ASYMMETRIC THREATS
TO BRITISH MILITARY INTERVENTION OPERATIONS

Squadron Leader Nicholas J. Newman MPhil RAF
Darwin College

A dissertation submitted to the Board of Graduate Studies in part
fulfilment of the requirements for the Degree of Master of Philosophy
in International Relations at the University of Cambridge

July 1999
# TABLE OF CONTENTS

**LIST OF TABLES** \(v\)

**LIST OF FIGURES** \(v\)

**PREFACE** vi

**GLOSSARY** viii

**INTRODUCTION** 1

## PART I

**CHAPTER I:**

**ASYMMETRIC CHALLENGES TO MILITARY INTERVENTION** 6

- **The Changing Nature of Conflict** 6
  - Defining Asymmetric Threats 6
- **Future Military Intervention** 7
  - Instability, Intervention and International Law 7
  - Political Decision-making 9
  - The Pitfalls of Military Intervention 9
- **British Vulnerability** 10
  - Unilateral Intervention 11
  - Coalition Partner 11
  - Coalition Leader 12

**CHAPTER II:**

**MEANS, MOTIVE AND OPPORTUNITY** 13

- **Means** 13
  - Military Approaches 13
  - Technological Approaches 14
  - Unconventional Approaches 14
- **Motives** 15
Opportunities

- Alliance and Coalition Fragility
- Domestic Sensitivities
- Reliance on Scarce, High-Value Assets
- Vulnerability of ‘First-Echelon’ Forces
- Host-Nation Constraints
- Information Dependence
- Accessibility of National Strategic Infrastructure

PART II

CHAPTER III: MILITARY ASYMMETRIC CHALLENGES

- Weapons of Mass Destruction
  - Introduction
  - Nuclear Weapons
  - Chemical Weapons
  - Biological Weapons
- Ballistic Missiles
- The Revolution in Military Affairs
  - Cruise Missiles
  - Sub-Surface Weapons
- Clandestine Operations

CHAPTER IV: NON-MILITARY ASYMMETRIC CHALLENGES

- Technological Approaches
  - Strategic Information Warfare
  - Military C4ISR Systems
  - National Strategic Infrastructure
- Unconventional Approaches
  - Atrocities
  - State-Sponsored Terrorism
PART III

CHAPTER V: RISK ANALYSIS  45

Introduction  45
Deterrence  45
Disruption  46
Exhaustion/Attrition  48
Coercion  49
Summary  51

CHAPTER VI: COUNTERMEASURES  53

Introduction  53
Deterrence  53
Threat Management (Pre-emption)  54
Defence  55
  Active Defence (Prevention)  55
  Passive Defence (Protection)  58

CONCLUSION  59

BIBLIOGRAPHY  64
LIST OF TABLES

Table 1: Iraq’s Unaccounted Biological Warfare Agents (1999). 24
Table 2: Ballistic Missile Proliferation. 26
Table 4: Information Warfare Techniques. 34
Table 5: ‘Home-Made Explosive’ Attacks (1990-1997). 43
Table 6: Chronology of Terrorist Attacks Against US Embassies and Bases Overseas. 44

LIST OF FIGURES

Figure 1: Conflict Asymmetries. 3
Figure 2: Asymmetric Approaches and Means. 15
Figure 3: Political and Military Vulnerabilities. 17
Figure 4: Twentieth Century ‘Revolutions in Military Affairs’. 28
Figure 5: Notional Threat Stand-off Footprints. 32
Figure 6: Terrorism Statistics (1983-1997). 41
Figure 7: Asymmetric Approaches: Motives and Means. 52
PREFACE

This work is dedicated to Tracy, for her support and forbearance; Alexander, whose three year-old antics have provided a remarkable insight into the mind of the international terrorist; and Francesca, for reassuring me that not all children are terrorists!

In addition to expressing my appreciation to the Royal Air Force for granting me this wonderful opportunity to study at the University of Cambridge and, in particular, to the Director Defence Studies (RAF) and his staff for their professional support, I would like to thank a number of individuals for their inspiration and guidance. My interest in asymmetric approaches to warfare was inspired by David Shlapak and Alan Vick's RAND paper on the evolving ground threats to USAF bases, and then excited by Colonel Lawrence Lane's account of the investigation into the 1996 terrorist bombing of the Khobar Towers USAF accommodation complex in Dhahran, Saudi Arabia. Finally, the issues were placed in context for me by Peter Wilson’s paper on ‘Asymmetric Threats’ in the USNDU 1998 Strategic Assessment. Therefore, I am extremely grateful to David, Alan and Peter for taking the time to see me at RAND, and to Colonel Lane for permitting me to visit the Headquarters of the USAF Air Mobility Command Security Forces Directorate. My gratitude is due to far more people than I am able to mention individually here; however, all are named in the bibliography - including those whose remarks are not specifically cited, but whose comments were invaluable in informing my broader understanding of the issues concerned. Nevertheless, I must single out the following for particular acknowledgement:

- At the Pentagon, Brigadier General Coleman (Director of USAF Security Forces) for his insights on emerging threats to USAF operations; and Colonel Steven Loving, US Army (Chief of Strategic Planning, Concepts and Doctrine Division) for providing me with the Selected Readings on Asymmetric Approaches to Warfare from the Joint Chiefs of Staff 1999 Strategy Review.
- At RAND’s Washington Office, Dr Bruce Hoffman (Director) for his hospitality, and for permitting me to discuss this topic with his senior researchers.
- At the US Center for Strategic and International Studies, Daniel Gouré for his inspired observations and Colonel Pete Johnson USAF, for co-ordinating my visit.
- At the US Army War College, Lieutenant Colonel Scott Heintz for providing me with the anthology of the College’s 1998 ‘Annual Strategy Conference’ concerning asymmetric challenges to the US.
- At Headquarters USAF Air Mobility Command, Scott Air Force Base, Colonel Daniel Matarazzo (Deputy Director) and the staff of the Security Forces Directorate for their comprehensive briefings on emerging USAF ‘Force Protection’ doctrine.

I am most grateful to Group Captain David Bremner for supporting my initial application and for assisting and encouraging me throughout my studies, and to those other colleagues and friends who read the paper and offered so many comments and suggestions; in particular, Group Captain Andrew Thomson, Major Tony Bettaney and Major Patricia Bettaney. Finally, I would like to thank Dr. Philip Towle for his supervision and guidance in the preparation of this dissertation.
Whilst this thesis would not have been possible without the inputs already mentioned and many others, I alone am responsible for any errors, omissions or misinterpretations of information provided willingly and in good faith.

This dissertation complies with the stipulations of the Board of Graduate Studies regarding dissertations submitted for the Degree of Master of Philosophy in International Relations. It is entirely the product of the author’s own work. All the sources from which I have derived my information appear in the footnotes and are open and unclassified.

_________________________________________________________________

The views expressed in this thesis are those of the author, not of the Ministry of Defence, London

_________________________________________________________________
### Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAR</td>
<td>Air-to-Air Refuelling</td>
</tr>
<tr>
<td>ABM</td>
<td>Anti Ballistic Missile [Treaty]</td>
</tr>
<tr>
<td>AN/FO</td>
<td>Ammonium Nitrate/Fuel Oil [Explosive]</td>
</tr>
<tr>
<td>ATGM</td>
<td>Anti-Tank Guided Missile</td>
</tr>
<tr>
<td>AWACS</td>
<td>Airborne Warning and Control System</td>
</tr>
<tr>
<td>BTWC</td>
<td>Biological and Toxin Weapons Convention</td>
</tr>
<tr>
<td>BM</td>
<td>Ballistic Missile</td>
</tr>
<tr>
<td>BMDS</td>
<td>Ballistic Missile Defense System</td>
</tr>
<tr>
<td>BW</td>
<td>Biological Weapons</td>
</tr>
<tr>
<td>C2W</td>
<td>Command-and-Control Warfare</td>
</tr>
<tr>
<td>C^4ISR</td>
<td>Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance</td>
</tr>
<tr>
<td>CBW</td>
<td>Chemical and Biological Weapons</td>
</tr>
<tr>
<td>CCD</td>
<td>Camouflage, Concealment and Deception</td>
</tr>
<tr>
<td>CEP</td>
<td>Circular Error Probable</td>
</tr>
<tr>
<td>CMC</td>
<td>Computer Malicious Code</td>
</tr>
<tr>
<td>CONOPs</td>
<td>Concept of Operations</td>
</tr>
<tr>
<td>CONUS</td>
<td>Continental United States</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial, Off-The-Shelf</td>
</tr>
<tr>
<td>CSIS</td>
<td>Center for Strategic and International Studies</td>
</tr>
<tr>
<td>CW</td>
<td>Chemical Weapons</td>
</tr>
<tr>
<td>CWC</td>
<td>Chemical Weapons Convention</td>
</tr>
<tr>
<td>DBS</td>
<td>Direct-Broadcast Satellite</td>
</tr>
<tr>
<td>EIW</td>
<td>Economic Information Warfare</td>
</tr>
<tr>
<td>EMP</td>
<td>Electro-Magnetic Pulse</td>
</tr>
<tr>
<td>ESDI</td>
<td>European Security and Defence Identity</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EW</td>
<td>Electronic Warfare</td>
</tr>
<tr>
<td>FMB</td>
<td>Forward Mounting Base</td>
</tr>
<tr>
<td>FOG-M</td>
<td>Fibre-Optic Guided Missile</td>
</tr>
<tr>
<td>FP</td>
<td>Force Protection</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>FSU</td>
<td>Former Soviet Union</td>
</tr>
<tr>
<td>HARM</td>
<td>High-speed Anti-Radiation Missile</td>
</tr>
<tr>
<td>HCDC</td>
<td>House of Commons Defence Committee</td>
</tr>
<tr>
<td>HNS</td>
<td>Host-Nation Support</td>
</tr>
<tr>
<td>HVA</td>
<td>High-Value Assets</td>
</tr>
<tr>
<td>IBW</td>
<td>Intelligence-Based Warfare</td>
</tr>
<tr>
<td>ICBM</td>
<td>Intercontinental Ballistic Missile</td>
</tr>
<tr>
<td>ICSA</td>
<td>International Centre for Security Analysis</td>
</tr>
<tr>
<td>INSS</td>
<td>Institute for National Strategic Studies</td>
</tr>
<tr>
<td>IRBM</td>
<td>Intermediate-Range Ballistic Missile</td>
</tr>
<tr>
<td>IW</td>
<td>Information Warfare</td>
</tr>
<tr>
<td>JIR</td>
<td><em>Jane’s Intelligence Review</em></td>
</tr>
<tr>
<td>JRDF</td>
<td>Joint Rapid Deployment Force</td>
</tr>
<tr>
<td>JRRF</td>
<td>Joint Rapid Reaction Force</td>
</tr>
<tr>
<td>JSTARS</td>
<td>Joint Surveillance and Target Attack Radar System</td>
</tr>
<tr>
<td>MANPADS</td>
<td>Man-Portable Air Defence System</td>
</tr>
<tr>
<td>MaRV</td>
<td>Manoeuvring Re-entry Vehicle</td>
</tr>
<tr>
<td>MEII</td>
<td>Minimum Essential Information Infrastructure</td>
</tr>
<tr>
<td>MTR</td>
<td>Military Technical Revolution</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NBC</td>
<td>Nuclear, Biological and Chemical [Weapons]</td>
</tr>
<tr>
<td>NMD</td>
<td>National Missile Defence [System]</td>
</tr>
<tr>
<td>NPT</td>
<td>[Nuclear] Non-Proliferation Treaty</td>
</tr>
<tr>
<td>NSI</td>
<td>National Strategic Infrastructure</td>
</tr>
<tr>
<td>NW</td>
<td>Nuclear Weapon</td>
</tr>
<tr>
<td>PGM</td>
<td>Precision Guided Munition</td>
</tr>
<tr>
<td>PIRA</td>
<td>Provisional Irish Republican Army</td>
</tr>
<tr>
<td>PSYW</td>
<td>Psychological Warfare</td>
</tr>
<tr>
<td>RMA</td>
<td>Revolution in Military Affairs</td>
</tr>
<tr>
<td>RUSI</td>
<td>Royal United Services Institute</td>
</tr>
<tr>
<td>SDR</td>
<td>Strategic Defence Review</td>
</tr>
<tr>
<td>SIPRI</td>
<td>Stockholm International Peace Research Institute</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>SIW</td>
<td>Strategic Information Warfare</td>
</tr>
<tr>
<td>SPF</td>
<td>Special Purpose Forces</td>
</tr>
<tr>
<td>SRBM</td>
<td>Short-Range Ballistic Missile</td>
</tr>
<tr>
<td>STUFT</td>
<td>Ships, Taken Up From Trade</td>
</tr>
<tr>
<td>TD</td>
<td>Taepo-Dong [Missile]</td>
</tr>
<tr>
<td>TMD</td>
<td>Theater Missile Defense [System]</td>
</tr>
<tr>
<td>UAV</td>
<td>Uninhabited Aerial Vehicle</td>
</tr>
<tr>
<td>UNSCOM</td>
<td>United Nations Special Commission</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USAF</td>
<td>United States Air Force</td>
</tr>
<tr>
<td>USNDU</td>
<td>US National Defense University</td>
</tr>
<tr>
<td>USSR</td>
<td>Union of Soviet Socialist Republics</td>
</tr>
<tr>
<td>WMD</td>
<td>Weapons of Mass Destruction</td>
</tr>
</tbody>
</table>
INTRODUCTION

‘An army may be compared to water, for water in its natural flowing avoids the heights and hastens downwards. So in a war, an army should avoid strength and strike at weakness. As water shapes its flows in accordance with the nature of the ground, an army manages to be victorious in relation to the enemy it is facing. As water retains no constant shape, so in war there are no constant conditions. One who can modify his tactics in accordance with the enemy’s situation and succeed in gaining victory may be called divine.’

Sun Tzu (Fourth Century B.C.)

In its broadest sense, the concept of asymmetry in conflict describes ‘warfare that seeks to avoid an opponent’s strengths; ... an approach that tries to focus whatever may be one side’s comparative advantages against its enemy’s relative weaknesses.’ The expression ‘asymmetric warfare’ has found its way into the international security lexicon only since the end of the Cold War and this sudden attention to asymmetric threats appears to suggest the emergence of a new phenomenon. However, the concept of asymmetric approaches in warfare is hardly new; it reflects any non-linear response to the employment of mainstream military force and the search for asymmetries, as a fundamental element of military strategy, can be traced back to David’s defeat of Goliath with a sling and a pebble. Thus any study of the phenomenon is vulnerable to the challenge that there is nothing about contemporary concepts of asymmetric warfare that would not be recognisable to any of history’s great military strategists - a position that is supported by the opening extract from the writings of Sun Tzu. Furthermore, there is a danger that the term has become something of a cliché, that is widely used as a means of labelling an approach or strategy with little indication that it describes anything new or unique. This particular concern is developed by the RAND researcher, David Shlapak, who observes that every concept has a life-cycle, starting with the juvenile period when people argue about its meaning; followed by a transitional period of respectable maturity, when people understand the meaning and are able to use the concept in a creative and meaningful way. Finally, however, it enters a period of senescence in which the term becomes simply a ‘buzzword’ that is used excessively, with little evidence that anyone remembers what it was intended to mean when the concept was coined. Shlapak fears that the concept of ‘asymmetric warfare’ has passed straight from the juvenile to the senescent stage and has entered the technical jargon without the intellectual scrutiny of the transitional period.

The emerging debate about the relevance and importance of asymmetric challenges, as

---

1 Hanzhang, General Tao, Sun Tzu: The Art of War, (Wordsworth, 1993), 56.
4 ‘RAND’ is a US non-profit institution that aims to improve policy and decision-making through research and analysis.
a counter to Britain’s ability to project military power in support of national or alliance interests, generates a number of questions:

- If the concept of asymmetry in warfighting is not new, what triggered the sudden attention in contemporary military and strategic studies literature?
- Are there specific and unique circumstances which characterise the post-Cold War era and predispose our potential opponents to this form of warfare?
- What are the fundamental ‘asymmetries’ which define contemporary conflict?

