplar. In practice the list will be derived from the detailed hazard and threat assessment led by J2.
[8] Calculated from the Risk Matrix Diagram at Figure 3.1 taking into account the measures determined at Step 3.
[9] Calculated from the Risk Matrix Diagram at Figure 2.1

Legend

AEW	Airborne Early Warning
CAP	Combat Air Patrol
CBRN W&R	Chemical, Biological, Radiological and Nuclear Warning and Reporting
COLPRO	Collective Protection
DAS	Defensive Air Suites
DCA	Defensive Counter Air
ECM	Electronic Counter Measures
EH	Environmental Health
FPE	Force Protection Engineering
HUMINT	Human Intelligence
IED	Improvised Explosive Device
IEDD TF	Improvised Explosive Device Disposal Task Force
Int	Intelligence
IPE	Individual Protective Equipment
MANPADS	Man Portable Air Defence System
MCM	Mine Counter Measures
Mgt	Management
Ops	Operations
PAR	Post Attack Recovery
TTP	Training, Techniques and Procedures

CHAPTER 4 – JOINT FORCE PROTECTION EXECUTION

SECTION I – FORCE PROTECTION CAPABILITIES AND MEASURES

401. The Force protection measures required by the Joint Force will be provided by a combination of dedicated force elements and adapted or *ad hoc* capabilities. These will evolve in response to the threats and hazards highlighted by the Joint Intelligence Preparation of the Environment (JIPE). Force protection capabilities can be applied at the theatre level, to installations or platforms and to individual personnel. The total capability against a particular threat or hazard is likely to comprise of a number of different measures applied at different levels. Measures such as Chemical, Biological, Radiological and Nuclear (CBRN) protection or Ground-based Air Defence are generally controlled at the theatre level. Installations, platform or individual measures may, or may not, require coordination at the theatre level depending on the level of operational risk presented by the threat or hazard.

Force Protection Measures

402. Force protection measures seek to prevent an opponent from attacking successfully (or minimising the effects of an attack or hazard) so as to enable the continued prosecution or resumption of operations with the minimum of degradation or delay. Force protection measures can be both proactive, in order to counter assessed threats and hazards, as well as reactive, in order to respond rapidly once a threat or hazard has occurred, to mitigate the effect of the incident. Proactive force protection measures are given the highest priority in order to shape the battlespace to best advantage. The effectiveness of any force protection measures will be diminished if Operations Security (OPSEC) regarding their nature and employment is not maintained.

403. Force protection measures can be further broken down into 3 main areas:

a. **Active**. Active measures are those measures necessary to deter, prevent, nullify or reduce the effectiveness of an enemy attack and to counter hazards. These measures are primarily proactive in nature where core functions are simplistically to find, fix, and strike at any threats and hazards before they effect operations, with the intention to exploit the situation further wherever possible.

b. **Passive**. Passive measures are those measures necessary to minimise the effects of enemy attack and hazards. These measures are employed proactively prior to any attack or hazard materialising. Passive measures can include:

(1) Physical protection, including Force Protection Engineering, platform hardening and individual protective equipment.

(2) Camouflage, concealment and deception.

(3) Dispersal and redundancy.

(4) Detection and warning systems.

(5) Electronic countermeasures.

(6) CBRN protective measures.

(7) Behavioural – the avoidance of establishing recognisable routines or patterns of activity.

c. **Recuperative**. Recuperative measures are necessary to recover from the effects of an enemy attack, restore essential services and, where appropriate, enable operations to continue with the minimum of disruption. Recuperative measures are therefore pre-planned responses that are reactively employed and may include activity such as:

(1) Fire fighting and rescue.

(2) Medical facilities.

(3) Explosive Ordnance Disposal (EOD) assets.[1]

(4) Repair and reconstitution facilities.

(5) Defensive lines to take/rebuttal.

[1] Explosive Ordnance Disposal (EOD) and Search also contribute to active measures.