In the immediate aftermath of the Cold War, the decisive coalition victory against Iraq in the 1991 Gulf War\textsuperscript{6} was a defining moment, leading many commentators to conclude that future opponents would not attempt to confront the West’s military and technical superiority ‘force-on-force’. Thus, even though potential adversaries may possess sizeable conventional military forces, to meet regional security challenges, the broadly accepted hypothesis is that they are unlikely to rely on these ‘symmetrical’ capabilities in future confrontations with the West. The key factor which led to Iraq’s overwhelming defeat was the West’s (and in particular, the United States’ (US)) exploitation of ‘high-tech’ military capabilities associated with the so-called ‘Revolution in Military Affairs’ (RMA).\textsuperscript{7} On the face of it, this does not represent anything unique, since the history of warfare is a catalogue of major changes in warfighting that can be characterised as asymmetric responses to the opponent’s technical superiority. However, the current RMA is characterised by the reliance on advanced command, control, communications, computer, intelligence, surveillance and reconnaissance (C\textsuperscript{4}ISR) systems. Whereas nations have traditionally emulated (and sought to surpass) successful strategies, it is perceived that these capabilities may simply prove too expensive, with little incentive for opponents to attempt to match the particular style of military operations that is being developed in the West. Furthermore, the West’s emerging concept of operations (CONOPS) reflects the assumption that the possibilities for ‘silicon-based’ warfare can be exploited to permit expeditionary wars to be fought with very high efficiency and low casualties. In these circumstances asymmetric, or ‘adaptive’, strategies provide the logical checkmate, particularly if small or medium powers exploit the opportunities afforded by the inevitable technology proliferation for developing ‘niche’ capabilities which permit them to strike at long range, whether using ballistic missiles (BMs), information-warfare (IW) or terrorism. Thus, the defining asymmetry, which describes the inherent imbalance between the military-technical capabilities of the advanced powers and those of the developing powers, is Configuration Asymmetry. In the calculus of asymmetrics this presents a unique opportunity for small or weak powers, whereby ‘…the advantages accruing to the modern force [may be] neutralised and the disadvantages enormously magnified.’\textsuperscript{8}

What remains unclear is the extent to which opponents specifically seek asymmetric capabilities, as a means of challenging the West; or whether the phenomenon is simply an inevitable trend based on either economic constraints, or technological

\textsuperscript{6} Hereafter referred to as the Gulf War (as opposed to the 1980-88 Iran-Iraq ‘Gulf War’).
\textsuperscript{8} Matthews, op. cit., 20.
proliferation which facilitates the acquisition of niche capabilities. An alternative hypothesis claims that the dominant asymmetry is that of Legal Compliance, between those nations whose actions are properly constrained by the moral and ethical codes enshrined in international treaties and conventions, and opponents whose values and objectives are so fundamentally different that any conflict is inherently asymmetric; indeed, the opponent may not even be conscious of ever having possessed any symmetric options.

The third hypothesis focuses on the asymmetry of Stake, which is a defining characteristic of contemporary military intervention operations. According to this theory, military intervention in support of less-than-vital interests enables the opponent to threaten the will or commitment of the intervening power, rather than having to defeat its military forces specifically; indeed, the US experience in Beirut and Mogadishu illustrates that when interests are limited, an adversary need impose only a modest cost to defeat their opponent’s will. The recognition of this

10 In October 1983 the battleship USS New Jersey, in support of Lebanese government troops, heavily shelled military positions in the hills around Beirut. This was effectively countered by a suicide bomb attack on the US Marine compound and French Headquarters of the Multi-National Force, which killed 241 American servicemen and injured more than 80, resulting in the withdrawal of all US forces including the naval presence. See: Williamson, A.C., ‘Challenges Facing Military Power’, in Peach, S. (ed.), Perspectives on Air Power: Air Power in its Wider Context, (HMSO, 1998), 329. In October 1993, following a US operation in the Somali capital, Mogadishu, to capture two of General Mohammed Aideed’s key lieutenants, eighteen American servicemen were killed in what turned out to be the US force’s single worst fire-fight since Vietnam. However, it was the subsequent television coverage of the Somali’s brutal treatment of two American corpses and one injured prisoner which led to the complete withdrawal of all American forces from Somalia within 6 months of the battle. See: Shukman, D., The Sorcerer’s Challenge: Fears and Hopes for the Weapons of the Next Millennium
fundamental asymmetry is essential if the intervening power is to achieve the optimum relationship between the mission objectives and the instruments of military power. The inter-relationship between asymmetries of configuration, legal compliance and stake is illustrated in Figure 1.

A survey of the contemporary international military and strategic studies literature on this subject reveals the unique perspectives based on the observers’ status and world view. Russian literature demonstrates a conceptual approach to asymmetry; Chinese writers provide an intuitively asymmetric attitude in responding to the RMA; and less prominent nations (Iran, India) show interest in crafting asymmetric sufficiency. As military allies of the US, Britain and France are viewed as independent parallel observers of the RMA and therefore differ from the other nations in that they present possible targets of asymmetric actions.

Accordingly, a central challenge of this paper is to determine how much of the contemporary US analysis is credible, and relevant, to the British debate concerning emerging threats; the first obstacle is to judge the counterclaims of those critics who challenge the motives of commentators who herald a bleak future, in which the West’s military and technological superiority is negated by a weaker power. A cynical appraisal holds that the intense hyperbole surrounding the threat reflects a conspiracy, conjured up by the Western military-industrial complex, in order to sustain high defence investment following the demise of the former Soviet threat (against which expenditure was historically benchmarked). Commentators who favour the primacy of cultural asymmetry argue that perceived “technological” challenges are almost welcomed by the defence industry since it provides enormous opportunities for sales of new equipment to Western forces fearful of technological obsolescence. Alternatively, the emphasis on asymmetric threats may represent a politically-generated counter to the media-induced interventionist fervour of a public who demand military intervention, but whose casualty sensitivity places limits on the military options. Where the government and/or military doubt the wisdom of intervention, an emphasis on the potential for an ‘asymmetric’ backlash (especially against domestic targets) may reduce public pressure for military action. These perspectives highlight the tendency for correspondents to focus on single-issues, emphasising either military, technical or cultural asymmetries, supported by analysis of specific asymmetric approaches; typically the use of weapons of mass destruction (WMD), IW or terrorism. This presents an opportunity for a study which draws together the existing literature in order to determine the linkage between the opponent’s motives, and the specific asymmetric approaches which may be employed at each stage of conflict escalation.

The aim of this paper is to analyse the full spectrum of potential asymmetric


11 ‘Asymmetric Sufficiency’ in this context often denotes a sea-denial strategy; that is, a strategy capable of deterring an RMA-type force from its objectives without necessarily defeating its forces.


approaches in order to determine Britain’s vulnerability to specific challenges prior to, and during, a future military intervention. Part One provides an overview of the asymmetric challenges to British military intervention; first, exploring the British perspective on military ‘power-projection’ and the specific vulnerabilities that emerge as a result of the country’s interventionist stance; then, examining the generic opponent’s ‘means, motives and opportunities’ as a conceptual framework for determining how potential adversaries may identify and exploit the Achilles’ Heel of a particular military intervention. Part Two identifies and analyses the full spectrum of potential asymmetric approaches, focusing first on military capabilities by examining the proliferation of WMD and BM technology, plus the potential for developing powers to acquire and exploit niche capabilities associated with the RMA. This chapter also provides a brief analysis of the military utility of clandestine operations, which specifically target the West’s increasing reliance on scarce, ‘high-value assets’ (HVA). The following chapter explores non-military capabilities, focusing instead on technological and unconventional approaches: on one hand, the adversary who chooses to exploit technology proliferation in order to mount a ‘Strategic Information Warfare’ (SIW) campaign against either military C⁴ISR systems or the National Strategic Infrastructure (NSI); on the other, the opponent at the opposite end of the cultural spectrum, who perceives his comparative advantage not in technological terms but in the ‘collective psyche and will of his people.’

This section explores the potential for opponents to rely on unconventional approaches which blur the boundaries between actions considered crimes and those viewed as warfare, and analyses the utility of atrocities and state-sponsored terrorism as asymmetric tools. In Part Three, the specific threat and the potential countermeasures are assessed; first, through a comprehensive ‘risk analysis’ which analyses the relative utility of each of the potential asymmetric ‘tools’ as a means of achieving key political/military objectives, including deterrence, disruption and coercion. The final chapter evaluates the utility of deterrence strategies and of pre-emptive, preventative and protective measures, as a means of countering asymmetric challenges. In concluding, this paper reviews the British perspective on future military intervention and assesses the range of options from isolationism to rampant interventionism. It explores the tension between the tendency to overestimate the opponents’ capabilities and intentions, and the equally damaging failure of imagination which constrains our awareness of the emerging threat from potential enemies who pursue the ‘twin pillars’ of conceptual innovation and advanced military capabilities. After a brief review of Britain’s future defence and security requirements, which highlights deficiencies in current policy, the paper closes with a case for widening the debate about emerging asymmetric threats.

---

CHAPTER I:

ASYMMETRIC CHALLENGES TO MILITARY INTERVENTION

The Changing Nature of Conflict

During the Cold War, military conflict was characterised by the relative symmetry of the opposing forces. Superpower bipolarity ensured that any engagement was going to be either a catastrophic confrontation between the Warsaw Pact and the North Atlantic Treaty Organization (NATO) or, as it turned out, a series of regional conflicts fought between Superpower proxies. To use Freedman’s definition, these engagements could be classified as ‘symmetrical’ to the extent that they were conducted ‘between similar types of forces, so that superior numbers, training, leadership and technology [would] largely determine the outcome.’

The Superpower symmetry even cast a strategic shadow over those few occasions when one of the Great Powers confronted a small or weak power directly; in the US-led interventions in both Korea and Vietnam, the anticipated outcomes were corrupted by America’s inability to exploit its full military potential, for fear of escalation to a symmetrical Superpower confrontation involving the Soviet Union or China. Since the demise of the Soviet Union, and the emergence of the US as the sole Superpower, military engagements have been characterised by coalition operations, usually under the aegis of the United Nations (UN) or a regional organization such as NATO, against weaker powers such as Iraq and the Federal Republic of Yugoslavia, or Warlords in Somalia. Such confrontations between dissimilar forces are effectively asymmetrical and Freedman defines these as engagements where ‘the outcome is the result of an inability to defend against the force with which attacked.’

The asymmetry of force is a factor of the increasing technology gap between the weaker states and those who possess, or are developing, ‘power-projection’ capabilities. This has led defence and security analysts to predict that present and future opponents will inevitably expend considerable intellectual and material resources to develop political-military responses, designed specifically to disrupt or counter the great strengths inherent in these new force structures.

Defining Asymmetric Threats

In its single reference to emerging asymmetric threats to British interests, the Government’s 1998 Strategic Defence Review (SDR) warned that:

‘…where we (and our Allies) exploit technology to strengthen our existing superiority in conventional weapons, our potential adversaries may choose to adopt alternative weapons and unconventional (or ‘asymmetric’) strategies, perhaps attacking us through vulnerabilities in our open civil societies.’

15 Ibid., 38-9.
17 Ibid., para. 34.
However, whilst the Review provided a contextual basis for British discussions about the nature of future defence requirements, it did not develop detailed information about the future battlefield at the operational level of war. Specifically, the House of Commons Defence Committee (HCDC) identified the lack of attention to emerging asymmetric threats as a lacuna in the report; citing the Chairman of the Royal United Services Institute for Defence Studies (RUSI), the HCDC Report stated:

‘…there is a very profound problem underlying the defence posture that emerges from this Review … That is, we are going to have an extremely elegant and effective defence capability for dealing with a rather well defined set of contingencies which would involve getting in, doing something fairly rapidly and getting out again. I think that the discontented nations and groups are not [in the future] going to meet in our battle space at all.’

Part of the problem stems from the difficulty in establishing precisely what is meant by the term asymmetric threats; to borrow an analogy from Libicki, ‘coming to grips with [asymmetric] warfare is like the efforts of the blind men to discover the nature of the elephant: the one who touched its leg called it a tree, another who touched its tail called it a rope, and so on.’ Thus, definitions characteristically reflect the perspective of the author, in terms of their emphasis on either military, technical or cultural asymmetries. However, the early work on asymmetric strategy (attributed to analysts at RAND) has spawned the following broad definition:

‘Asymmetric strategies attack vulnerabilities not appreciated by the “target” (victim) or capitalize on the victim’s limited preparation against the threat. These strategies rely (primarily but not exclusively) on [concepts of operations] that are fundamentally different from the victim’s and/or from those of recent history. They often employ new or different weapons. Additionally, they can serve political or strategic objectives that are not the same as those the victim pursues.’

**Future Military Intervention**

**Instability, Intervention and International Law**

The SDR determined that the world was unlikely to face a global military challenge (on the scale of the former Soviet Union (FSU)) for at least the following two decades; there being no threat of strategic attack against NATO; no direct military

---

21 Bennett et al, *op. cit.*, 3.
threat to the UK or Western Europe, and the re-emergence of such a threat was not predicted. However, the Review projected a threat to security from instability, both inside Europe and elsewhere, and the risks to international stability were predicted to stem from ethnic and religious conflict; population and environmental pressures; competition for scarce resources; drugs, terrorism and crime; traditional expansionism; the disintegration of states and the overspill of regional conflict. This assessment provided the justification for the emphasis on ‘power-projection’ capabilities, reflecting a realisation that the liberal democracies would increasingly be called upon to intervene, especially in the face of overwhelming humanitarian need.

In the context to which it is referred in this paper, ‘intervention’ is defined by Freedman as:

‘… the use of armed force to influence the character and course of a developing conflict which is neither taking place upon nor directly threatening national territory, and does not touch upon any specific obligations to allies… In this sense, intervention is mainly distinguished from the many other contingencies for which armed forces prepare by the lack of a strategic imperative.’

This definition illustrates the changing nature of intervention which seems to be the emerging norm for operations in the post-Cold War era. Historically, force could only lawfully be employed for the purposes of Collective Self Defence in accordance with Article 51 of the UN Charter. This provided the foundation for the formation of NATO and the justification for the Coalition operation to liberate Kuwait during the Gulf War. Alternatively, and exceptionally, force can be authorised by the UN for the purpose of military ‘enforcement’ measures, mandated under Chapter VII of the Charter, for Collective Security operations where the Security Council determines the existence of a threat to international peace and security. Such a mandate provided the underlying authorisation for the Gulf Coalition and the specific authorisation for the UN’s subsequent operations in Somalia and Bosnia. However, as a rule, intervention remains precluded under Article 2(4) of the Charter which expressly prohibits the use of force against the territorial integrity or political independence of a state.

Humanitarian catastrophes present a grey area in international law; in theory, if a state begins to disintegrate through severe internal instability it might be permissible to use military forces to deliver and protect humanitarian aid, but otherwise intervention has to be confined to diplomatic efforts and economic sanctions. However, the doctrine of non-intervention has begun to give way to the emerging doctrine of ‘humanitarian intervention’. The British position on this matter was confirmed by Britain’s Foreign and Commonwealth Office, in a statement to the House of Lords on 9 March 1999:

‘… cases have arisen, for example in northern Iraq in 1991, when, in the light of all the circumstances, a limited use of force has been justified as the only means to avert an overwhelming humanitarian catastrophe in support of purposes laid down by the Security Council but without the Council’s express

---

22 SDR, op. cit., paras. 29-31.
This doctrine was implemented on 24 March 1999 when NATO launched air strikes against the Federal Republic of Yugoslavia, in order to precipitate an end to the humanitarian emergency in Kosovo, and this represented the first time that a coalition operating without specific UN authorisation had openly used force to prevent the effective ruler of a sovereign state from perpetrating crimes against his own people.  

Political Decision Making

Although the Kosovo operation was broadly supported on moral grounds, it nevertheless raised difficult questions concerning the future of armed intervention. Such decisions inevitably entail a delicate risk calculation by governments who have to balance the terrible results of internal strife in unstable countries with the inherent dangers in taking exceptional measures which may require significant sacrifices by their own people. The government dilemma, when faced with public demands for humanitarian intervention, is highlighted by Towle who examines the distinction between Britain’s political decision making prior to the Falklands and Gulf wars, and its subsequent engagement in Bosnia. He observes that government policy-making is aided when there is general consensus between the establishment and public that intervention is favourable; however, if the government and the armed forces doubt the wisdom of military action but the public press for humanitarian intervention this leads to inevitable friction. Towle’s conclusion may offer a credible explanation for the recent US literary explosion concerning emerging asymmetric threats to the homeland. A government that is faced with a hostile media calling for intervention to resolve an emerging humanitarian catastrophe, but which fears a lengthy entanglement for no definable national interest, may be able to suppress the public’s interventionist fervour if there are credible fears of an asymmetric backlash against domestic targets.

The Pitfalls of Military Intervention

This theme was developed by Sabin, in a Memorandum submitted to the HCDC (following the publication of the SDR) which highlights the ‘darker side’ to military intervention:

‘Using force for purposes other than direct defence can be extremely divisive and politically damaging both at home and abroad, as the Israelis found in Lebanon, the Soviets in Afghanistan and the Americans in Vietnam.’

Sabin noted that even humanitarian interventions can turn sour if the forces take high casualties for no apparent vital national interest, and that the capacity of Britain’s
potential opponents to inflict massive harm on the UK is growing, rather than diminishing, as the ‘insidious possibilities of bacteriological and information warfare’ develop:

‘…early intervention to nip a problem in the bud is better than waiting until the adversary has gained confidence and expanded his capability. However, the SDR never properly addresses the contrary possibility, that intervention may actually provoke regional powers into threatening the security of Britain itself.’  

British Vulnerability

In the 1990s, a spate of terrorist attacks against US military, political and symbolic domestic targets significantly increased the perception of America’s vulnerability to asymmetric challenges. Given the country’s military and technological preponderance, combined with its natural role as the Coalition leader, it is perhaps inevitable that America has become the prime target for attack. This has contributed to much of the apprehension concerning continued US participation in intervention operations, especially for humanitarian reasons where there is no clearly definable national interest. Nevertheless, Gompert notes that:

‘While hesitant about intervening militarily where national interests are not clearly at stake, the American public has nonetheless been willing to support the use of US forces in defense of important norms, provided other core states share in the risk.’

Britain has consistently demonstrated its firm commitment to risk-sharing in the fulfillment of international obligations. This was confirmed in 1993 by the then Secretary of State for Defence, who set out the criteria against which the UK should judge whether or not to become involved in military intervention:

‘The first criterion must be the national interest…. In addition, our obligations as a member of the Permanent Five, and expectations of us, both our own and those of others may tend to spread the net rather wider. The result is that it will sometimes not be desirable to avoid involvement in operations where the national defence interest is slight, or non-existent.’ [emphasis added]

This ‘pro-interventionist’ stance indicates that there may be circumstances in which it is plausible to argue that Britain, rather than the US, could become the central target of asymmetric attack: first, the unlikely but conceivable event that Britain could engage in a unilateral intervention; second, Britain’s continued role as a key US

28 Ibid.
29 See Tables 5/6.
coalition partner; and, third, Britain’s potential role as the Coalition Leader in a future non-Atlantic intervention, conducted under the auspices of the European Security and Defence Identity (ESDI).

Unilateral Intervention

Even if able to act unilaterally, there is little doubt that Britain would prefer to operate as part of a coalition, if only for enhanced international legitimacy. However, Britain has over ten million citizens living and working overseas and thirteen dependent territories around the world, so the possibility of unilateral action cannot be ruled out. The SDR aspired to project Britain’s defence requirements seventeen years forward - to 2015 - yet a Defence White Paper published seventeen years earlier, in 1981, failed to foresee events that unfolded only one year later, when Argentina invaded the Falkland Islands. Thus, one enduring legacy of the Falklands conflict is that ‘[f]or the hundredth time in her history, Britain was reminded that there is always an unexpected military threat which defence planning must be flexible enough to provide for.’

Coalition Partner

Britain’s participation as a key Coalition partner in future intervention operations may make her vulnerable to attack by opponents seeking to either increase the ‘entry price’ for any intervention force, or intimidate one or more allies into dropping out of a coalition. These threats are real and, on occasion, specific. During the military built up to planned air strikes against Iraq, in February 1998, a coalition of British-based fundamentalist groups threatened a jihad (holy war) in the UK. Omar Bakri Mohammed, the head of a militant Islamic group based in Britain, subsequently put his name to the anonymous fatwa (statement) which: ‘call[ed] on Muslims throughout the world to “confront by all means whether verbally, financially, politically or militarily” any “aggression”’. On 24 March 1998, the British Home Secretary confirmed that his Office had circulated an ‘all-ports warning’ which revealed that Iraq was plotting to smuggle quantities of anthrax into those ‘hostile countries’ who had threatened military action against the Baghdad regime the previous month. Then on 25 December 1998, shortly after Operation DESERT FOX (renewed US-British air strikes against Iraq), Osama Bin Laden declared in an interview with the London-based Arabic Newspaper Asharg Al-Awsat that the air strikes made it “a duty of Muslims to confront, fight and kill” Americans and Britons because “the British

32 SDR, op. cit., para. 20.
33 Observation attributed to: Garden, Sir Timothy (then Director, Royal Institute of International Affairs Chatham House). Cited in ‘Minutes of Evidence Taken Before The Defence Committee (22 July 1998)’ HCDC, op. cit. 442.
35 Omar Bakri Mohammed is the President of al-Muhajiroun (The Emigrant), a militant Islamic group based in Britain.
the American people loudly declare their support for their leaders’ decision to attack Iraq.”

Coalition Leader

Although current US policy maintains an activist, interventionist posture, America has declined the role of global policeman, concluding that: ‘Its friends need to bear international security responsibilities commensurate with their wealth and their equity in the core’s health, security and norms.’ Britain has been at the forefront of the European response to US calls for equitable burden sharing and has announced a firm commitment to the ESDI. The idea was first floated by Britain’s Prime Minister at an informal European Union (EU) summit in October 1998; in December that year, at the Anglo-French St. Malo Summit, the two governments issued a joint communiqué which concluded that the EU:

‘...must have the capacity for autonomous action, backed up by credible military forces, the means to decide to use them, and a readiness to do so [which requires] strengthened armed forces that can react rapidly to the new risks.’

Given Britain’s potential status as ‘Coalition Leader’ in a future non-Atlantic intervention - a leadership role that is currently almost exclusively filled by the US - it is credible to predict that Britain would inevitably become vulnerable to the same challenges that have, hitherto, been directed almost exclusively against American targets.


41 Walker, M., ‘Europe takes the first steps to common defence policy’ *The Guardian* (3 June 1999), 15.
CHAPTER II: MEANS, MOTIVE AND OPPORTUNITY

‘As any fan of mystery novels can attest, police seeking a suspect for some heinous crime look for a combination of means, motive and opportunity.’

Just as this analogy was used by Shlapak and Vick for analysing the evolving ground threat to US Air Force (USAF) bases, it also provides an effective conceptual framework for analysing how potential adversaries may identify and exploit the relative weaknesses of a particular military intervention. This chapter examines the generic adversary’s means, in terms of those military, technological or unconventional approaches which may be exploited to achieve a comparative advantage; the motives, which may include the deterrence, disruption or defeat of the use of military power; and the opportunities, presented by the nature of contemporary high-tech military forces and the open societies which characterise the liberal democracies.

Means

The means of perpetrating an asymmetric attack are diverse and centre on the adversary who possesses sophisticated military capabilities and highly advanced conventional forces, but targets these capabilities selectively, against specific vulnerabilities, rather than engaging in symmetrical ‘force-on-force’ combat. Alternatively, the high-tech adversary may decide not to rely on traditional military capabilities in challenging superior opponents (although he may possess these capabilities for regional security) but instead exploit technological comparative advantages by targeting his opponent’s military and civil reliance on information systems. At the opposite end of the cultural spectrum is the adversary who perceives his comparative advantages in terms of the asymmetry of legal compliance, and pursues unconventional strategies designed to attack his opponent’s will.

Military Approaches

In an influential paper on ‘asymmetric threats’, written for the US National Defense University (USNDU) 1998 Strategic Assessment, Wilson outlines the options that could represent an asymmetric response to US military and technological superiority; principally, the acquisition of WMD, long-range ballistic or cruise missiles, and key capabilities associated with the RMA (including high-technology sensors, communications and weapon systems). This theme is developed by Shlapak and Vick, who focus on the utility of advanced RMA-technologies for use by small units engaged in clandestine operations against HVA. However, the RMA encompasses a broad range of capabilities which also provide opportunities for the adversary who targets the asymmetry of technical, rather than military, configuration.

43 Wilson, P., ‘Asymmetric Threats’ in Binnendijk, op. cit., 170-78.
44 Shlapak and Vick, op. cit.
Technological Approaches

The dominance of technical configuration asymmetry is supported by Freedman, in his 1998 Adelphi Paper, which discusses the implications of the RMA for strategic affairs. Freedman emphasises the primacy of the digitized battlespace and information dominance for future high-tech military operations and concludes that the increasing reliance on information, for the successful prosecution of military and political objectives, may provide the motivation for technologically-competent opponents to develop IW techniques. This is supported by Wilson who identifies the exploitation of cyberspace as an asymmetric option, either to disrupt the rapid deployment phase of a military intervention or to ‘bring the war home’ by targeting the NSI.

Unconventional Approaches

The opponent who lacks the necessary fiscal, technological or operational resources to achieve sophisticated military or technological capabilities is likely to adopt unconventional approaches which exploit asymmetries in legal compliance. Wilson identifies the selection of unfavourable environments, such as urban areas and mountainous or jungle terrain, that degrade the armed force’s ability to find and attack militarily significant targets; however, this explanation of unconventional approaches should be expanded to include acts which exploit fears of collateral damage or regional conflict escalation. There is a separate school of thought which views cultural distinction as the dominant asymmetry in contemporary conflict and proponents argue that low-tech enemies, characterised by the ‘warrior societies’, are likely to resort to atrocities or acts of terrorism designed to defeat the will of the intervening power.

There is some overlap here between military and unconventional approaches, in terms of the victim’s perception, since acts viewed as legitimate military operations by the perpetrator may be portrayed as terrorism by the victim. This could apply in particular, to the opponent who employs small ‘special purpose forces’ (SPF) units to engage in clandestine operations against military targets outside the theatre of operations.

In summary, there are three distinct asymmetric approaches, each championed by different schools of thought and each encompassing specific means of attack - although there is inevitable overlap. The inter-relationship between the potential

---

46 Digitized Battlespace: the integration of cyberspace with the three-dimensional land, sea and air battlespace.
47 Information dominance: the exploitation of advanced C4ISR systems in order to optimise the free exchange of real time information.
49 See Chapter IV: Unconventional Approaches.
50 See footnote 136.
military, technological and unconventional approaches is illustrated in Figure 2 (and analysed in detail in Chapters III-IV).

![Figure 2: Asymmetric Approaches and Means](image)

**Motives**

The principal incentive for perpetrating an asymmetric attack against a superior opponent was emphasised by the decisive coalition victory in the Gulf War. This spawned the prediction that in any future confrontation the opponent would seek to neutralise, or at least reduce in effectiveness, the key components of the intervening force’s military power. The prominence of air power in the coalition and NATO operations in Iraq, Bosnia and Kosovo has focused attention on this particular component; however, asymmetric challenges could equally be targeted at high-value maritime and land-based assets, or at domestic targets including the NSI and civil population. The classical military paradigm offers three key motives for the weaker power to adopt an asymmetric strategy - deterrence, disruption and defeat\(^{51}\) — although there are others which are worthy of consideration. *Deterrence* strategies focus on intimidation, through the threatened use of force, in order to raise the ‘entry price’ for military intervention; the aim may be to deter allies and prospective partners from participating in military action or from permitting operations to be launched from their territory. If deterrence fails, the opponent is likely to attempt to *disrupt* military intervention by interrupting, hindering or suspending either the preparation, deployment or execution phases of the operation. The aim may be to disrupt operational tempo in order to undermine public confidence in the military’s ability to

\(^{51}\) Wilson (1998), *op. cit.*, 169-70
prosecute a successful campaign with minimal casualties, and to stimulate public pressure to limit the scope and duration of military involvement. Thus the opponent’s motives could also include *exhaustion*, which targets public impatience for a swift conflict resolution by stimulating the perception that continued intervention would be increasingly costly and futile; or *attrition*, which targets the increasing reliance on scarce, HVA. *Defeat* is a more contentious motive since, whilst it might be possible to defeat the *use* of military power, it is debatable whether or not it is possible to defeat the *user* through asymmetric strategies alone. The term suggests the destruction or surrender of the defeated party and, since modern intervention typically lacks strategic imperative, it is possible for the military to disengage rather than capitulate. Therefore, the more realistic motive is *coercion*, which Scott distinguishes from the deterrent use of force ‘in that it seeks to change an existing pattern of behaviour by that force application, rather than discourage the initiation of a course of action by threat.’

52 Thus, if a state is unable to deter military intervention - and other strategies fail to induce a withdrawal - coercive strategies could be employed in an attempt to undermine domestic public and political support for the continued use of military force.

**Opportunities**

The opportunities for a state to challenge a superior opponent using asymmetric strategy are determined by the opponent’s *relative* weaknesses, since this is where the weaker party will attempt to focus their military, technical and unconventional *comparative advantages*. These weaknesses stem from vulnerabilities and cultural sensitivities inherent in the character of both the armed forces and the open civil societies of the liberal democracies, and are illustrated in Figure 3.

Political vulnerabilities include the fragility of alliances and military coalitions, and the impact of domestic pressures on political and military decision-making processes. The inherent military *Achilles’ Heels* include the limited self-protection capacity of first-echelon ‘rapid reaction forces’; the reliance on scarce HVA; operational constraints imposed by Host-Nation interface; and information dependence. However, military power-projection is also reliant on civil transport and communications networks for power-projection, and therefore the accessibility of the NSI presents an additional vulnerability which may be exploited by an opponent.

---

Figure 3: Political and Military Vulnerabilities

Alliance and Coalition Fragility

The principle *Achilles’ Heel* of any military intervention is the inherent fragility of alliances and coalitions. Freedman notes that assembling an intervention force can be a politically complex process:

‘Putting such coalitions together takes time, and may lead to an over-dramatisation of the threat as well as intensive arm-twisting. As soon as an objective has been set, the reputation of the coalition members and the sponsoring institution, if there is one, is at stake.’

Thus, given the emphasis placed on coalition-building for the purposes of burden-sharing and international legitimacy, Wilson concludes that:

‘Much of what the potential regional predator will do in the coming decade will probably be focused on undermining a US-led political-military coalition, both in the region and at the United Nations.’

An associated vulnerability is the reliance on host-nation support (HNS) for ‘in-theatre’ bases and facilities from which to mount military operations. This provides a

---

lucrative, and potentially more accessible, opportunity for potential opponents who may direct asymmetric threats at potential hosts in order to deter them from offering their facilities to intervention forces.

**Domestic Sensitivities**

A second *Achilles’ Heel* is the vulnerability of political and military decision-making processes to domestic sensitivities, related particularly to casualty intolerance. A significant trend in Western military intervention is a humanitarian concern that reflects in the public’s sensitivity to casualties on *both* sides and American military historian, Walter Boyne, identifies two unique public demands that have been made since Vietnam:

‘The first of these demands is that we must fight our wars with the minimum of casualties to our forces. America wants no more Vietnams where our troops are forced to fight and die in unconscionable numbers. The second of these demands is unusual in history, for it is that we must also win our wars with a minimum number of casualties inflicted on the enemy.’\(^{55}\)

This is compounded by the public’s low tolerance of conflicts that do not involve the nation’s key interests; a factor which featured prominently in the conflicts in Afghanistan, Somalia, Bosnia and Kosovo. Williamson notes that there is likely to be a degree of ‘casualty insensitivity’ where national survival is at stake; however, the sensitivity will increase dramatically where the cause is essentially idealistic (such as the enforcement of UN mandates) varying in proportion to the scale of the casualties and whether or not the lives of nationals are at risk. Domestic casualty intolerance is frequently attributed to media-influence and Badsey claims that this has:

‘…distorted the foreign policies of western countries in the aftermath of the Cold war by forcing military intervention in such areas as former Yugoslavia, Somalia or Cambodia, while at the same time preventing that intervention from becoming effective by imposing arbitrary constraints on the level of force used, and on the willingness to risk both taking casualties and inflicting them.’\(^{56}\)

Memories of the near casualty-free Gulf War and the unprecedented intervention in Kosovo, which was resolved without a single NATO combat casualty, has stimulated concerns that the phenomenon has ‘…caused many Americans to conclude erroneously that the occurrence of any casualties [is] irrefutable proof that a campaign [is] inherently flawed and should, therefore, be abandoned.’\(^{57}\) Others reject the ‘myth’ of casualty intolerance, arguing that:

‘[America is] a society of bargain hunters and we are not willing to pay for


\(^{56}\) Badsey, S., ‘Modern Military Operations and the Media’ *The Occasional* No. 8 (Strategic and Combat Studies Institute, 1994), 3.

some things. What got us out of Vietnam was not our unwillingness to lose people but that we got tired of not knowing why we were losing people - tired of not having any sense that we were closer today to achieving our goals than we were yesterday.'

Nevertheless, whether or not the phenomenon is a myth, what matters is the opponent's perception and this has stimulated legitimate fears that some may seek to acquire limited capabilities which inflict serious casualties, rather than fight a typical operational campaign.

Reliance on Scarce, High-Value Assets

Of the four key Achilles' Heels of modern power-projection capabilities, the principle vulnerability is arguably the reliance on scarce HVA - a factor of the technological complexity and expense of advanced military systems. The early association of this vulnerability with air power stems from the work of the Italian strategist, General Guilio Douhet, who observed in 1921 that:

"it is easier and more effective to destroy the enemy’s aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air."

Douhet’s metaphor is equally applicable today, given the dependence on specialised aircraft, such as the Airborne Warning and Control System (AWACS) and the Joint Surveillance and Target Attack Radar System (JSTARS), which are few in number and typically too large to be parked in hardened hangars. Paradoxically, the increased complexity and sophistication of modern aircraft systems makes them increasingly vulnerable to even superficial shrapnel damage, such as that inflicted by an exploding mortar shell or a high-calibre sniper round, and this is compounded by the increasing reliance on advanced precision guided munitions (PGMs) which reduces both the number of weapons necessary to achieve a given objective and hence the number of aircraft required. Targeting advanced combat aircraft would yield the same results whether these platforms were airborne or on the ground; thus a successful attack on an air base may have a strategic effect out of all proportion to the resources expended. One measure to reduce this vulnerability is an increasing emphasis on carrier-based operations, confirmed by the British Government’s commitment to give the existing Invincible class carriers a wider power-projection role and by the decision to purchase two larger, more versatile carriers to replace the existing ships by the year 2012.

However, Wilson warns that the potential opponent’s logical response to this strategy is the acquisition of sufficient RMA-type capabilities to be able to challenge a

58 Shlapak, (11 May 1999), op. cit.
61 ‘For example, superficial shrapnel damage to a stealthy aircraft’s aerodynamic surfaces would… increase its radar cross-section, making it more vulnerable to detection and, hence, impairing its operational effectiveness, even if no vital components were damaged.’ Shlapak and Vick, op. cit., 14.
62 SDR, op. cit., para. 115.
superior power’s maritime rapid deployment capability. This might include the purchase or development of long-range ground and air-launched anti-ship cruise missiles, intelligent sea mines and submarines.

**Vulnerability of ‘First-Echelon’ Forces**

The rapid deployment phase of an intervention force is especially vulnerable to disruption and pre-emptive attacks against ports of embarkation, whilst attacks against lead elements of larger deploying forces could cripple the coalition strategy. In addition to ports, the staging airfields and in-theatre hub air bases are equally vulnerable; as Shlapak and Vick’s analysis of threats to USAF bases concluded,

‘…. any successful attack on a US airlift hub would produce significant *virtual attrition* - serials ( airlift sorties) delayed or cancelled as units stood down, however briefly, to reassess security arrangements and neutralise any residual threat. Even a brief delay in executing a large overseas deployment could have disastrous consequences if an enemy exploited the interruption to score early victories.’