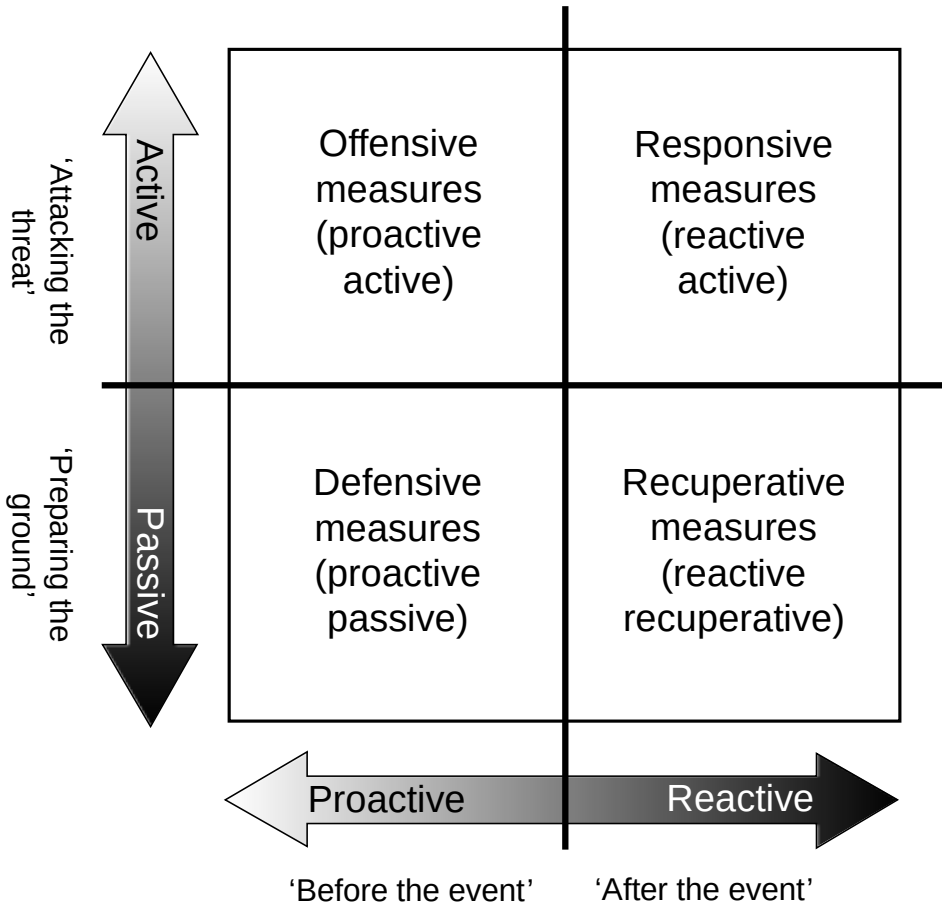

Figure 4.1 – Framework of Force Protection Measures[2]

Theatre-Level Measures

404. Theatre-level force protection capabilities are those which are either held at readiness (in the UK or forward as appropriate to the threat) to serve throughout the theatre of operations or, by their nature, have geographic reach across it. Some of the capabilities, such as Information Operations (Info Ops) or defensive counter-air, will be primarily focused on Joint action, but will still have a significant contribution to make to force protection. Liaison within the J3 and J5 staff to coordinate the use of these capabilities is essential. Many of the theatre-level capabilities could be of utility to the civilian or host nation population, or conversely the host nation may have equivalent capabilities which can be taken into account. Coordination between civilian and military authorities is particularly important in the face of an indiscriminate hazard or threat such as disease, ballistic missile attack or use of CBRN.

[2] Model developed by Land Warfare Centre.

Installation Measures

405. The installations necessary for the Joint Commander to fulfil the mission will vary widely depending on the length and type of operation and the existing infrastructure in theatre. Temporary positions occupied by manoeuvre forces in the course of their operations are outside the scope of Joint force protection. However, permanent or semi-permanent installations require protection measures coordinated at the operational level. These installations may include operating bases such as headquarters, sea ports of disembarkation, air ports of disembarkation and logistic bases. They also represent locations where the maritime, air and logistic components operate within the land environment. In these instances, the Joint Task Force Headquarters will need to issue clear direction to component commanders on force protection responsibilities as well as command and control arrangements.

406. A range of passive and recuperative measures can be incorporated into the site location, layout and construction of installations. This must be done on the basis of a comprehensive survey which considers the spectrum of hazards and threats which could potentially be brought to bear against the site. While there may be threats which are not yet employed by an adversary, but are within their capacity, consideration must be given to fitting the installation 'for, but not with' measures to counter them. Force Protection Engineering can be used to provide passive protection measures to both new and existing facilities, detailed guidance for which is provided in Joint Doctrine Publication 3-64.1 *Force Protection Engineering*.

407. In addition to Force Protection Engineering, a number of active measures, ranging from patrolling to defensive hard-kill systems, can be taken to reduce vulnerabilities. Where the installation is an operating base, such measures require careful battlespace management with wider operations (potentially in all environments). The coordination issues in time and space around a large operating base must be addressed early in the campaign plan and kept under review as the contents, purpose and protection requirements of the installation evolve with time and the changing threat.

Platform Measures

408. Fundamental to the force protection of platforms are the survivability measures built into the ships, aircraft and vehicles from the design stage. While modification of these measures may be necessary through-life, basic capabilities, such as Collective Protection (COLPRO) against CBRN threats, are extremely costly to fit retrospectively. Less radical modifications or additional bolt-on equipment may be cost-effective and can provide specific counter-threat capabilities in particular theatres. As discussed in Chapter 3, where such threats constitute a risk at the operational level, the coordination of such measures becomes an issue for the Joint force protection staff.

Individual Measures

409. The concept of individual survivability is very similar to that for platforms. With individuals, the political and moral imperative to ensure that every practicable measure has been taken is acute. This will include, where appropriate, the provision of personal protective equipment. A significant factor in individual survivability is the mitigation provided by the medical services, with the provision of timely medical evacuation being of particular importance. While this is outside the remit of the force protection staff, medical coverage must be factored into the overall risk assessment process.