This vulnerability extends to the intervention forces once they have been successfully deployed into theatre; indeed, the SDR identified that Britain’s existing ‘Joint Rapid Deployment Force’ (JRDF) was especially exposed as ‘...it [was] relatively small, lightly armed and potentially vulnerable if attacked before it [could] be reinforced by heavier forces.’ Nevertheless, although the Review announced the formation of new Joint Rapid Reaction Forces (JRRF) ‘... with real punch and protection.’ [emphasis added] it was not specified how this new force structure would be configured to provide protection against the range of asymmetric threats to which ‘first-echelon’ forces could be exposed.

**Host-Nation Constraints**

The reliance on ‘Host-nation’ deployment bases for expeditionary operations presents specific vulnerabilities which particularly affect the forward-deployment of air power assets; however, these vulnerabilities can also extend to in-theatre ports and logistics depots. RAND analysts have identified special dangers arising from four key sources: first, a lack of HNS and infrastructure including shelters, dispersal space, secure accommodation, and adequate pre-prepared fighting positions and defence plans; second, the increased use of inherently insecure civilian facilities (i.e. ports and airfields) which provide limited access control and no protection for key resources such as fuel; third, minimal experience with host-nation security forces which makes local operational planning and co-ordination difficult, particularly where the host

---

66 SDR, *op. cit.*, para. 91.
constrains the intervention force’s ability to operate effectively (e.g. by restricting their movement ‘outside the wire’); and, finally, host-nations will often be confronted by a significant internal threat - indeed, many post-Cold War operations, including Haiti, Somalia and Rwanda, were undertaken in response to internal disarray in a country.68

Information Dependence

The fourth Achilles’ Heel of military power-projection reflects the maxim that ‘technologically advanced, information-intensive military organizations are more vulnerable to information warfare simply because they are information dependent.’69

Accessibility of National Strategic Infrastructure

Finally, one of the characteristics of modern armed forces is their rapidly increasing dependence on the civil infrastructure for mobility, power-projection and support. Therefore a further source of vulnerability is the relative accessibility of the NSI, leading Wilson to predict that attacks could be targeted against:

‘…the major elements of the national economy: the public telecommunications network, the financial and banking system, the electric power grid, the oil and gas networks, and the national transportation system – specifically, the air transportation system.’70

Wilson’s focus is principally the emerging IW threat; however, an equally lucrative means of attack would be conventional terrorism and this was illustrated by the Provisional Irish Republican Army’s (PIRA) change of strategy in the latter half of the 1990’s from directly attacking military objectives to the targeting of the City of London, Heathrow Airport and Britain’s motorway and railway networks.

---

68 Shlapak and Vick, op. cit., 61.
CHAPTER III: MILITARY ASYMMETRIC CHALLENGES

Weapons of Mass Destruction

Introduction

In his 1998 *Foreign Affairs* paper, Betts argues that the role WMD play in international conflict is changing:

‘They no longer represent the technological frontier of warfare. Increasingly they will be weapons of the weak - states or groups that militarily are at best second-class.’

In addition to the technical advances, analysts have noted the increased ease with which the necessary materials and equipment can be acquired, and an associated expansion in the number of actors, delivery means and types of material involved. The acquisition of WMD by potential adversaries will greatly increase the difficulty of forming and sustaining a coalition so, for weaker states, the use or threatened use of WMD may present the optimum counter to intervention. Following the end of the Cold War, the proliferation of nuclear, biological and chemical (NBC) weapons highlights the paradox that there is now less danger of complete annihilation but potentially more danger of mass destruction. This section addresses the military use of WMD by small powers (the potential for their use by non-state actors, as ‘terror’ weapons is assessed in Chapter IV).

Nuclear Weapons

The motives for acquiring a nuclear weapons (NW) capability may be rooted in prestige, a desire to punish or destroy neighbours or to deter military intervention. The use of NW for deterrence purposes is analysed by Preston who notes, in his analysis of the impact of nuclear proliferation on interstate security relationships, that: ‘...the ability of new nuclear states to deter aggressors ... is determined by the capabilities and survivability of their nuclear forces, as well as the degree to which their threats are seen as credible by opponents.’

Thus, for small states, nuclear capability would not necessarily guarantee the ability to deter Great Power intervention, since nuclear threats would only seem credible if the small power’s central interests were critically threatened. Nevertheless, Schelling observes that ‘the power to hurt is bargaining power’ and this may motivate Great Powers to bargain with small nuclear states and avoid threats to their own central interests. Preston uses the analogy of the Gulf War to argue that, had Iraqi *Scud* missiles been carrying nuclear warheads, it is difficult to imagine a scenario in which this would not have significantly altered the course of events:

73 Schelling, in Preston, *ibid.*, 93.
‘Would the United States have been willing to trust that a Saddam Hussein would not have dared to strike its conventional military forces in the Saudi/Kuwait desert if a ground war had begun which actually threatened his regime’s survival?’

It is conceivable that NW could also be used in a ‘less-than-lethal’ IW mode, and Wilson observes that:

‘…several could be used to generate wide-area electromagnetic pulse (EMP) effects during a critical phase of a military operation in order to damage a wide array of C4ISR assets…’

However, notwithstanding the deterrence or disruptive value of nuclear threats the actual use of NW would provide the nuclear powers with the legitimate right of nuclear retaliation and this factor alone should weigh heavily against their overt military use. Therefore, opponents are unlikely to launch attacks in such a fashion that the source could be easily determined, favouring instead nuclear terrorism for which the sponsoring state could be reasonably assured of plausible deniability.

**Chemical Weapons**

The military use of chemical weapons (CW) was brought to the forefront of attention in the last quarter of the twentieth century, following their use by Iraq against Iranian troops in the 1980-88 Gulf War, and against Kurdish civilians in 1988. CW are more widely available than NW because the technology required to produce them is simpler and a large number of countries have undertaken CW programmes; however, logistically and operationally, it remains very difficult to deliver CW in significant quantities over wide areas. This limits the ability to inflict a large number of casualties in a single strike, leading Betts to argue that CW are not really in the same class as other WMD. More than ninety countries have ratified the 1993 Chemical Weapons Convention (CWC); however, some notable signatories (Russia) have not ratified the document and other known CW proliferants (Libya, Syria, Iraq, North Korea) have refused to sign. When added to doubts about the ‘good faith’ of promises by Iran and China, many analysts have expressed doubts about the relevance of the Treaty. CW remain easier to obtain than NW, despite the existence of a treaty regime and adequate verification measures; however, they lack ‘killing capacity’ and, given the comprehensive CW defence measures implemented by most advanced military powers, the deterrence value of such weapons is reduced.

**Biological Weapons**

Biological weapons (BW) have received less attention than the others but arguably present the greatest danger; Betts notes that:

‘…biological weapons combine maximum destructiveness and easy availability. Nuclear arms have great killing capacity but are hard to get;
chemical weapons are easy to get but lack such killing capacity; biological weapons have both qualities.\textsuperscript{77}

Moreover, the long delay time associated with the effects of BW reduces the risk of the attacking state being definitively identified, making their use to induce widespread illness without mass casualties an attractive form of disguised warfare. Of particular concern is the global diffusion of dual-use biotechnology, ideally suited to countries with small budgets. Fears of BW proliferation were highlighted by the UN Special Commission’s (UNSCOM) experience in Iraq following the Gulf War; the Baghdad regime had taken extraordinary steps in order to prevent bio-warfare inspections and in early 1999 a UNSCOM spokesman reported that thirty tons of BW agents remained unaccounted for (see Table 1).\textsuperscript{78}

<table>
<thead>
<tr>
<th>BW Agent</th>
<th>Quantity</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botulinum Toxin</td>
<td>19,000 litres</td>
<td></td>
</tr>
<tr>
<td>Anthrax</td>
<td>8,500 litres</td>
<td></td>
</tr>
<tr>
<td>Af.latoxins</td>
<td>2 tons</td>
<td>potent liver carcinogen (not immediately lethal) possible cover for the production of a lethal toxin (such as Clostridium perfringens) which Baghdad has admitted producing only in limited quantities.</td>
</tr>
<tr>
<td>Trichothecene mycotoxins</td>
<td>unknown</td>
<td>by-products of fungal metabolism: potent blistering and vomiting agents suspected to have been used by the FSU in Afghanistan, Laos and Kampuchea.</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>30 tons</td>
</tr>
</tbody>
</table>

Obtained from a declaration made by Iraq, which UNSCOM has been unable to verify.

Source: JIR\textsuperscript{79}

The significant problem remains that while most nations (including Russia, Iraq and Iran) have signed and ratified the 1972 Biological and Toxin Weapons Convention (BTWC) it remains the only international arms convention not to include verification regimes. Indeed in 1992, Russian President Boris Yeltsin acknowledged that the FSU had continued to work on an offensive BW programme despite being a co-signatory of the BTWC.\textsuperscript{80} The use of BW would certainly risk overwhelming reprisal; but, in theory, those countries who have ratified the BTWC/CWC, and who are in compliance with the negative security assurances issued in accordance with the Nuclear Non-proliferation Treaty (NPT)\textsuperscript{81} - including the US and Britain - would be restricted to massive conventional retaliation.

\textsuperscript{77} Ibid., 32.
\textsuperscript{78} Buchanan, E., (UNSCOM Spokesman) cited in Venter, A., ‘Biological warfare: the poor man’s atomic bomb’ Jane’s Intelligence Review (JIR) (March 1999), 42.
\textsuperscript{79} Ibid.
\textsuperscript{81} UN Security Council Resolution 984 embraces unilateral security assurances made on 6 April 1995, in which the five acknowledged nuclear powers undertook not to use or threaten to use NW against states who are party to, and in compliance with, the NPT: Programme for Promoting Nuclear Non-Proliferation: Newsbrief, (No. 30, 2nd Quarter 1995), 28-32.
Ballistic Missiles

The established motive for the emerging powers acquiring a BM capability is to possess a strategic counter to the advanced powers’ conventional and information-based military superiority, through the ability to threaten their homeland, military forces, partners and allies. One of the most authoritative and reliable BM threat assessments, available in the public domain, is the 1998 Rumsfeld Commission report\(^{82}\) which highlights two distinct US concerns: that intercontinental ballistic missiles (ICBMs) might be launched against the Continental United States (CONUS) and that short- to intermediate-range missiles (SRBM/IRBMs) might be launched against US security partners or forward-deployed intervention forces. Such concerns remain controversial, given that only Russia and China present a current ICBM threat to the CONUS and both are generally regarded as potential partners rather than enemies. However, the report concluded that a developing threat was posed by those transition states (North Korea, Iran and Iraq) who were making concerted efforts to acquire BMs and who would be able to deploy a credible capability within approximately five years of the acquisition decision (ten years in the case of Iraq). The progress of the key proliferants is summarised in Table 2.

The three crucial factors which shape the emerging threat are deemed to be the reduced development time (with less emphasis on standards of missile accuracy, reliability and safety in comparison with traditional US and Soviet development standards); the increased availability of foreign technical assistance; and the increased ability and motivation to conceal the development programme. However, the inaccuracy of these new systems means that they are generally regarded as poorly suited for use against military targets and, since they are too expensive for developing countries to procure in sufficient quantities to compensate for inaccuracy, attacks on the population would provide the greatest strategic impact.

Notable examples of this form of intimidation include the Iran-Iraq ‘War of the Cities’ and Iraq’s 1991 Scud missile attacks against Saudi Arabia and Israel. The origins of both the technology and tactics can be traced to German V1 and V2 rocket attacks on London during the Second World War and illustrate that the political and psychological impact of BMs far outweighs the physical destruction caused. This factor is explored by Sheppard, in his analysis of BM proliferation, which focuses on the targeting of cities and the potential to exploit uncertainty about the use of WMD warheads as a psychological weapon. He argues that the subtlety behind a missile’s ability to exert terror is twofold:

‘…firstly, the suddenness or short warning time of an attack presents a sense of helplessness among civilians, especially those who are not protected by missile defences, and secondly the anxiety from the ambiguity surrounding the type of missile warhead being delivered.’\(^{83}\)

---


\(^{83}\) Sheppard, B., ‘Ballistic missile proliferation and the geopolitics of terror’ JIR (December 1998), 41.
### Table 2: Ballistic Missile Proliferation

<table>
<thead>
<tr>
<th>Country</th>
<th>Ballistic Missile</th>
<th>Range</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>North Korea</td>
<td>ICBM Taepo Dong 2 (TD-2)</td>
<td>4000 km†</td>
<td>Tested in August 1998 ‡ Based on scaled-up Scud technology</td>
</tr>
<tr>
<td></td>
<td>IRBM TD-1</td>
<td>1,500 km†</td>
<td>Assessed that lightweight variations of TD-2 could fly as far as 10,000 km</td>
</tr>
<tr>
<td></td>
<td>IRBM No Dong</td>
<td>1,300 km</td>
<td>Tested once in 1993</td>
</tr>
<tr>
<td>Iran</td>
<td>ICBM</td>
<td></td>
<td>Estimated that Iran has the technical capacity and resources to demonstrate an ICBM-range capability (similar to TD-2) within 5 years of decision to proceed.</td>
</tr>
<tr>
<td></td>
<td>IRBM Shahab-3</td>
<td>1,300 km</td>
<td>Test-fired in July 1998‡</td>
</tr>
<tr>
<td>Iraq</td>
<td>MRBM Scud Al Abbas</td>
<td>900 km</td>
<td>Iraq produced and then modified Scuds to produce these missiles. Expertise and some equipment/materials from this programme remain and provide a strong foundation for a revised BM programme</td>
</tr>
<tr>
<td></td>
<td>MRBM Scud Al Hussein</td>
<td>600 km</td>
<td></td>
</tr>
<tr>
<td>India</td>
<td>IRBM Agni-II</td>
<td>2,000 km</td>
<td>Test-fired in April 1999¥</td>
</tr>
<tr>
<td></td>
<td>IRBM Agni</td>
<td>1,500 km</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SRBM Prithvi/Prithvi II</td>
<td>150 km† 250 km†</td>
<td></td>
</tr>
<tr>
<td>Pakistan</td>
<td>IRBM Ghauri-II</td>
<td>2,300 km</td>
<td>Test-fired in April 1999; flew for 1,400 km although officials claim its potential range is 2,300 km¥</td>
</tr>
<tr>
<td></td>
<td>IRBM Ghauri/Hatf V</td>
<td>1,300 km 1,500 km‡</td>
<td>Version of North Korean No Dong (tested in April 1998)</td>
</tr>
<tr>
<td></td>
<td>SRBM M-11</td>
<td>350 km</td>
<td>Acquired from China</td>
</tr>
<tr>
<td></td>
<td>SRBM Tarmuk</td>
<td>350 km</td>
<td>(under production?) Based on M-11</td>
</tr>
</tbody>
</table>

Range:  
ICBM > 5,500 km.  
IRBM > 1,000 km.  
MRBM 500-1,000 km.  
SRBM < 500 km.  

SOURCE: ‘Rumsfeld Commission’ Report  
Notes in italics:  
† IISS Military Balance 1996.  
‡ JIR, December 1998.  
¥ The Economist 17 April 1999.

Notwithstanding recent dramatic advances in missile technology, adapting BMs for WMD-delivery continues to present considerable technical obstacles for developing countries; however, Sheppard observes that the psychological trauma of BMs, armed with chemical or biological weapon (CBW) warheads, derives from the mere threat or suggestion of use. He illustrates his case with casualty statistics from the conventionally-armed Scud attacks against Israeli cities during the Gulf War (Table 3), which illustrate that twenty-eight per cent of the total casualties could be attributed to the fear of CW attack, rather than to any direct injury.

---

Table 3:

84 ‘Special re-entry vehicles are required to prevent a CBW warhead being damaged by heat upon re-entering the Earth’s atmosphere. Furthermore, the agent must be correctly released at the right altitude and dispersed as an aerosol cloud in particles of adequate size to ensure significant lethality.’ *Ibid.*, 42.
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total War Casualties</td>
<td>773 Admitted to Israeli hospitals following BM attacks</td>
</tr>
<tr>
<td>Total Deaths</td>
<td>8 2 from direct hits</td>
</tr>
<tr>
<td></td>
<td>6 from gas mask asphyxiation</td>
</tr>
<tr>
<td>Indirect Injuries</td>
<td>208 falsely injected themselves with nerve agent antidote (Atropine)</td>
</tr>
<tr>
<td>Population Movements</td>
<td>14,000 Left Israel</td>
</tr>
<tr>
<td></td>
<td>100,000 Evacuated Tel-Aviv and Ramat Gan.</td>
</tr>
</tbody>
</table>

Source: JIR

Even though no country has yet launched a CBW missile attack, Israel implemented dramatic precautionary measures in anticipation of attacks during the February 1998 Gulf crisis, appropriating US$68 million to buy and distribute nerve gas antidotes, gas masks and protective equipment. This reaction highlights the dilemma facing governments whose response risks fuelling the fear when opponents threaten to use WMD - what matters is the perception of the populace, rather than the true intentions of the adversary; however, the implementation of precautionary measures inevitably heightens the population’s threat perception.

Overall, the threat or use of BMs offers a lucrative strategy for a rogue state seeking to deter, disrupt or defeat an intervention, especially where this includes the implicit threat of non-conventional strikes. Even without direct military participation, credible intimidation might deter a state from participating in a military coalition or from permitting military strikes to be launched from its territory. Alternatively, attacks on the population would have a dramatic and disruptive influence on the execution of an intervention, especially in circumstances of negligible national interest where public opinion could be expected to be less resilient. Finally, sustained attacks on large unprotected urban areas could coerce states into scaling down military involvement, or withdrawing altogether, particularly when the population is already demoralised.

**The Revolution in Military Affairs**

Like the expression ‘asymmetric warfare’, the acronym ‘RMA’ entered the international security lexicon in the wake of the Gulf War to reflect the realisation that:

‘...a growing range of targets has become almost irredeemably exposed to attack by “smart” weapons. The protection afforded by distance, size, terrain and weather has declined, a process accelerated through the application of information technology.’

However, the tendency to regard the recent qualitative developments in technological sophistication and capability as ‘The RMA’ is something of a misnomer, since the term was first coined in connection with the major changes in warfare that occurred in the sixteenth and seventeenth centuries. Indeed, the expression ‘military-technical

85 Ibid.
86 Ibid., 42.
88 Ibid., 7.
‘RMA-1’ represents the World War 1 (WW 1) technology associated with the internal combustion engine (the aeroplane, tank and submarine) and first generation telecommunications. This technology matured during WW 2, concurrent with the evolution of ‘RMA-2’, which describes the development of long-range bombardment and atomic energy, to create BMs based on German V1/V2 technology and NW. RMA-2 matured during the Cold War and gave rise to ‘RMA-3’ which represents current technology associated with silicon-based sensors, weapons and communications systems. According to Wilson’s thesis, the Gulf War illustrated that RMA-3 can defeat RMA-1, but not RMA-2, since the Coalition was able to decisively defeat Iraq’s air force and tank armies yet, despite total air supremacy.

---

unable to suppress the Scud missile system. Therefore, viewed from the opponent’s perspective, the logical challenge to RMA-3 is the acquisition of RMA-2 capabilities, and this suggests that future adversaries will seek to obtain BMs and NW. However, they may conclude that there are political and military risks associated with relying too heavily on such weapons and decide instead to acquire niche capabilities - selected high-tech sensors, communications and weapons systems - associated with RMA-3. In theory, this strategy would also provide a potential counter to ‘RMA-4’: the emerging space and nanotechnologies\textsuperscript{93} that the West is developing in order to defeat RMA-2.\textsuperscript{94}

In a paper prepared for the Office of the US Secretary of Defense,\textsuperscript{95} analysts at the ‘Foreign Systems Research Center’ investigated the asymmetric responses of less-developed nations (Iran, India) and concluded that they may seek to develop ‘asymmetric sufficiency’, in the form of a sea-denial strategy, as a counter to opponents who aim to exploit maritime power-projection.\textsuperscript{96} Of particular concern is the potential for small or medium powers to acquire anti-ship cruise missiles or subsurface weapons to target maritime HVA, including aircraft carriers and logistics ships.

**Cruise Missiles**

The extensive use of conventionally-armed cruise missiles during, and since, the Gulf War has led analysts to speculate that future adversaries may develop their own versions:

‘[They] may choose to mass-produce cruise missiles on a scale similar to that of the German V-1 program, which led to the production of thousands of weapons. Relying on GPS guidance and made of inherently low-observable materials (fiberglass), a new generation of V-1 may appear in many potential [Major Theater Wars].’\textsuperscript{97}

This concern is supported by the Stockholm International Peace Research Institute (SIPRI), which highlights a specific emerging challenge to US maritime supremacy:

‘…supersonic P-80/3M80 Moskit (SS-N-22 Sunburn) anti-ship missiles sought by China from Russia might deter or defeat US intervention on behalf of Taiwan and … Chinese anti-ship missiles transferred to Iran create new risks for forces in the Persian Gulf.’\textsuperscript{98}

Wilson notes that the USSR was developing a counter-carrier missile capability (SS-

\textsuperscript{93} Nanotechnology: ‘the branch of technology that deals with dimensions and tolerances of less than 100 nanometers (one thousand-millionth of a meter).’ \textit{The Concise Oxford Dictionary} (9\textsuperscript{th} Edition, Clarendon, Oxford, 1995) 903.

\textsuperscript{94} For an analysis of weapons research and future military projects see: Shukman, \textit{op. cit.}

\textsuperscript{95} Beck \textit{et al}, \textit{op. cit.}, iii, 50.

\textsuperscript{96} See footnote 11.

\textsuperscript{97} Wilson (1998), \textit{op. cit.}, 171.

N-13, based on a radar-guided ‘Manoeuvring Re-entry Vehicle’ (MaRV). Such a weapon, equipped with a GPS receiver and a high-performance auto-pilot, could be flown several thousand kilometres and land within a Circular Error Probable (CEP) of fifty meters, enabling opponents to attack exposed HVA during the opening phases of a military intervention. However, the utility of this system would depend on accurate targeting information and, for use against mobile assets such as shipping, ‘real-time’ imagery would be essential. The opponent who is able both to develop a MaRV capability, and access real-time intelligence from space-based reconnaissance platforms, would in theory be able to deny access to the sea-lanes. Alternatively, Uninhabited Aerial Vehicles (UAVs) represent a potentially more accessible source of real-time imagery, yet these are vulnerable to countermeasures:

‘…no matter how efficient [UAVs] might be, and no matter how long they could loiter using only solar power, anything inside the atmosphere is subject to counteraction … Even if they were able to travel to a target area, the data would have to be transmitted back to the launch site … Each of those links would have to be put into position and protected against jamming.’

Commercially-available satellite imagery would not offer the ‘real-time’ data necessary to locate mobile targets, but the opponent who exploits this intelligence source would nonetheless possess a potent capability to strike at static, land-based targets; particularly air bases and logistics depots.

Sub-Surface Weapons.

An alternative hypothesis argues that the probability of potential adversaries waging high-tech war against the advanced military powers is small, since few nations possess the necessary fiscal, technological or operational resources to achieve such capabilities. The American officer and noted speaker and writer on US national security issues - Colonel Charles Dunlap - argues that future adversaries are more likely to combine available low-tech equipment with a culturally-orientated strategy; he posits an asymmetric approach which seeks to exploit the West’s casualty sensitivity by causing losses which would, in turn, erode support for the military effort. This could include the use of mines, which proved to be a factor in the decision not to mount an amphibious assault on Kuwait, during the Gulf War, following damage to the USS Tripoli and the USS Princeton. Alternatively, the acquisition and deployment of submarines, with the sole motive of sinking a maritime HVA would present a similar threat; indeed, the British experience during the 1982 Falklands Conflict illustrates the disruptive potential of submarines and it may only be necessary to reveal a presence, or inflict minor damage, before the sea-lanes are...
declared impassable.\textsuperscript{104}

**Clandestine Operations**

An alternative method of targeting HVA is to engage in clandestine operations using SPF; moreover, since much of the emerging military technology is both accessible and affordable, this creates the potential for nations to dramatically increase the lethality of small military units. This challenge is explored by Shlapak and Vick, in their RAND paper on the evolving ground threat to USAF Bases\textsuperscript{105} and, whilst the focus of this paper is specifically the vulnerability of air power assets, it is evident that many of the conclusions are applicable to any static HVA (particularly ports or logistics depots). The RAND paper is based on Vick’s historical analysis of ground attacks on air bases between 1940-1992\textsuperscript{106}, which establishes that such attacks occurred at least 645 times in ten separate conflicts, destroying or damaging over 2000 aircraft. Whilst only three per cent of attacks penetrated the base perimeter, seventy-five per cent exploited stand-off attacks (small units launching weapons from outside the perimeter) and twenty-two per cent employed both techniques.\textsuperscript{107} The paper concludes that extremely unsophisticated opponents are likely to continue to rely on penetrating attacks, particularly where perimeter defences are weak; however, the increasing commercial availability and affordability of military technologies dramatically increases the vulnerability of static HVA to the stand-off threat:

‘…new technologies, weapons and precision munitions may give small standoff attacks a consistent lethality, which they lacked in the past.’\textsuperscript{108}

Global news reports, plus commercial satellite imagery and geographical information services, enable attackers to determine force deployments; whilst traditional human intelligence (‘humint’) sources, employing night-vision devices and thermal sensors, can provide detailed target information on base defences and operating routines. Mission plans can be constantly updated using cellular and satellite communications and ‘notebook’ computers; and small units are able to exploit a range of weapons optimised for stand-off attacks:

‘…the most promising technologies are PGMs for mortars, large-calibre sniper rifles, man-portable anti-tank guided missiles (ATGMs), fiber-optic-guided missiles (FOG-M), and man-portable surface-to-air missiles (e.g., MANPADS).’\textsuperscript{109}


\textsuperscript{105} Shlapak and Vick, \textit{op. cit.}


\textsuperscript{107} Shlapak & Vick, \textit{op. cit.}, 21, 34.

\textsuperscript{108} \textit{Ibid.}, 35.

\textsuperscript{109} \textit{Ibid.}, 49. For a detailed analysis of emerging ‘stand-off’ weapon technologies see 49-54.
Figure 5 depicts a notional ‘stand-off footprint’ - the extensive area beyond a base perimeter - from which munitions may be launched or fired against targets within (or aircraft approaching/departing) the base; this illustrates that defending against, and defeating, the threat from the opponent who engages in clandestine operations requires defence forces to dominate an extensive area ‘outside the wire’. Therefore, the extended range and lethality of advanced weapons, combined with the increased dependence on scarce, HVA, means that intervention forces will become increasingly reliant on dedicated, specially trained and equipped defence forces to dominate the extensive stand-off footprint around vital facilities.

110 Ibid., 59.
CHAPTER IV: NON-MILITARY ASYMMETRIC CHALLENGES

Technological Approaches

Strategic Information Warfare

As the continuous flow of secure communications across the battlespace has become the key priority of strategic and tactical planning, ‘information’ has emerged as the modern force multiplier. However, the information revolution has also led to claims of an unprecedented security risk in the form of SIW, which potentially permits opponents to exploit information as a ‘weapon of mass disruption’. In 1998, CIA director George Tenet identified SIW as an ideal asymmetric strategy for the weaker state:

‘These countries recognise that cyber attacks….against [military or] civilian computer systems in the US represent the kind of asymmetric option they will need to “level the playing field” during an armed crisis against the United States.’

Definitions are elusive and, in his 1995 paper for the USNDU’s ‘Center for Advanced Concepts and Technology’, Libicki observes that there is a tendency for single constituencies to champion individual aspects of IW, which then assume the role of the entire concept and become grossly inflated in importance. Libicki identifies seven distinct forms of IW which are summarised in Table 4; these are command-and-control warfare (C2W), intelligence-based warfare (IBW), electronic warfare (EW), psychological warfare (PSYW), hacker warfare, economic information warfare (E IW), and cyberwarfare. Of these, ‘cyberwarfare’ is arguably the most fictitious, yet the term is widely used as a synonym of IW in its broadest sense.

Libicki argues that the global information infrastructure has yet to evolve to the point where many of these forms of warfare are possible, noting that ‘such considerations are akin to discussions in the Victorian era of what air-to-air combat would be.’ However, there is consensus in the contemporary literature on the two principle threats: first, the potential vulnerability of military C4ISR networks to what Libicki defines as ‘hacker attack’; and second, the vulnerability of the NSI to IW attacks designed to disrupt military power-projection or distract the political leadership from national security duties.

112 ‘CIA chief fears “cyber attacks”’, BBC On-line, (published at 05.05 GMT 25 June 1998).
113 Libicki, op. cit., 3.
114 Ibid., 75.
Table 4: Information Warfare Techniques

<table>
<thead>
<tr>
<th>Form</th>
<th>Subtype</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Anti-neck</td>
<td>Severs links between C2 ‘head’ and fielded military forces (‘body’).</td>
</tr>
<tr>
<td>IBW</td>
<td></td>
<td>Targets ISR systems that sense the battlespace and disseminate results</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(i.e. AWACS, JSTARS).</td>
</tr>
<tr>
<td>EW</td>
<td>Anti-radar</td>
<td>Either by jamming or direct attack using High-speed Anti Radiation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Missiles (HARM).</td>
</tr>
<tr>
<td></td>
<td>Anti-communications</td>
<td>i.e. ‘Spoofing’ (substituting deceptive messages for valid ones).</td>
</tr>
<tr>
<td>Cryptography</td>
<td></td>
<td>Code-making/breaking.</td>
</tr>
<tr>
<td>PSYW</td>
<td>Anti-will</td>
<td>Propaganda using global media/Direct-Broadcast Satellites (DBS); based</td>
</tr>
<tr>
<td></td>
<td></td>
<td>on ‘the iron fist in a velvet glove’.</td>
</tr>
<tr>
<td></td>
<td>Anti-troop</td>
<td>Instil fear of death among fielded forces/resentment ‘between the trench</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and the castle’.</td>
</tr>
<tr>
<td></td>
<td>Anti-Commander</td>
<td>‘Nothing so much suggests the imminence of defeat than confused and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disorientated commanders’.</td>
</tr>
<tr>
<td>Hacker</td>
<td>Warfare</td>
<td>Penetrating computer networks using ‘Computer Malicious Codes’ (CMCs)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in order to read, distort or destroy vital information.</td>
</tr>
<tr>
<td>EIW</td>
<td>Economic (Information)</td>
<td>Blocking (or restricting access) to high bandwidth information flows</td>
</tr>
<tr>
<td></td>
<td>Blockade</td>
<td>which facilitate global commerce.</td>
</tr>
<tr>
<td>Cyber</td>
<td>Info-Terrorism</td>
<td>Terrorists using information means to achieve their goals.</td>
</tr>
<tr>
<td>warfare</td>
<td>(‘cyber-terrorism’)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Semantic Attack</td>
<td>Unlike ‘hacker attack’ which produces random or systematic failures and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>systems cease to operate, a system under ‘semantic attack’ will be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>perceived as operating correctly but will generate answers at variance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with reality.</td>
</tr>
<tr>
<td></td>
<td>Simula-warfare</td>
<td>‘Virtual Reality’ warfare; based on the premise that fighting a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>simulated war could prove to the enemy that it would lose.</td>
</tr>
<tr>
<td></td>
<td>‘Gibson’ Warfare</td>
<td>The stuff of science-fiction (named after William Gibson’s movie</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Neuromancer).</td>
</tr>
</tbody>
</table>

Source: US National Defense University

Ibid., 87-89.
Military C4ISR Systems

Since most military C4ISR networks, including all satellite communications systems, are computer-operated (and therefore software-based) they are vulnerable to ‘hacking’, enabling potential opponents to read, distort or destroy vital information. Lorenzo Valeri, of the ‘International Centre for Security Analysis’ (ICSA)\(^\text{116}\) argues that the dependence on computer systems and information networks represents not only the strength of today’s military forces but also their major weakness; he notes that ‘[t]his may be exploited by the enemy through a new kind of weapon: computer malicious codes (CMCs).’\(^\text{117}\) CMCs include the *virus*, *worm*, *Trojan Horse*, *logic bomb* and *trap door*\(^\text{118}\) which become effective weapons when inserted inside the target’s computer or information networks through direct or indirect coupling. Direct coupling requires the CMC to be manually inserted which, although relatively prevalent in the commercial sector, presents a lower risk in military installations. However, a more realistic threat is the insertion of CMCs through the least defended links of tactical or strategic information networks, such as phone switches and defence-industrial sites, and this risk is increasing as governments strive towards greater integration of computer networks.

Military vulnerability to CMC attack would depend on the enemy’s potential goals which might include deception, through the targeting of data management systems; disruption, to create confusion and loss of trust in an information infrastructure; or the elimination of the opponent’s information superiority. There is a growing body of evidence which supports concerns of an emerging IW threat. In February 1999, British security sources confirmed that hackers had intercepted the link between the control centre and the ground station for one of their *Skynet* military communication satellites, and had managed to reprogramme a satellite control system.\(^\text{119}\) The following month the US Deputy Defense Secretary, John Hamre, reported that the Pentagon’s military computer systems were being subjected to ongoing, sophisticated and organised IW attacks.\(^\text{120}\) Two previous incidents, in 1994 and 1998, were subsequently attributed to teenage hackers;\(^\text{121}\) however, according to the ‘Center for Strategic and International Studies’ (CSIS), the second incident disrupted troop deployments to the Gulf in February 1998 and was so expertly conducted that President Clinton was warned in the early phases that Iraq was most probably the attacker.\(^\text{122}\) Therefore, although crucial military systems are supposed to be designed

\(^{116}\) The ICSA is a consultancy research arm of the Department of War Studies, Kings College London.
\(^{118}\) For an explanation of these terms see *Ibid.*, 380.
\(^{121}\) In 1994, a 16 year-old English boy gained access to US Air Force systems and a network owned by the missile and aircraft manufacturer *Lockheed*. See Graves, D., ‘CIA thought British computer boy was more harmful than the KGB’ *Daily Telegraph*, (22 March 1997). In 1998 an 18 year-old Israeli reportedly infiltrated the Pentagon’s systems, NSA and a NW research laboratory. Cilluffo, *et al*, *op. cit.*, foreword.
\(^{122}\) This was confirmed by The Pentagon on 25 February 1998: ‘The Pentagon said yesterday it was concerned that hackers who had infiltrated its computer systems in the last two weeks may have been waging “information warfare” on behalf of Iraq.’ Uhlig, R., ‘Hackers renew “cyber terrorism” fears’ *Daily Telegraph*, (26 February 1998).
with sufficient security and redundancy to defeat such attacks, it is evident that even low-level hacking can have strategic effects out of all proportion to its complexity or intended outcome.