Force Health Protection

410. The medical services underpin the response to every hazard or threat. The political impact of casualties and fatalities will vary according to the context of the operation, but for both humanitarian and political reasons, achieving the best possible treatment of casualties is an enduring responsibility of the commander and one which plays a key role in protecting the moral component of fighting power. Although ‘scaleable’ in line with the overall operation, the medical capability in a particular theatre has a finite capacity and flow-rate determined by a complex interaction of clinical and logistical factors. If saturated, it could become a constraint on the commander’s freedom of action. Health protection measures aimed at preventing disease and non-battle injury can have a disproportionate effect in reducing casualties from these causes which might otherwise reduce the availability of medical resources for battle casualties. Medical counter measures can also mitigate the threat posed in a CBRN threat environment.

Exploitation

411. Information and intelligence from attempted or successful attacks on the Joint force is collected as part of Material and Personnel Exploitation (MPE). MPE is '*the systematic collection, information processing and dissemination of intelligence obtained as a result of tactical questioning, interrogation and the extraction of data from recovered materiel*'.[3] It is a responsive process which aims to maximise the intelligence value of captured or detained personnel and recovered materiel. Material collected from incidents is analysed using forensic techniques in theatre or via reachback to the UK and can determine the construction, method of operation and possible origin of the components of devices[4] used to attack the Joint force. MPE is of particular importance in countering irregular forces. Force protection measures against such forces should be implemented with a view to exploiting any attempt to attack the Joint Force. MPE is coordinated at the theatre level.

Joint Personnel Recovery

412. Joint Personnel Recovery (JPR) is a recuperative measure, controlled at theatre level, which seeks to reduce the risk of personnel being captured, killed or taken hostage following the loss of an aircraft or compromise of a mission in enemy-held territory. It has a wider utility in protecting the moral component of fighting power throughout the force. JPR is covered in detail in Joint Warfare Publication (JWP) 3-66 *Joint Personnel Recovery*,[5] which notes that JPR includes both individual Training, Technique and Procedures (TTPs) carried out by Survival, Evasion, Resistance and Extraction (SERE) trained individuals and a number of active capabilities, including combat rescue,[6] not all of which may be provided by the UK.

[3] Joint Doctrine Note (JDN) 02/09 *Material and Personnel Exploitation*.
[4] These are not limited to Improvised Explosive Devices, but include improvised Indirect Fire weapons and Chemical, Biological and Radiological devices.
[5] Currently under review by PJHQ.
[6] Tactical level doctrine is under development by the Joint Helicopter Command, Air Warfare Centre and Joint Force Air Component Commander.

SECTION II – HAZARDS, THREATS AND COUNTER MEASURES

413. The tables in the following pages, which are neither exclusive nor exhaustive, show a range of capabilities that could be employed against the spectrum of hazards and threats. As shown in the example below, the measures taken against a particular threat or hazard, such as Air Attack, can be considered as the total of the theatre-level, installation, platform and individual capabilities shown on the row for that threat. Any of these could potentially be an issue for coordination at the operational level if the risk that they present is operationally or strategically significant.

Measures controlled at theatre level

Measures may need to be coordinated at theatre level

Threat	Theatre Measures	Installation Measures	Platform Measures	Individual Measures
Air Attack	Control of Air Ops Integrated Air Defence System	GBAD / AAW FPE Sense and Warn CCD	GBAD / AAW CCD	All Arms Air Defence IPE

Threat

Sum of measures comprises ‘counter threat’ capability

AAW	Anti-Air Warfare
CCD	Camouflage Concealment and Deception
FPE	Force Protection Engineering
GBAD	Ground-based Air Defence
IPE	Individual Protective Equipment

Figure 4.2 – Example of Force Protection Measures Brigaded Against a Threat

FORCE PROTECTION EXECUTION

Note: All hazards and threats which may result in casualties are mitigated by the appropriate theatre, installation, platform and individual medical measures described in JDP 4-03 *Medical Support to Joint Operations*. For reasons of brevity, these are therefore not included in the table.

Potential Hazards and Threats[7]	Theatre Measures	Installation Measures	Platform Measures	Individual Measures	Remarks/References
Hazards					
Altitude	Pre-Deployment Training (PDT) Reception Staging Onward Movement and Integration (RSOI) briefing	Site location	Platform selection modifications	Acclimatisation Fitness Training Tactics & Procedures (TTPs)	JDP 3-64.1 *Force Protection Engineering* Consider effect of altitude on equipment performance and endurance (J4 liaison)
Climate	PDT RSOI briefing	Site location Climate Control	Platform selection Climate Control	Acclimatisation Fitness TTPs Hydration Rations/Clothing	JDP 3-64.1 Consider effect of climate on equipment serviceability (J4 liaison)
Cultural	PDT RSOI briefing Key Leadership Engagement (KLE) Political Adviser (POLAD)	Local KLE		Training	JDN 1/09 *The Significance of Culture to the Military* JWP 3-80 *Information Operations* Info Ops required to allay

[7] Listed in alphabetical order and not intended to be exhaustive.

Potential Hazards and Threats[7]	Theatre Measures	Installation Measures	Platform Measures	Individual Measures	Remarks/References
	Info Ops				fears/counter rumours and as a reactive measure in the event of an incident with cultural dimensions.
Disease	PDT RSOI briefing Force Protection Health measures Theatre wide surveillance	Site location Environmental Health measures	Hygiene checks	Hygiene measures Acclimatisation Fitness TTPs	JDP 4-03.1 *Clinical Guidelines for Operations* 2009DIN03-004 *Management of Environmental and Industrial Hazards on Operations* Disease prevention and surveillance measures will also mitigate the effect of biological weapons threat.
Fire	PDT RSOI briefing	Site layout Fire Prevention Plan/Orders Fire Services	Fire Prevention Orders and equipment	Training TTPs Clothing	Joint Service Publication (JSP) 426 *MOD Fire Safety Policy* Joint Warfare Publication (JWP) 4-05 *Infrastructure Management* JDP 3-64.1
Fratricide	Battlespace Management Information operations	Battlespace Management Combat	Combat ID Protected Mobility	Training TTPs Individual	JDP 3-62 *Combat Identification* JDP 3-70 *Battlespace*

Potential Hazards and Threats[7]	Theatre Measures	Installation Measures	Platform Measures	Individual Measures	Remarks/References
		Identification (ID) Force Protection Engineering (FPE)		Protective Equipment (IPE)	*Management* Information operations may be required in the event of a fratricide incident occurring to mitigate the effect at the strategic level.
Toxic Industrial Materials (TIM)	Joint Intelligence Preparation of the Environment (JIPE) Survey Secure TIM sites Medical Knowledge Management Warning and Reporting	Knowledge of local TIMs COLPRO (Collective Protection) available Knowledge Management Detection Warning and Reporting Medical	Hazard avoidance COLPRO Detection	Detection IPE TTPs Training	2009DIN03-004 *Management of Environmental and Industrial Hazards on Operations* See also Chemical Biological and Radiological and Nuclear (CBRN) references below
Unexploded Ordnance	PDT RSOI briefing JIPE Explosive Ordnance Disposal (EOD) Specialist Staff and Teams	Local Survey EOD Teams	Protected Mobility	Training TTPs IPE	JDP 2/02 *Joint Service EOD* JDN/ 1/04 *Joint Search* JSP 364 *Joint Service EOD Manual.* Liaison required with J3 or J9 CIMIC teams and NGOs.

Potential Hazards and Threats[7]	Theatre Measures	Installation Measures	Platform Measures	Individual Measures	Remarks/References
Non Battle Injuries (inc Road Traffic Accidents) and Occupational Health	PDT RSOI briefing	Awareness Orders	Safety Equipment	Work/Rest cycles Training TTPs Protective equipment Stress Management	JDP 4-03.1 JSP 375 *MOD Health and Safety Handbook*
Threats					
Air Attack (including Unmanned Combat Aerial Vehicles)	Control of Air Ops Integrated Air Defence System (IADS)	Ground-based Air Defence (GBAD) FPE Sense and Warn Camouflage, Concealment and Deception (CCD)	GBAD/Anti Air Warfare CCD (including signature control)	All Arms Air Defence (AAAD) IPE	AJP-3.3.1(A) *Counter Air Operations* JDP 3-63 *Joint Air Defence* JDP 3-63.1 *GBAD* JDP 3-64.1 JDP 3-70
CBRN	JIPE CBRN Specialist staff Knowledge Management Detection Medical counter-measures Sampling and Identification of Biological, Chemical and Radioactive Agents	CBRN specialist staff Fixed detectors COLPRO Decontamination	CBRN specialist staff Platform detectors Platform COLPRO Decontamination	Medical counter-measures Training TTPs IPE Decontamination	AJP-3.8 *CBRN Defence* AJP-3.8.1 Series Vols 1-3. JDP 3-61.1 Joint *CBRN Defence* Allied Tactical Publication (ATP)-65 *The Effect of Wearing CBRN IPE on Operations*. ATP-70 *CBRN COLPRO*