National Strategic Infrastructure

Wilson observes that the modern armies of the industrial democracies are characterised by their rising dependence on the civilian infrastructure for power-projection and support for military operations; thus, even if the C2 system is secure, the military may be vulnerable to other forms of interference.\textsuperscript{123} Aside from attacks designed to disrupt military operations, IW could be directed at the NSI in order to disrupt the deployment of military forces or to undermine coalitions:

‘The possibility exists that a regional adversary might use SIW threats or attacks to deter or disrupt US power projection plans in a regional crisis. Targets of concern include infrastructures in the United States vital to overseas force deployment, and comparable targets in allied countries. A key ally or coalition member under such attack might refuse to join a coalition - or worse, quit a coalition in the middle of a war.’\textsuperscript{124}

This analysis is based on a 1996 RAND study, commissioned by the US Secretary of Defense, into the range of potential national security issues related to the concept of IW. The study found that:

‘The United States has substantial information-based resources, including complex management systems and infrastructures involving the control of electric power, money flow, air traffic, oil and gas and other information-dependent items. US allies and potential coalition partners are similarly increasingly dependent on various information infrastructures. If and when potential adversaries attempt to damage these systems using IW techniques, information warfare inevitably takes on a strategic perspective.’\textsuperscript{125}

The RAND studies established that many existing information systems are vulnerable to some level of disruption or misuse, although ‘...developments in cyberspace are so dynamic that existing vulnerabilities may well be ameliorated as part of the natural building of immunities to threats that accompany any such rapidly evolving entity.’\textsuperscript{126} The solution appears to lie in the identification of the minimum essential information infrastructure (MEII) whose protection would permit the conduct of essential military and governmental activities, even if the country were subjected to a massive and sustained IW attack. However, just as their dependence on information systems is increasing, governments do not currently possess the capability to determine whether the source of a particular attack is a foreign power, a mischievous hacker, or even a hacker unwittingly acting on behalf of someone with hostile intentions.

\textsuperscript{123}Wilson, (11 May 1999), op. cit.
\textsuperscript{125}Molander, R.C., Riddile, A.S., Wilson, P.A., Strategic Information Warfare: A New Face of War (RAND, National Defense Research Institute, 1996), xiii.
\textsuperscript{126}Ibid., xviii.
**Unconventional Approaches**

At the opposite end of the cultural spectrum is the opponent who perceives his advantages not in terms of technological capabilities, but in exploiting what the Western mindset sees as its virtue: its liberal-democratic system which emphasises moral strengths and ethical standards as the foundations of legitimacy in military intervention. A substantial contribution to the topical literature is made by Dunlap, who perceives cultural distinction, and a disparate emphasis on ‘legal compliance’, as the dominant asymmetries in contemporary conflict; he asserts that ‘…adversaries willing to abandon Westernised legal and ethical regimes may well consider them as things to exploit and manipulate.’ The widely televised ‘cockpit-video’ footage from the Gulf War, portraying the unprecedented accuracy of PGMs, coupled with ethical demands that civilians must be deemed innocent unless proven guilty, has contributed to a public intolerance of ‘collateral damage’. Following the end of the Cold War this particular aversion was exploited by Somali Warlords, Libya, Iraq and Serbia, through their use of innocents as ‘human shields’, and illustrates how ‘moving the collateral to the target’ represents the obvious and direct ‘low-tech’ counter to precision weaponry. This strategy is designed to present the military commanders with moral conundrums which complicate efforts to mount effective attacks, and it increasingly involves the concealment of military assets in populated areas or adjacent to ‘high-value collateral’, such as schools, hospitals and religious buildings. Alternative PGM countermeasures include the dispersal of military assets into small, mobile combat teams that combine only when required to strike a common objective; or, the simple avoidance of presenting any militarily significant targets through the use of comprehensive camouflage, concealment and dispersal (CCD) techniques. This simple, yet unconventional approach is particularly effective in extending the time-line of a military operation, exploiting public impatience for a swift resolution whilst increasing the probability of errors which generate adverse political impact. Alternative approaches have included the use of military hostages,

---


129 Somali Warlords used women and children as human shields against coalition forces during the intervention of the early 1990s; Libyans threatened to encircle a facility, alleged to be involved with the production of WMD, with ‘millions of Muslims’ in order to deter Western attacks; and Saddam Hussein surrounded his palaces and other buildings with non-combatant civilians during the threatened, and subsequent Anglo-US air strikes in 1998 (see Dunlap, (1998) *op. cit.*, 8). Subsequently, Belgrade Serbs, wearing ‘target’ patches, lined the main bridges to deter NATO air strikes on the City during the 1999 Kosovo Conflict. See Simpson, J., ‘Nato “giving Serbs air raid tip-offs to cut casualties”’, *The Sunday Telegraph* (11 April 1999).

130 Following the 1999 Kosovo conflict it became evident that much Serbian equipment had been successfully hidden from sophisticated Nato surveillance by camouflage techniques. See Hibbs, J., ‘Tories call for inquiry into bomb damage’ *The Daily Telegraph* (25 June 1999).

131 This danger was highlighted by the mistaken NATO attacks on Albanian refugee convoys in Kosovo on 14 April 1999. See Rooney, B., Helm, T., Laville, S., ‘Our planes bombed refugee convoy, admits Nato’ *The Daily Telegraph* (15 April 1999).
such as downed aircrew or peacekeeping troops as human shields\textsuperscript{132}, and the use of innocents in an attempt to escalate the conflict by destabilising neighbouring countries through enforced refugee movements.\textsuperscript{133} An emerging concern is that future opponents will exploit the West’s operational emphasis on air power and armoured ‘manoeuvre’ warfare, by luring their forces into fighting in environments which degrade the capacity to locate and attack militarily significant targets; in particular, urban, jungle or mountainous areas which present specific problems associated with the reliance on electronic C4ISR. Moreover, urban targets present the added risk of collateral damage which can also be exploited for psychological operations (‘psy-ops’) by manipulating global news media.\textsuperscript{134}

\textbf{Atrocities}

Whilst traditional ‘unconventional approaches’ blur the boundaries between actions viewed as warfare and those considered crimes, events in Somalia in 1993 remind us that military interventions may face enemies who are prepared to commit atrocities in order to exploit their opponent’s casualty sensitivity and the ‘asymmetry of stake’.\textsuperscript{135} This is explored by Peters, in his analysis of ‘The New Warrior Class’, in which he questions the developed powers’ military and political strength of will to defeat an enemy who has nothing to lose:

‘When we face warriors, we will often face men who have acquired a taste for killing, who do not behave rationally according to our definition of rationality, who are capable of atrocities that challenge the descriptive powers of language, and who will sacrifice their own kind in order to survive.’\textsuperscript{136}

This theme is developed by Dunlap in a creative account, influenced by his own military service in Somalia, which describes a future American defeat at the hands of a ‘warrior society’. \textit{How We Lost the High-Tech War of 2007}\textsuperscript{137} describes a new form of conflict which Dunlap defines as “neo-absolutist war”:

‘...a vicious form of confrontation that extends across the spectrum of warfare. It differs from more traditional “total war” by, among other things, the propensity of the aggressor to focus on shattering the will of an opponent by

\textsuperscript{132} In May 1995 Bosnian Serbs captured some 370 UN personnel as prisoners of war and chained some to possible targets of NATO air-strikes throughout Serb-held territory. See: ‘British put on TV by Serb army: UN captives labelled ‘prisoners of war’ as injured soldiers are shown in Bosnian hospital’ \textit{The Daily Telegraph} (30 May 1995).

\textsuperscript{133} The intensified Serb ‘ethnic cleansing’ of Kosovo Albanians, following the commencement of NATO Air Strikes in March 1999, led to widespread media speculation that the resulting mass exodus into Albania and Macedonia was engineered by the Serbian regime in order to destabilise the region. See Jones, G., ‘Nato set to intensify attacks’ \textit{The Daily Telegraph} (30 March 1999).

\textsuperscript{134} According to US psy-ops specialists this strategy was employed by Serbia, during the 1999 Kosovo conflict: following the onset of NATO air strikes in March 1999 the Serbian regime hired a French public relations company which (among other things) was responsible for producing the image of the Eiffel Tower, shattered and ablaze, which adorned bill-board hoardings in Belgrade and whose photograph was depicted in the international media. (Cited by Gouré, (5 May 1999) \textit{op. cit.}).

\textsuperscript{135} See footnote 9.


\textsuperscript{137} Dunlap, (1996a) \textit{op. cit.}.
employing brutality openly and unapologetically against combatants and non-combatants alike.’

Dunlap identifies a number of characteristics of the West’s contemporary warfighting procedures, which present certain comparative advantages to warrior societies: particularly that their populations are inherently more casualty tolerant and better able to endure deprivation; their military forces have more austere logistical and support requirements; and they are fundamentally unconstrained by international legal conventions. Based on his own definition of asymmetrical warfare - ‘…an approach that tries to focus whatever may be one side’s comparative advantages against its enemy’s relative weaknesses’ - Dunlap draws on the public reaction to the media portrayal of the brutal treatment of US servicemen in Mogadishu, and projects that the strategy of the warrior society will ‘…capitalize on television’s power to influence decisionmakers by aiming to wage war in the most brutish - and public - way.’ In particular, he focuses on the contemporary debate concerning the role of women in combat and the apprehension connected with their vulnerability to abuse in captivity:

‘However prepared the Americans thought they were to see their daughters come back in body bags, they were not ready to see them returned home strapped to wheelchairs, horribly mutilated, and shrieking in agony.’

This account also discusses the potential for opponents to broadcast images of abuse and torture of POWs, exploiting video and the internet, with the intention of making continued use of force so psychologically costly that the intervening power would lose its will to win. However sensationalised Dunlap’s account, this strategy has a chilling precedent in the events surrounding the execution of President Samuel Doe, during the 1990 Liberian coup: following the event, guerrilla leader Prince Johnson circulated a video throughout West Africa which depicted him cutting Doe’s ears off before the President was tortured to death. Finally, an alternative approach could exploit environmental and health sensitivities, through the deliberate contamination or pollution of the environment, or the targeting of unprotected agriculture and livestock. Again, there is some precedent in the burning of the Kuwaiti oilfields, prior to Iraq’s defeat in 1991, and the intense media attention concerning ‘Gulf War Syndrome’ illustrates the degree of public concern about the health and well-being of military personnel engaged in interventionary operations. However, Daniel Gouré, of the CSIS, urges a note of caution concerning the unpredictable response that physical or environmental atrocities are likely to generate:

‘... if our interests are minimal and there is a limited sense of progress we might disengage. However, if we felt that our interests really were engaged, or if the

138 Dunlap acknowledges that brutality has characterised warfare throughout history but argues that information-age technology modernises it (hence the term ‘neo’). Dunlap, (1996b) op. cit.
139 Dunlap in Matthews (ed.), op. cit., 1.
141 Ibid., 26.
adversary had demonstrated himself to be a great threat to mankind, the backlash could be severe.'

State-Sponsored Terrorism

Goverments have long engaged in the systematic use of terror to overcome both domestic and foreign enemies; however, Hoffman distinguishes between historical examples and the type of state-sponsorship that has emerged since the early 1980s, arguing that:

‘…some governments have now come to embrace terrorism as a deliberate instrument of foreign policy: a cost-effective means of waging war covertly, through the use of surrogate warriors or “guns for hire” - terrorists.'

Despite an overall decline in terrorist incidents, Figure 6 illustrates that there has been a substantial increase in the number of fatalities, and this trend has led analysts to talk of Catastrophic Terrorism - which describes an event where the resulting horror and chaos would exceed all historic precedent. The precedent for the terrorist use of WMD was set with the 1995 Sarin nerve gas attack on the Tokyo subway, by the Aum Shinrikyo religious cult; however, conventional terrorism could equally achieve catastrophic impact and investigators believe that the bomb which damaged New York’s World Trade Center, in 1993, was intended to make one tower collapse onto another, killing up to 250,000. Few terrorist groups have shown an interest in inflicting true mass destruction, although it is less clear whether this limitation has been due to a powerful underlying reason or a simple lack of capability. Nevertheless, the trend of increased lethality, combined with the impact of domestic casualty sensitivity, makes terrorism a potentially lucrative weapon for rogue states who seek to deter military intervention or intimidate traditional allies into distancing themselves from the intervening power.

143 Gouré, (5 May 1999), op. cit.
146 Cameron, G., ‘Nuclear Terrorism: a real threat?’ JIR (September 1996), 425.
**Nuclear Terrorism.** There have been no recorded instances of terrorists resorting to NW for mass destruction; nevertheless, in 1994 the Director General of the UK’s MI5 intelligence agency stated that:

‘Some two dozen governments are currently trying to obtain such technology. A number of these countries sponsor or even practise terrorism and we cannot rule out the possibility that these weapons could be used for that purpose.’\(^ {149}\)

In the FSU, the poor security of fissile materials - combined with the disenchantedm of industry and military staff with the deterioration in standards of living, budgets and social status - presents considerable potential for rogue states or non-state actors to exploit the availability of personnel and materials. Moreover, Russia’s former national security chief, Alexander Lebed, prompted anxiety when he claimed in 1997 that 100 mini-nuclear ‘suitcase bombs’ had gone missing.\(^ {150}\) There are parallel fears over the security of industrial-grade fissile material, which is adequate for use in a ‘dirty bomb’ - a conventional device with a highly radioactive content - and there is evidence that this low-level nuclear terrorism is already a reality.\(^ {151}\) Overall, NW are unlikely to be the WMD of choice for non-state groups, since they require huge investments and infrastructure and, as Cameron observes:

‘…sponsoring states would have to be completely certain of plausible deniability in perpetuity for any terrorist attack since the repercussions from states that have been the victim of an act of nuclear terrorism could be immense.’\(^ {152}\)

---

\(^{149}\) Rimmington, S., cited in Cameron, *op. cit.*, 424.
\(^{150}\) ‘The New Terrorism’ *op. cit.*, 18.
\(^{151}\) On 23 November 1995, Chechen guerrilla leader, Shamyl Basayev, attempted ‘nuclear blackmail’ against the Moscow authorities, after concealing a case of radioactive *caesium* in the city. Cameron, *op. cit.*, 425.
Although, the increased availability of fissile material may have little impact on the likelihood of a terrorist nuclear bomb attack, it has made the feasibility and thus the credibility of a nuclear threat or hoax a much more realistic possibility.

**Chemical Terrorism.** There are two recorded terrorist attempts at mass destruction using CW: first, following the 1993 World Trade Center bombing, unconfirmed evidence emerged that the perpetrators had added sodium cyanide to the bomb, but that the high energy of the explosion rendered the chemical harmless;\(^\text{153}\) then, in 1995, the Sarin nerve-gas attack on the Tokyo subway which killed 12 and left 5,500 injured. This attack was undoubtedly intended to inflict far greater casualties and investigators later discovered that the sect possessed a substantial chemical stockpile. Nevertheless, in his analysis of CW proliferation, Croddy argues that three key restraints limit the terrorist use of such weapons: first the potential political backlash against any organization that employs such a reviled form of weaponry; second, contrary to media accounts, the manufacture of CW agents remains costly and difficult; and third, CWs are extremely difficult to store and handle, even by well trained military personnel.\(^\text{154}\) Moreover, it remains difficult for a terrorist group to accumulate a sufficiently large chemical stockpile for a credible attack without arousing suspicion, and the creation of near instantaneous casualties (unlike BW) would aid the authorities in mounting an effective emergency response, thus reducing the potential strategic impact of CW terrorism.

**Bio-terrorism.** In his 1997 paper on *The Threat of Bioterrorism*, Carus\(^\text{155}\) observed that:

‘[w]hile some terrorist groups had explored biological weapons as a potential tool, only a handful had attempted to actually acquire agents and even fewer tried to use them. Yet there is strong reason to worry that bioterrorism could become a much greater threat.’\(^\text{156}\)

Unlike CW, bioterrorism requires only minute amounts of biological agent to inflict many thousands of casualties, whose symptoms might not take effect for several days, and this creates a difficulty of attribution for attacks whose consequences would not materialise until long after the attacker had escaped the vicinity. A 1993 study by the ‘US Office of Technology Assessment’ claims that a single aeroplane, delivering 100 kilograms of anthrax spores by aerosol over the Washington, D.C. area, could kill between one million and three million people - three hundred times as many fatalities as if the plane delivered Sarin gas in amounts ten times larger.\(^\text{157}\) However, Tucker - of the ‘CBW Non-proliferation Program’ at the Monterey Institute of International Studies - argues against the media-generated hyperbole that has become associated with this threat, pointing out the significant difficulties of developing sufficiently

\(^{153}\) Reported by US District Judge Kevin Duffy; cited in Croddy, E., ‘Putting the lid back on the chemical box’ *JIR* (January 1998), 43

\(^{154}\) Croddy, *op. cit.*, 43.

\(^{155}\) Dr W Seth Carus is a visiting fellow at the USNDU’s Center for Counter-proliferation Research.