Potential Hazards and Threats[7]	Theatre Measures	Installation Measures	Platform Measures	Individual Measures	Remarks/References
	(SIBCRA)				
Criminality	JIPE KLE Custody/detention agreement Specialist Teams	Physical security Personnel security Access control	Physical security	Training TTPs	JSP 440 *Defence Manual of Security* JDP 1-10.3 *Detainees* JDP 3-40 *Security and Stabilisation: The Military Contribution*
Electronic Warfare (EW) including Computer Network Attack (CNA)	Information assurance Access to expertise Resilience/redundancy	Design and layout Resilience/ redundancy	Signature control TEMPEST	Training TTPs	JDP 6-00 *CIS Support to Joint Ops* JSP 440
Improvised Explosive Devices (IEDs) and Mines[8]	Counter-IED Strategy: • Attack the Network • Defeat the Device • Prepare the Force Theatre Exploitation facilities Counter-IED specialists PDT RSOI briefing JIPE	Electronic Counter Measures (ECM) Patrolling Military working dogs	Protected Mobility ECM	Training TTPs IPE ECM	AJP-3.15 *Allied Joint Doctrine for C-IEDs* JDP 3-64.1 JDN/ 1/04 *Joint Search* JSP 364 Land Warfare Centre Doc Note 09/04 *C-IED Activity at Formation and BG Level*

[8] These measures consider the use of mines by an irregular force which are countered and mitigated in the same way as IEDs. Conventional mine fields would either be marked and avoided, or breached as a deliberate operation and thus fall outside the scope of force protection.

Potential Hazards and Threats[7]	Theatre Measures	Installation Measures	Platform Measures	Individual Measures	Remarks/References
Indirect Fire	Theatre Exploitation facilities	Sense & Warn Intercept/GBAD FPE Patrolling Counter-fire	CCD	Training TTPs IPE Entrenchment	JDP 3-64.1 JDP 3-70
Influence	KLE Information Operations			Internal communication	JWP 3-80 *Information Operations* JWP 3-45.1 *Media Operations*
Intelligence Surveillance and Reconnaissance (ISR) (including UAVs)	Deception Counter-intelligence RSOI OPSEC	Layout Camouflage & Concealment Security	Camouflage & Concealment	Training TTPs	AJP-2 *Allied Joint Intelligence, Counter Intelligence & Security Procedures* AJP-2.2 *Counter Intelligence & Security Procedures* JDP 2-00 *Intelligence* JDN 2/06 *Countering the Threat of UAVs*
Man portable Air Defence Systems (MANPADS) and Surface to Air Fire (SAFIRE) – adversary	JIPE	JIPE Ground Defence Area (GDA) Patrolling (APOD – TESSARAL &	Defensive Aid Suite (DAS) TTPs		AP3241 *RAF Force Protection Doctrine for Air Operations*

Potential Hazards and Threats[7]	Theatre Measures	Installation Measures	Platform Measures	Individual Measures	Remarks/References
employment against friendly air.		SAFIRE)			
Maritime attack[9]	Sea control/denial operations	Maritime patrol Mining Booms	Maritime Warfare and Damage Control MAPLE matrix	TTPs	AJP-3.1 *Allied Joint Maritime Operations* ATP-1D *Allied Maritime Tactical Instructions and Procedures* ATP-74 *Allied Maritime FP against Asymmetric Threats in Harbour & Anchorage.* BR 8988 *RN Manual of Military Training, Operations and Tactics*
Media[10]	Communication strategy Media engagement	Media handling arrangements		Training Internal communication	JDP 3-45.1
Maritime Mines	Sea control/denial operations	Maritime patrol Counter mining	Damage control	TTPs	CB 8557 series *Mine Countermeasures*

[9] A Maritime Attack on the Joint Force while embarked is considered to be Maritime Warfare rather than Force Protection and is covered by single-Service doctrine. Air Attack or Indirect Fire on a target in the Land environment originating from a maritime platform could be countered by sea control or denial operations but would be countered in the same way as that from other sources. This entry thus refers to measures to counter and mitigate the threat to ships alongside or land installations from a maritime force.

[10] This entry considers the threat to reputation and Operational Security by friendly or neutral media who may be reporting on the activities of the Joint Force. Measures to counter the effect of influence by the adversary are covered under Influence earlier in the table.

Potential Hazards and Threats[7]	Theatre Measures	Installation Measures	Platform Measures	Individual Measures	Remarks/References
	ISTAR Specialist MCM platforms	Booms			*Techniques*
Sabotage/Subversion	JIPE	Physical security Personnel security Access control Layout and resilience	Physical security	Training TTPs	JDP 3-64.1 JSP 440
Theatre Ballistic Missiles[11]	Theatre Ballistic Missile Defence (TBMD) Warning & Reporting	TBMD FPE	Maritime BMD Camouflage & Concealment	Entrenchment	JDP 3-63 *Joint Air Defence* JDP 3-70 JDP 3-64.1 CBRN protection measures may also apply depending on the threat.

[11] The UK has no Ballistic Missile Defence capability at present. Liaison will be required with alliance and coalition partners.

(INTENTIONALLY BLANK)

LEXICON

This Lexicon contains acronyms/abbreviations and terms/definitions used in this publication. Many of the terms and their definitions detailed in Part 2 are either *new* or *modified* following a recent review of this and other Capstone/Keystone doctrine.[1] The source of each term is shown in parenthesis. For fuller reference on all other UK and NATO agreed terminology, see the current edition of Joint Doctrine Publication (JDP) 0-01.1 *The UK Glossary of Joint and Multinational Terms and Definitions*.

PART 1 - ACRONYMS AND ABBREVIATIONS

AAAD	All Arms Air Defence
ADP	Army Doctrine Publication
AEW	Airborne Early Warning
APOD	Air Port of Disembarkation
AJP	Allied Joint Publication
BDD	British Defence Doctrine
BMD	Ballistic Missile Defence
CAP	Combat Air Patrol
CASEVAC	Casualty Evacuation
CBRN	Chemical, Biological, Radiological and Nuclear
CCD	Camouflage, Concealment and Deception
CDS	Chief of the Defence Staff
CIMIC	Civil-Military Cooperation
Combat ID	Combat Identification
C-IED	Counter Improvised Explosive Device
CIS	Communications and Information Systems
CJO	Chief of Joint Operations
CJTF	Combined Joint Task Force
CJTFC	Combined Joint Task Force Commander
COLPRO	Collective Protection
COMBRITFOR	Commander British Forces
CONOPS	Concept of Operations
CONPLAN	Contingency Plan
CNA	Computer Network Attack
CND	Computer Network Defence
CNO	Computer Network Operations

[1] This Lexicon also includes new/modified Terms/Definitions and Acronyms/Abbreviations extracted from JDPs 01 (2nd Edition) *Campaigning* and 5-00 (2nd Edition) *Campaign Planning*.

DAS	Defensive Aid Suite
DCA	Defensive Counter Air
DCDC	Development, Concepts and Doctrine Centre
DCDS (Ops)	Deputy Chief of the Defence Staff (Operations)
DCMO	Defence Crisis Management Organisation
DEW	Directed Energy Weapons
ECM	Electronic Counter Measures
EMS	Electromagnetic Spectrum
EOD	Explosive Ordnance Disposal
FPE	Force Protection Engineering
GBAD	Ground Based Air Defence
GDA	Ground Defence Area
HUMINT	Human Intelligence
IADS	Integrated Air Defence System
IED	Improvised Explosive Device
IEDD TF	Improvised Explosive Device Task Force
Info Ops	Information Operations
IPE	Individual Protective Equipment (by common usage, against CBRN threats and hazards)
ISR	Intelligence, Surveillance and Reconnaissance
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
JDP	Joint Doctrine Publication
JDN	Joint Doctrine Note
JFACC	Joint Force Air Component Commander
JFC	Joint Force Commander
JFHQ	Joint Force Headquarters
JFLogC	Joint Force Logistic Component
JIPE	Joint Intelligence Preparation of the Environment
JOA	Joint Operations Area
JPR	Joint Personnel Recovery
JTF	Joint Task Force
JTFC	Joint Task Force Commander
JTFHQ	Joint Task Force Headquarters
JWP	Joint Warfare Publication
KLE	Key Leadership Engagement

MANPADS	Man Portable Air Defence System
MASD	Military Assistance to Stabilisation and Development
MCM	Mine Counter Measures
MPE	Materiel and Personnel Exploitation
NCC	National Contingent Commander
NGO	Non-governmental Organisation
OGD	Other Government Department
OPSEC	Operations Security
PAR	Post Attack Recovery
PDT	Pre-Deployment Training
PJHQ	Permanent Joint Headquarters
PMSC	Private Military and Security Company
POLAD	Political Adviser
PPE	Personal Protective Equipment (by common usage, against kinetic or ballistic threats or hazards)
RFI	Request for Information
ROE	Rules of Engagement
RO-RO	Roll On, Roll Off shipping
RSOI	Reception, Staging, Onward Movement and Integration
RTA	Road Traffic Accident
SofS	Secretary of State
SERE	Survival, Evasion, Resistance and Extraction
SF	Special Forces
SIBCRA	Sampling and Identification of Biological, Chemical and Radioactive Agents
SOFA	Status of Forces Agreement
TBMD	Theatre Ballistic Missile Defence
TIM	Toxic Industrial Material
TMD	Theatre Missile Defence
TTPs	Training, Techniques and Procedures
UAV	Unmanned Aerial Vehicle

(INTENTIONALLY BLANK)

PART 2 – TERMS AND DEFINITIONS

Analysis
The examination of all the constituent elements of a situation, and their inter-relationships, in order to obtain a thorough understanding of the past, present and anticipated future operational context. (JDP 01 2nd Edition)

Analysis
In intelligence usage, a step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation. (AAP-6)

Anti-submarine Warfare
Operations conducted with the intention of denying the enemy the effective use of his submarines. (AAP-6)

Area of Operations
A geographical area, defined by a Joint Force Commander within his Joint Operations Area, in which a commander designated by him (usually a component commander) is delegated authority to conduct operations. *See also Joint Operations Area*. (JDP 01 2nd Edition)

Asymmetric Threat
A threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain a disproportionate result. (AAP-6)

Assessment
The evaluation of progress, based on levels of subjective and objective measurement in order to inform decision-making. (JDP 01 2nd Edition)