\(^{157}\) Betts, *op. cit.*, 32.
virulent strains, coupled with the technological obstacles associated with weaponisation and delivery.\footnote{158}

**Conventional Terrorism.** Empirical evidence suggests that terrorists do not need to resort to WMD to achieve their objectives and Cameron notes that conventional weaponry is cheaper, easier to obtain, harder for the authorities to detect, and probably safer to use given most terrorist’s unfamiliarity with non-conventional weapons.\footnote{159} The large number of recent terrorist incidents using ammonium nitrate fertiliser and fuel oil (AN/FO) explosives (see Table 5) illustrates that this home-made explosive is particularly attractive because it is cheap, relatively stable, and there is currently no way to trace or render impotent the common ingredients used in this type. However, there have also been a number of devastating terrorist bomb attacks using commercial or military-class high explosives and Semtex was used by suspected Libyan terrorists in the 1988 bombing of PAN AM Flight 103 over Lockerbie; by the PIRA in their bombings of London’s Baltic Exchange (1992) and Bishop’s Gate financial district (1993); and by radical Islamist terrorists in the 1996 bombing of the Khobar Towers military housing complex in Dhahran, Saudi Arabia.

<table>
<thead>
<tr>
<th>Date</th>
<th>Target</th>
<th>Explosive</th>
<th>Casualties</th>
</tr>
</thead>
<tbody>
<tr>
<td>1990</td>
<td>IRS Building, California, USA</td>
<td>Ammonium Nitrate/fuel oil (AN/FO)</td>
<td>(No detonation)</td>
</tr>
<tr>
<td>1993</td>
<td>World Trade Center, New York, USA</td>
<td>AN/FO</td>
<td>6 killed</td>
</tr>
<tr>
<td>1994</td>
<td>Buenos Aires, Argentina</td>
<td>AN/FO</td>
<td>1 killed</td>
</tr>
<tr>
<td>1994</td>
<td>Bangkok, Thailand</td>
<td>AN/FO</td>
<td>(No detonation)</td>
</tr>
<tr>
<td>1995</td>
<td>Oklahoma City, USA</td>
<td>AN/nitromethane</td>
<td>168 killed</td>
</tr>
<tr>
<td>1995</td>
<td>Skopje, Macedonia</td>
<td>AN/?</td>
<td>1 injured</td>
</tr>
<tr>
<td>1995</td>
<td>Algeria</td>
<td>AN/?</td>
<td>5 killed</td>
</tr>
<tr>
<td>1995</td>
<td>Reno, Nevada, USA</td>
<td>AN/FO</td>
<td>(No detonation)</td>
</tr>
<tr>
<td>1996</td>
<td>West Virginia, USA</td>
<td>AN/nitromethane</td>
<td>(No detonation)</td>
</tr>
<tr>
<td>1996</td>
<td>London, UK</td>
<td>AN/FO</td>
<td>(No detonation)</td>
</tr>
<tr>
<td>1996</td>
<td>Zamboanga City, Philippines</td>
<td>AN/?</td>
<td>(No detonation)</td>
</tr>
<tr>
<td>1996</td>
<td>San Borja, Peru</td>
<td>AN/FO</td>
<td>10 injured</td>
</tr>
<tr>
<td>1996</td>
<td>Barrancabermeja, Columbia</td>
<td>AN/?</td>
<td>1 killed, 2 injured</td>
</tr>
</tbody>
</table>

The chronology of attacks against American and European Embassies and overseas’ bases (Table 6) testifies that the intrinsic level of physical violence associated with this form of attack, combined with the potential for high casualty numbers, makes conventional terrorist bombings a potent means of creating a strategic event.

\footnote{158} Tucker, J., cited in Venter, *op. cit.*, 47.  
\footnote{159} Cameron, *op. cit.*, 425.  
\footnote{160} Ibid., 42.
<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Occurrence</th>
<th>Casualties</th>
</tr>
</thead>
<tbody>
<tr>
<td>1965</td>
<td>Saigon</td>
<td>Viet Cong terrorist explodes a car bomb outside the American Embassy.</td>
<td>20 killed including 2 Americans</td>
</tr>
<tr>
<td>1983</td>
<td>Beirut</td>
<td>Suicide bomber driving a yellow Mercedes truck packed with explosives destroys a United States Marine temporary barracks.</td>
<td>241 American servicemen killed more than 80 injured</td>
</tr>
<tr>
<td>1983</td>
<td>Kuwait City</td>
<td>Islamic fundamentalist sets off bombs outside American and French Embassies</td>
<td>6 killed and dozens wounded</td>
</tr>
<tr>
<td>1995</td>
<td>Riyadh</td>
<td>Car bomb attack on a temporary American training facility</td>
<td>5 Americans killed</td>
</tr>
<tr>
<td>1996</td>
<td>Dhahran</td>
<td>Truck bomb explodes outside United States Air Force housing complex</td>
<td>19 killed, 500 injured</td>
</tr>
<tr>
<td>1998</td>
<td>Nairobi</td>
<td>Simultaneous car bomb attacks on American Embassies</td>
<td>260+ killed including 12 Americans.</td>
</tr>
<tr>
<td></td>
<td>Dar es Salaam</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Newsweek\textsuperscript{161}

\textsuperscript{161} ‘Terror Times Two’ \textit{Newsweek} (17 August 1998), 20.
CHAPTER V: RISK ANALYSIS

Introduction

This Chapter explores the pragmatic (rather than possible) strategies that a small or weak power is likely to seek in order to prevent a superior challenger from intervening militarily in its affairs. This is based on an analysis of the relative utility of deterrence, disruption, exhaustion, attrition and coercion at each stage of an intervention, and examines the asymmetric approaches that provide the optimum capabilities with which to fulfil these motives.

Deterrence

Prior to the assembly and deployment of a coalition (or unilateral) intervention, the opponent’s main effort would be applied to the acquisition of capabilities which offer the maximum deterrence value; measures intended to raise the ‘entry price’ of military action beyond that which participating states would be willing to pay, such that the challenger would restrict its engagement to political, diplomatic or economic sanctions, rather than resorting to the use of force. This strategy is likely to be based on intimidation, through the threatened use of force, in order to deter states from participating in the opposing coalition or from permitting military strikes to be launched from their territory.

Plausible deterrent threats demand the ability to inflict unacceptable levels of damage upon the opponent, and the optimum capability with which to guarantee such threats is the possession of NW together with a credible delivery system. The value of NW in Great Power deterrence theory is broadly accepted; however, in his 1997 article on nuclear proliferation and interstate security relationships, Preston argues that in future even small nuclear states will be able to deter Great Power threats because of four critical lessons demonstrated by the Gulf War:

‘(1) the effectiveness and survivability of covert nuclear weapons programs; (2) the effectiveness and survivability of small state delivery systems; (3) the ineffectiveness of strategic defense systems in intercepting potential attacks; and (4) the fact that threats of unconventional weapons use by small states are taken seriously by Great Powers.’

However, nuclear threats against Great Powers would appear credible only when small state central interests are critically threatened, and there is some tension between the deterrent value of credible nuclear threats and the equally credible counter-threat of massive retaliation in kind. An alarming scenario is described by Gouré as ‘The three nuke problem’, whereby the small nuclear power invests in a

---

162 Russia and China’s large nuclear arsenals are frequently cited as one explanation for the West’s failure to take a more robust stance against alleged human rights abuses in Chechnya and Tibet. See: Johnson, B., ‘Cold War warrior [Henry Kissinger] scorns “new morality”’ The Daily Telegraph, (28 June 1999).
163 Preston, op. cit., 79.
164 Ibid., 91.
deterrent capability with no intention of attempting to fight and win a nuclear war.\textsuperscript{165} The first weapon is detonated to demonstrate the capability; as Libicki observes:

‘Had the United States possessed more nuclear weapons during World War II, it might have chosen to light the first off Tokyo harbor for effect rather than in Hiroshima for results.’\textsuperscript{166}

If absolutely necessary, the second weapon would be used against a ‘legitimate’ military target, to demonstrate intent, and the third to threaten an attack on an unprotected urban area. Although a high risk strategy, this relies on the calculation that the Great Power would not be prepared to risk even one city by relying on the threat of massive nuclear retaliation, particularly if it doubted its ability to locate and destroy the opponent’s third weapon.

According to Wilson’s thesis,\textsuperscript{167} the opponent who is unable to develop or acquire a nuclear capability, or who calculates that the risk of retaliation in kind detracts from the deterrent value of limited nuclear threats, is nevertheless likely to pursue the acquisition of RMA-2 capabilities which defeat the West’s increasing reliance on RMA-3 technology. They will therefore seek BMs, together with a limited but credible CBW capability, in order to create the implicit threat of WMD strikes against the unprotected population centres of coalition states, their allies or dependent territories. The relative inaccuracy of emerging BM systems suggests that they possess very limited utility against protected military targets; moreover, satellite surveillance means that the source of the attack can be easily identified, permitting rapid reprisals against the aggressor state. However, the psychological impact of non-conventional strikes far outweighs the physical destruction caused and dictates that the possession of BMs presents more value as a deterrent, or coercive, capability than as a means of disruption.

Technological approaches and lesser military capabilities, associated with the RMA, have less deterrent value since such measures typically lack the psychological impact necessary to achieve a decisive influence on public opinion and political decision-making. On the contrary, unconventional approaches such as terrorism and atrocities do create psychological impact; however, in the early diplomatic stages of a potential intervention, when deterrent strategies have optimum utility, the target set is restricted to military formations at their home bases, and symbolic political and civil objectives. Aside from the practical difficulties, associated with ‘exporting’ terrorism within a short time-frame, the likely public demand for extreme measures against the perpetrators would militate against this form of attack as a deterrent strategy.

**Disruption**

Once a coalition is assembled and committed to military intervention, the motive would change from deterrence to *disruption*, in order to interrupt or hinder military operations and undermine public confidence and support; however, it is likely that

\textsuperscript{165} Gouré, (5 May 1999), *op. cit.*
\textsuperscript{166} Libicki, *op. cit.*, 79.
\textsuperscript{167} Wilson, ‘Twentieth Century Revolutions in Military Affairs’ (see Figure 4).
opponents would carefully measure the impact of individual attacks to minimise the risk of massive retaliation, since there is a danger of provoking exactly the kind of response they are seeking to avoid. Arguably, the ‘centre of gravity’ of intervention operations is the point of deployment (particularly if military formations are targeted at their home bases, or between the home base and the port of embarkation) since a successful attack at this stage would have the greatest detrimental impact on military credibility and public confidence. This strategy would depend on the opponent having the capabilities and resources in place to permit rapid strikes; however, they may exploit the period of ‘preventative diplomacy’ which emphasises coalition building and the threat of force, to mobilise their counter-intervention capabilities. Alternatively, they may exploit the second ‘window of opportunity’ which presents itself during the deployment of land forces and logistics into the theatre of operations; as the Friedmans observe:

‘The gap between the decision to intervene and the buildup of supplies in theater to begin offensive (or even defensive) operations can be dangerously long. Yet it is built into [military] strategy. For example, over a year elapsed from the decision to invade France to the completion of the buildup in May 1944. In Desert Storm, it took six months from the decision to intervene to the ability to mount an assault.’

Any approach which lengthens, or complicates the period of time required to deploy and intervene may have a strategic impact, out of all proportion to the actual operational effects, and this is exacerbated by the metaphorical ‘clocks’ that are ticking: not least the pressure to maintain coalition unity and consensus; public impatience for a swift conflict resolution; and the slim window of opportunity, imposed by weather and visibility, which present limitations for certain military options.

The aims of disruption strategies are to undermine public confidence in the military’s ability to prosecute a successful campaign with minimal casualties, and to stimulate political pressure to limit the scope and duration of military involvement. This can be achieved by simultaneously exploiting a range of capabilities which target vulnerabilities during the sensitive deployment phase. At first, a SIW campaign waged against the NSI could corrupt the essential infrastructure required for the rapid movement of military formations between their home bases and the air and maritime ports of embarkation; particularly if attacks target transport, port and air traffic control services, or fuel and power supplies to key facilities and military bases. Of course the same level of disruption could be achieved using conventional terrorism, and with far greater psychological impact, although an attack at this critical stage would limit the credibility of ‘plausible deniability’ and would arguably be more likely to stiffen the intervening power’s resolve. Once the intervention force deploys, the optimum target becomes the means of power-projection: aircraft carriers, maritime transport (often unprotected merchant ‘ships taken up from trade’ (STUFT)) and strategic airlift. The opponent who is able to exploit high-tech RMA capabilities could target aircraft carriers using anti-ship cruise missiles, and even the low-tech opponent could inflict some level of attrition against less valuable (but more vulnerable) air and maritime

---

168 Friedman, G. & M., op. cit., 412.
transport, using surface-to-air missiles, submarines or mines. With the exception of aircraft carriers, the loss of individual ships and aircraft would be damaging, but low levels of attrition have minimal operational impact; however, clandestine operations against in-theatre ‘hub’ air bases or ports would cause significant virtual attrition, through the interruption of further movements while units reassessed security arrangements and neutralised residual threats.

Lightly-armed ‘first echelon’ rapid deployment forces are particularly vulnerable if the opponent is able to obstruct the deployment of heavier, ‘second echelon’ forces, using WMD, SIW or unconventional approaches. WMD may be used as less-than-lethal ‘weapons of mass disruption’: for example, the small nuclear power who wishes to demonstrate capability and intent, whilst reducing the risk of guaranteed nuclear retaliation, may detonated a weapon at high altitude to achieve wide-area EMP effects. This could seriously degrade the military capabilities of C4ISR-dependent forces without inflicting widespread casualties or environmental damage associated with blast and radiological effects. Persistent chemical agents would undoubtedly cause some tactical disruption, although not long-term operational impact against forces trained and equipped to function in a chemical environment; however, the release of biological agents could cause longer-term disruption due to mass illness.

In theory, the potential for a severe backlash militates against the resort to WMD, unless the opponent calculates that the ‘stake’ is low; in which case their psychological value suggests that WMD have greater utility against the ‘home-front’ where they can be exploited to induce fear amongst families and civilian support staff. Alternatively, the opponent may simply capitalise on the implicit threat of WMD strikes by launching indiscriminate BM attacks. These are likely to distract air and ground forces from their primary war aims in an effort to interdict the missile systems before they trigger either a collapse of coalition unity or a dramatic conflict escalation. The opponent who possesses advanced technological capabilities may wage a SIW campaign against military C4ISR systems, corrupting the transmission of vital communications and degrading the deployed force’s ability to exploit information as a force multiplier. Alternatively, the opponent at the opposite end of the technical and ‘legal compliance’ spectrum, may exploit the unconventional approach through measures designed to distract military forces from their principle tasks. This strategy was successfully exploited by Serbian forces during NATO’s intervention in Kosovo, through the creation of a mass refugee exodus which presented NATO Peacekeeping forces with a humanitarian catastrophe and the risk of regional instability which threatened to undermine the solidarity of key regional allies.

**Exhaustion/Attrition**

If disruption fails, or if the opponent is unable to strike within the window of opportunity between the decision to intervene and the launch of offensive operations,

---

169 During the 1991 Gulf Conflict, Iraq launched missiles against Saudi Arabia and Israel in an unsuccessful attempt to undermine coalition unity. However, in an effort to neutralise this threat, the coalition diverted a significant proportion of the air campaign to interdiction tasks yet, after six weeks intensive bombing and complete air superiority, the ‘Great Scud Hunt’ proved ineffective in locating and destroying the missiles prior to launch. (Gulf War Air Power Survey, 1993), cited in Preston, op. cit., 100.
the motive will switch to *exhaustion* or *attrition*. Both strategies exploit public aversion to lengthy commitments, although ‘exhaustion’ focuses on approaches specifically intended to extend the duration of the conflict, which stimulate public concern about the futility of a lengthy and inconclusive military commitment; Dunlap argues that the proliferation of global news media is responsible for this distinct characteristic of contemporary conflict:

‘The technology-empowered media and the proliferation of personal information/communication devices will have the effect of limiting the practical ability of casualty averse democracies to engage in combat for much more than thirty days.’

The alternative ‘attritional’ approach targets the characteristic numerical inferiority of intervention forces, and focuses on approaches which increase the levels of destruction and casualties on *either* side; this was a significant factor in the failure of US strategy in Korea and Vietnam:

‘Long-range operations have meant that numerically inferior forces faced superior forces. Under those circumstances, the United States needed to end wars as quickly and painlessly as possible…. Rather than controlling the tempo and scope of the war and carrying the fight to the enemy to force a rapid decision, in Korea and Vietnam the United States ended up engaging in attritional warfare on the enemy’s timetable.’

Unconventional approaches offer the most lucrative means of defeating an intervention through exhaustion, since the simple failure to present a militarily significant target forces the intervening power into ever more risky tactics in order to achieve some sense of progress with which to appease domestic public opinion. The opponent’s strategy classically involves the dispersal or concealment of military assets, or the use of human shields and ‘high-value collateral’ to deter military strikes which risk unacceptable civilian casualties. Alternatively, attrition may be achieved by exploiting clandestine operations or ‘RMA’ capabilities which progressively damage or destroy key HVA, or through a terror campaign which targets domestic casualty sensitivity.