Battlespace
All aspects of a Joint Operations Area within which military activities take place subject to Battlespace Management. *See also Battlespace Management and Joint Operations Area*. (JDP 01 2nd Edition)

Battlespace Management
The adaptive means and measures that enable the dynamic synchronisation of activity.
(JDP 3-70)

Ballistic Missile
A missile which does not rely upon aerodynamic surfaces to produce lift and consequently follows a ballistic trajectory when thrust is terminated. (AAP-6)

Campaign
A set of military operations planned and conducted to achieve strategic objectives within a Theatre of Operations or Joint Operations Area, which normally involves joint forces. (JDP 01 2nd Edition)

Campaign Design
Campaign Design develops and refines the commander's (and staff's) ideas to provide detailed, executable and successful plans. (JDP 01 2nd Edition)

Campaign Plan
A campaign plan is the actionable expression of a Joint Force Commander's intent, articulated to subordinate commanders through plans, directives and orders.
(JDP 5-00 2nd Edition)

Civil-Military Cooperation
The process whereby the relationship between military and civilian sectors is addressed, with the aim of enabling a more coherent military contribution to the achievement of UK and/or international objectives. (JDP0-01.1)

Coalition
An *ad hoc* arrangement between 2 or more nations for common action.
(JDP 0-01.1)

Collective Chemical, Biological, Radiological and Nuclear Protection (COLPRO)
Protection provided to a group of individuals in a chemical, biological, radiological and nuclear environment, which permits relaxation of individual chemical, biological, radiological and nuclear protection.

Combat Identification
The process of combining situational awareness, target identification, specific tactics, training and procedures to increase operational effectiveness of weapon systems and reduce the incidence of casualties caused by friendly fire. (JDP 0-01.1)

Command
The authority vested in an individual to influence events and to order subordinates to implement decisions.
Note: It comprises 3 closely inter-related elements: leadership, decision-making (including risk assessment) and control. (BDD 3rd Edition)

Components
Force elements grouped under one or more component commanders subordinate to the operational level commander. (JDP 0-01.1)

Comprehensive Approach
Commonly understood principles and collaborative processes that enhance the likelihood of favourable and enduring outcomes within a particular situation.
(BDD 3rd Edition)

Computer Network Operations
Actions to attack, exploit and defend friendly and adversary computers, computer networks and any other information system and the software and data resident on them. Computer Network Operations encompass Computer Network Attack, Computer Network Defence and Computer Network Exploitation. (UK under development)

Contingents
Force elements of one nation grouped under one or more multinational component commanders subordinate to the Joint Task Force Commander. (JDP 0-01.1)

Contingency Plan
A plan which is developed for possible operations where the planning factors have identified or can be assumed. This plan is produced in as much detail as possible, including the resources needed and deployment options, as a basis for subsequent planning. (AAP-6)

Contingency Planning
Planning, in advance, for potential military activity in the future.
(JDP 5-00 2nd Edition)

Control
The coordination of activity, through processes and structures that enable a commander to manage risk and to deliver intent. (BDD 3rd Edition)

Counter-fires
Fire intended to counter or neutralise enemy weapons. (AAP-6)

Counter-Improvised Explosive Device
The collective efforts at all levels to defeat the IED system by attacking the networks, defeating the device and preparing the force to reduce or mitigate the effects of all forms of IEDs in use against friendly forces and non-combatants. (AJP-3.15 Edition 2 SD1)

Crisis Management
The process of preventing, containing or resolving crises before they develop into armed conflict, while simultaneously planning for possible escalation.
(BDD 3rd Edition)

Crisis Response Planning
Planning, often at short notice, to determine an appropriate military response to a current or imminent crisis. (JDP 5-00 2nd Edition)

Cyberspace
A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. (UK under development)

Decisive Condition
A specific combination of circumstances deemed necessary to achieve a campaign objective. (JDP 01 2nd Edition)

Directive
A military communication in which policy is established or a specific action is ordered. (AAP-6)

Electromagnetic Pulse
A short intense discharge of long-wavelength radio frequency electromagnetic energy produced by a nuclear detonation or other non-nuclear means. The resulting electric and magnetic fields may interact with electrical and electronic systems to produce damaging current and voltage surges. (AAP-21)

Electronic Counter Measures
That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum through the use of electromagnetic energy. There are 3 subdivisions of electronic counter-measures: electronic jamming, electronic deception and electronic neutralisation. (AAP-6)

Exploitation
Taking full advantage of any information that has come to hand for tactical or strategic purposes. (AAP-6)

Fires
The deliberate use of physical means to support the realisation of, primarily, physical effects. (BDD 3rd Edition)

Force Protection
The coordinated measures by which threats and hazards to the Joint Force are countered and mitigated in order to maintain an operating environment that enables the Joint Commander the freedom to employ Joint Action. (JDP 3-64)

Improvised Explosive Device
A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores, but is normally devised from non-military components. (AAP-6)

Influence Activities
The capability, or perceived capacity, to affect the character or behaviour of someone or something. (BDD 3rd Edition)

Intelligence, Surveillance, Target Acquisition and Reconnaissance
The prioritised integration, coordination and synchronisation of collection capabilities and activities to acquire and disseminate information and intelligence, as part of the intelligence cycle, in direct support of operations. (JDP 3-00 3rd Edition)

Joint
Adjective used to describe activities, operations and organisations in which elements of at least two Services participate. (AAP-6)

Joint Action
The deliberate use and orchestration of military capabilities and activities to realise effects on other actors' will, understanding and capability, and the cohesion between them. (JDP 01 2nd Edition)
Note: It is implemented through the coordination and synchronisation of Fires, Influence Activities and Manoeuvre.

Joint Commander
The Joint Commander, appointed by CDS, exercises the highest level of operational command of forces assigned with specific responsibility for deployments, sustainment and recovery. (JDP 0-01.1)

Joint Force
A force composed of significant elements of 2 or more Services operating under a single commander authorised to exercise operational command or control. (JDP 0-01.1)

Joint Force Commander
A general term applied to a commander authorised to exercise operational command or control over a Joint force. (JDP 0-01.1)

Joint Operations Area
An area of land, sea and airspace defined by a higher authority, in which a designated Joint Task Force Commander plans and conducts military operations to accomplish a specific mission. A Joint Operations Area including its defining parameters, such as time, scope and geographic area, is contingency/mission specific. (JDP 0-01.1)

Manoeuvre
Coordinated activities necessary to gain advantage within a situation in time and space. (BDD 3rd Edition)

Manoeuvrist Approach
An approach to operations in which shattering the enemy's overall cohesion and will to fight is paramount. It calls for an attitude of mind in which doing the unexpected, using initiative and seeking originality is combined with a ruthless determination to succeed. (JDP 0-01.1)

Military Risk
The probability and implications if an event of potentially substantive positive or negative consequences taking place. (JDP 01 2nd Edition)

Multi-agency
Activities or operations in which multiple agencies, including national, international and non-state organisations and other actors, participate in the same or overlapping areas with varying degrees of inter-agency cooperation. (JDP 01 2nd Edition)

Multinational
Adjective used to describe activities, operations and organisations, in which forces or agencies of more than one nation participate. *See also Joint*. (JDP 0-01.1)

Non-Governmental Organisation
A voluntary, non-profit making organisation that is generally independent of government, international organisations or commercial interests. The organisation will write its own charter and mission. (JDP 0-01.1)

Offensive Counter-Air Operations
An operation mounted to destroy, disrupt or limit enemy air power as close to its source as possible. (AAP-6)

Operational Art
The orchestration of a campaign, in concert with other agencies, involved in converting strategic objectives into tactical activity in order to achieve a desired outcome. (JDP 01 2nd Edition)

Operational Level
The level of warfare at which campaigns are planned, conducted and sustained to accomplish strategic objectives and synchronise action, within theatres or areas of operation. (BDD 3rd Edition)

Operation Order
A directive, usually formal, issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. (AAP-6)

Operation Plan
A plan for a single or series of connected operations to be carried out simultaneously or in succession. It is usually based upon stated assumptions and is the form of directive employed by higher authority to permit subordinate commanders to prepare supporting plans and orders. The designation 'plan' is usually used instead of 'order' in preparing for operations well in advance. An operation plan may be put into effect at a prescribed time, or on signal, and then becomes the operation order. (AAP-6)

Operations Security
The discipline which gives a military operation or exercise appropriate security, using active or passive means, to deny a target decision-maker knowledge of essential elements of friendly information. (JDP 3-80.1)

Protective Security
The organised system of defensive measures instituted and maintained at all levels of command with the aim of achieving and maintaining security. (AAP-6)

Security
The condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorised disclosure. (AAP-6)

Security is the provision and maintenance of an operating environment that affords the necessary freedom of action, when and where required, to achieve objectives. (JDP 0-01)

Supporting Effect
The intended consequence of actions. (JDP 01 2nd Edition)

Theatre Missile
Ballistic, cruise and air-to-surface missiles whose targets are within a given theatre of operations, with a range of a few hundred to several thousand miles. (JDP 0-01.1)

Theatre of Operations
A geographical area, or more precisely a space, defined by the military-strategic authority, which includes and surrounds the area delegated to a Joint Force Commander (termed the Joint Operations Area), within which he conducts operations. (JDP 01 2nd Edition)

Toxic Industrial Hazards
The hazard resulting from the release by any means of toxic industrial material resulting in the contamination or irradiation of personnel or the environment, area or any particular object.

Toxic Industrial Material
A generic term for toxic or radioactive substances in solid, liquid, aerosolized or gaseous form. These may be used, or stored for use, for industrial, commercial, medical, military or domestic purposes. Toxic Industrial Material (TIM) may be chemical, biological or radioactive and described as toxic industrial chemical, toxic industrial biological or Toxic Industrial Radiological.