**Coercion**

Finally, if disruption, exhaustion or attrition fail, the opponent is likely to resort to *coercion* in order to intimidate coalition partners or allies into withdrawing their support or facilities. Coercion represents the riskiest strategy, since it would require a decisive, even catastrophic, event (combined with the credible threat of further attacks) in order to achieve such a dramatic policy reversal; however, such measures could equally harden public support. This is addressed by McNaugher, at RAND, who argues that the fundamental issue which constrains opponents from employing extreme countermeasures is the strategic calculation: ‘…at what point does an

---

170 Dunlap, (1996b), *op. cit.*
171 Ibid., 396.
asymmetric attack trigger massive retaliation?’\textsuperscript{172} One coercive approach is to exploit what US Defense Department strategists have defined as ‘Escalation Asymmetry’,\textsuperscript{173} which targets the tension between the overwhelming desire to limit war aims and the perception that the failure to respond to the opponent’s escalatory, war-widening activities would be viewed as weakness. This is explored in the French 1994 ‘Defence White Paper’\textsuperscript{174}, which identifies attacks against the national integrity overseas as one of six challenges most likely to require a military response, and reflects a vulnerability to which Britain is equally exposed. The first scenario, which French observers consider less likely, is direct aggression with the attempt to seize territory; the second, focuses on indirect actions aimed at destabilising a territory. Alternatively, the opponent who is facing a military defeat may resort to ‘shock’ tactics in an effort to stimulate the capitulation of the intervening force. In the first instance, in order to minimise the risk of massive retaliation, this is likely to be limited to strikes against ‘legitimate’ military and political targets. However, the opponent with his ‘back against the wall’, who fears the defeat or collapse of the regime itself, may resort to ferocious measures using catastrophic means - striking at targets of symbolic, rather than military value, in order to be noticed.

‘Shock’ may be achieved through the creation of any strategic event designed to inflict as much damage \textit{politically} to the conduct of a war as the loss of a major battle would, operationally or militarily. To be effective it would need to be timely, and to achieve the necessary strategic impact it would also need to be catastrophic. These aims could be achieved through the use of a tactical ‘battlefield’ nuclear weapon, which would signal capability and intent but whose restricted strategic impact might reduce the risk of an automatic nuclear response.\textsuperscript{175} Alternatively, indiscriminate missile attacks with the implicit threat of non-conventional warheads, could also be used to intimidate allies into withdrawing from the coalition or withdrawing permission for military strikes to be launched from their territory. A significant military victory, such as the sinking of a carrier, could achieve a similar impact, particularly if the time required to reconstitute the intervention force compelled the abandonment of short-term war aims. It would be more difficult for the opponent to inflict the same strategic impact against land-based assets, since it would require substantial damage or destruction to create the same operational and psychological impact as the loss of a carrier. Nevertheless, an alternative strategy would be to target key personnel since a successful clandestine operation or terrorist strike at a critical stage in the conflict

\textsuperscript{172} McNaugher, T.L., Deputy Director Arroyo Center, RAND Washington Office, in an interview 11 May 1999.
\textsuperscript{174} Summary published in French Defence Monitor (Vol. 1, No. 1, August 1994); cited in Beck, \textit{op. cit.}, 36-7.
\textsuperscript{175} There is a broad school of thought in the US which considers that NW have no utility as tools of retaliation against small powers: ‘Nuclear weapons are such a gross instrument of power that they really have no utility. They work against you, in that they are best used to destroy cities, and kill women and children. Now first, that’s morally wrong; second, it doesn’t make sense; and then, of course, there is the real threat of nuclear weapons in the hands of irresponsible or desperate powers. If you own them, you legitimize them just by your own ownership.’ Horner, General Charles, USAF (Retd.) in Schell, J. ‘The Gift of Time’ \textit{Nation}, (2-9 February 1998).
would exploit domestic sensitivity to ‘body bags’ and could inflict substantial operational damage; particularly if it targeted a scarce resource such as combat-ready aircrew who are potentially irreplaceable in the short-term.\textsuperscript{176} Finally, the adversary at the far end of the ‘legal compliance’ spectrum, whether due to culture or because they perceive they have nothing to lose, may exploit the perceived ‘asymmetry of stake’ by resorting to atrocities or catastrophic terrorism. The optimum target for terrorist attacks would be unprotected urban areas of coalition partners, their allies or dependencies, in an attempt to demoralise the population and trigger the collapse of public and political support; however, this is a high-risk strategy since, paradoxically, terrorist attacks against forward deployed military forces are likely to engender a completely different public reaction to acts of terrorism directed at domestic targets; as Dunlap observes:

‘Although the objective of both might be to maximise casualties, the former could succeed in undermining support for an overseas operation while the latter may well evoke a demand for extreme measures against the perpetrators.’\textsuperscript{177}

**Summary**

Figure 7 summarises the relationship between the opponent’s motives and the asymmetric approaches they are likely to employ to achieve those ends. Whilst this is not intended to be an exhaustive assessment, it does illustrate the capabilities which offer the greatest value in particular circumstances. In particular, it highlights the utility of BMs (together with a limited but credible CBW capability) as an asymmetric tool which may be exploited to deter or disrupt military intervention or, ultimately, to coerce coalition partners or allies into withdrawing their support or facilities.

\textsuperscript{176} Before the start of the 1939 Russo-Finnish war, Finnish pilots had been targeted for assassination by Soviet agents (although, in the event, the plan was never put into practice). Williamson, *op. cit.*, 344.

\textsuperscript{177} Dunlap in Matthews, *op. cit.*, 10.
Figure 7: Asymmetric Approaches: Motives and Means

DETERRENCE

Nuclear Weapons (EMP)

Ballistic Missiles + Chem/Bio Warheads

Strategic Information Warfare

Unconventional Approaches

DISRUPTION

COERCION

Nuclear Weapons

RMA Clandestine Ops Terrorism

Atrocities

EXHAUSTION

ATTRITION

Newman: 99-04
CHAPTER VI: COUNTERMEASURES

Introduction

This chapter explores the three broad measures that may be implemented to combat the threat posed by future adversaries who exploit asymmetric approaches to oppose military intervention: countermeasures include deterrence, through the maintenance of robust nuclear and conventional capabilities; threat management, through pre-emptive measures which reduce or remove the means of attack; and defence, through both active (preventative) and passive (protective) measures.

Deterrence

NATO’s deterrence policy relies on the threat of second-strike retaliation; however, in the event of the opponent’s first-use of WMD, the ratification of the BTWC and the CWC limits the legitimate responses to either nuclear or conventional retaliation. In theory, the opponent’s first-use of NW would justify retaliation in kind; although there are those in the defence community who argue that NW have limited utility, particularly in the context of Great Power retaliation against small or weak states.\footnote{Schell, op. cit., See footnote 175.} Moreover, the reliance on nuclear deterrence restricts the options for retaliation against an opponent’s use of non-nuclear WMD and this provides a case for an asymmetric deterrence strategy, in which NW might be used in retaliation to the first use of any WMD. This is supported by Betts, in a 1998 Foreign Affairs paper, in which he argues that the ratification of the BTWC/CWC ‘…practically precludes a no-first-use policy for nuclear weapons, since they become the only WMD available for retaliation.’\footnote{Betts, op. cit., 31.} The only credible alternative is massive conventional retaliation, but this would inevitably detract from the force of future deterrent threats, setting the precedent that opponents could use WMD without suffering similar destruction in return. Nevertheless, asymmetric deterrence presents its own difficulties and, in their response to Betts’ article, Yarmolinsky and Schlefer argue that, the abandonment of the US’ ‘no-first-use’ policy would indicate to potential opponents that the most powerful nation in the world is unable to protect itself against CBW attack without threatening nuclear retaliation.\footnote{Yarmolinsky, A. and Schlefer, M., ‘Two Wrongs…’ Foreign Affairs (May/June 1998) 157.} Citing Iran’s experience as the victim of CW attack, they note that this strategy might provide a justification for weaker powers to acquire a NW capability. Moreover, they highlight that any threat or use of NWs would violate the terms of the 1995 ‘Unilateral Security Assurances’\footnote{See footnote 81.} in which the five acknowledged nuclear powers undertook not to use or threaten to use NW against states who are party to, and in compliance with, the NPT. A compromise lies in the US’ adoption of ambiguous declaratory policies concerning whether or not they would resort to the use of NW in response to non-nuclear WMD attacks; indeed, controversy remains about whether the threat of nuclear retaliation by the US and its nuclear-armed allies (the UK, France, or Israel) deterred Saddam Hussein from authorising the use of Iraq’s extensive CW arsenal during the Gulf War. The then US Secretary of Defense, James Baker, subsequently indicated that the Bush
Administration had ruled out any prospect of an asymmetric retaliation, although they ‘…purposely left the impression that the use of chemical or biological agents by Iraq could invite tactical nuclear retaliation.’\textsuperscript{182} Writing in the USNDU \textit{Strategic Assessment}, Nacht concludes that ‘US decisionmakers, de facto if not \textit{de jure}, would consider nuclear weapons as weapons of last resort…’ but notes that:

‘[i]t would probably take a direct attack using WMD on a major US military force or population … An extraordinary provocation would be necessary before their use would be authorized.’\textsuperscript{183}

The main obstacle to the credibility of ‘second-strike’ deterrent threats is the reliance on accurate and timely knowledge of the attacker’s identity and the source of the attack. It is difficult to frame a viable strategy for fighting states or non-state groups ruthless enough to commit indiscriminate killing and, while military force may be used to inflict punishment on the states which sponsor violence, it is often difficult to identify the government which can rightly be held accountable for the perpetrator’s actions - a dilemma that was clearly illustrated by the controversial cruise missile strikes against a Sudanese pharmaceuticals factory, in response to the 1998 terrorist bombings of American Embassy buildings in Kenya and Tanzania.\textsuperscript{184}

One deterrent solution may lie in a proposal, presented in a 1998 \textit{Foreign Affairs} paper on \textit{Catastrophic Terrorism}, that the development of prohibited weapons should become a universal crime under international law, opening the way to prosecute and extradite offenders using the power of national criminal law against \textit{individuals} rather than the power of international law against governments.\textsuperscript{185} However this policy would need to be backed up by guarantees that Western governments would deal decisively with barbarism when confronted by it, using all necessary and legitimate means (including the use of massive conventional force) in order to deter rogue powers from daring to oppose them.

\textbf{Threat Management (Pre-emption)}

The problems associated with framing a credible deterrence policy has led many in the defence establishment to favour pre-emption; typical measures aim to control or restrict an opponent’s capabilities, and focus on arms control initiatives, and enforced disarmament. Such initiatives are based on treaty regimes and require intrusive verification measures and parallel export control regimes; however, Betts argues that these do not deter the problem countries who want to obtain WMD - unless, like Iraq and North Korea in the 1980s, they violate international law after signing to accept the legal obligation.\textsuperscript{186} In exceptional cases enforced disarmament may be possible, such as those measures imposed upon Iraq by the UN in 1991, although this is only likely

\textsuperscript{183} Nacht, M., ‘Nuclear Weapons’ in Binnendijk, \textit{op. cit.}, 203.
\textsuperscript{184} Despite US claims that the Khartoum factory they destroyed on 20 August 1998 produced chemicals for use in toxic nerve gas, critics argue that the al-Shifa pharmaceutical factory made only medicines: Gimson, A., ‘German envoy challenges Sudan arms plant claim’ \textit{The Daily Telegraph} (31 August 1998).
\textsuperscript{185} Carter \textit{et al}, \textit{op. cit.}, 86.
\textsuperscript{186} Betts, \textit{op. cit.}, 35.
to be a viable option when a disarmament regime is imposed post-conflict, as part of the military settlement; indeed, Preston argues that:

‘[w]ithout the invasion of Kuwait to provide a rationale for eliminating Iraq’s nuclear programme, it is highly unlikely that effective action would have been taken by either the US or the international community to prevent Iraq from becoming a nuclear state.’\(^{187}\)

Where rogue states defy treaty obligations or Security Council Resolutions, traditional arms control measures may need to be complemented by *counterforce*, using precision conventional weapons to destroy the opponent’s capabilities, either pre-emptively or in retaliation. Such attacks may also have deterrent value, though only if they destroy targets highly valued by the rogue state, and one of the key lessons of the 1991 *Desert Storm* air campaign is that even prolonged and extensive military operations may be unable to locate or destroy an opponent’s WMD facilities.\(^{188}\) This highlights the limitations on the ability of Great Powers to militarily pre-empt such programmes, leading Betts to conclude that if measures aimed at controlling an opponent’s *capabilities* cannot eliminate the dangers, an alternative strategy would be to address the opponent's *intentions*. This presents the dilemma between isolationism and engagement: on the one hand, the best way to prevent an opponent’s attack is to avoid intervention in their conflicts; on the other, it is neither sensible, nor even acceptable, to reject engagement simply to avoid the risks of retaliation.

**Defence**

If deterrence fails, and given that there is scant precedent for pre-emptive action to limit or remove a potential opponent’s capabilities,\(^{189}\) the focus of countermeasures shifts to defensive responses, designed to *prevent* an attack from occurring or to *protect* against the effects of a successful attack.

**Active Defence (Prevention)**

In the aftermath of the Gulf War, analysis of the vulnerability of Coalition forces and regional allies to Iraqi *Scud* attacks prompted the US to develop an integrated Ballistic Missile Defence System (BMDS), based on the deployment of a theatre missile defence (TMD) network and the development of a limited national missile defence (NMD) capability, to be deployed in 2005-2010.\(^{190}\) However, NMD is a controversial step, since it remains unclear whether or not it would breach the terms of the Anti-Ballistic Missile (ABM) Treaty which restricts the freedom to employ an ABM system to defend the national homeland.\(^ {191}\) Moreover, opponents fear that the strategy risks stimulating Chinese or Russian nuclear force modernisation and argue that the vast investment required to defend against one limited option would not

---

188 See footnote 169.
189 With the exception of the 1981 Israeli air attacks which destroyed Iraq’s nascent nuclear programme. See Preston, *op. cit.*, 88.
190 Nacht, *op. cit.*, 196.
191 Under the terms of the 1972 ABM Treaty, and subsequent related agreements, a theatre-anti missile system can only be used to defend forward-deployed troops.
counter other means of WMD delivery, including aircraft, cruise missiles and unconventional means. Betts dismisses the BMDS as ‘...expensive investments that might or might not work against a threat the US probably will not face for years, but would do nothing against the threat it already faces.’\textsuperscript{192} However, much of his case is based on the projection that ‘Rogue States’ such as Iraq, Iran and North Korea would not possess the capability to deploy ICBMs for some years and this is at odds with the Rumsfeld Commission findings.\textsuperscript{193} Moreover, it fails to account for the fact that the BMDS needs to be deployed before a regional opponent achieves an ICBM capability and that forward deployed military forces - the principle target of an opponent who wishes to retain a degree of international legitimacy - are already vulnerable to shorter range systems.

In addition to the general threat of missile or WMD attack, preventative measures need to address the specific threats to HVA; particularly the potential vulnerability of maritime assets to cruise-missile and sub-surface attack; and of static targets (such as air bases, ports and logistics depots) to ground attack by SPF or non-state actors. The evolving maritime threat will inevitably force aircraft carriers to operate further from the coastal littoral, posing problems for short-range combat aircraft which will become more dependent on air-to-air refuelling (AAR). Alternatively, land-based air operations will increasingly fall within the opponent’s long-range artillery fan, as munitions are delivered by ballistic and cruise missiles, and it will become more difficult to obtain HNS from allies who fear direct attack. Both scenarios suggest that the inevitable solution lies in an emphasis on long-range bombardment, launched from outside the menace theatre, although an alternative strategy would be to focus on the development of RMA-4 technologies, designed to defeat either the delivery systems or the target intelligence source; typically satellites or UAVs.\textsuperscript{194}

Preventative countermeasures also need to focus on other military and unconventional threats to personnel, and the 1996 terrorist bombing of the Khobar Towers US military housing complex has made the ‘force protection’ (FP)\textsuperscript{195} of deployed personnel a high priority for defence planners. Sceptics fear that the US military enthusiasm for FP has become an obsession, and serving officers complain that ‘Force Protection has become the Mission’; indeed the failure of the Pentagon to commit US Apache attack helicopters to combat in Kosovo generated suspicion that, among other factors, FP concerns were overshadowing operational considerations.\textsuperscript{196} However, the absence of terrorist attacks against Western military targets since 1996, particularly in Bosnia, has prompted other analysts to assess the military’s enhanced FP policy as a success.

The paradox of successful protection measures is that they may encourage terrorists to consider larger or unconventional attacks which inflict higher casualties. The most

\begin{itemize}
  \item \textsuperscript{192} Betts, op. cit., 36.
  \item \textsuperscript{193} See footnote 82.
  \item \textsuperscript{194} See Figure 4.
  \item \textsuperscript{195} Emerging UK Joint doctrine defines Force Protection as ‘a process which aims to conserve the fighting potential of the force by countering the wider threat to its elements from adversaries, natural and human hazards, and fratricide.’ \textit{Unpublished.}
  \item \textsuperscript{196} Butcher, T., ‘US air cavalry to the rescue - but when will it attack?’, \textit{Sunday Telegraph} (25 April 1999).
\end{itemize}
successful FP measures are assessed to be \textit{isolation}, reducing the unprotected physical proximity of deployed military personnel to locals; or, where the mission involves close interaction, \textit{dispersal} - mixing thoroughly so that terrorists or SPF have difficulty targeting military personnel. Following the \textit{Khobar} incident, the Anglo-US Coalition chose to isolate military forces in Saudi Arabia, moving them from Dhahran to a remote desert air base; however, whilst reducing the vulnerability to terrorist or clandestine attacks, ironically this course of action presents a single, concentrated HVA which may be targeted using BMs and WMD, with minimal risk of collateral damage. In Bosnia, UN/NATO forces favoured dispersal - distributing military accommodation among civilian hotels and apartment buildings - which affords reduced protection for individuals but removes the opponent’s opportunity to achieve a strategic event.\footnote{Clawson, P.M. ‘Nonstate Threats’ in Binnendijk, \textit{op. cit.}, 208.}

One of the most valuable lessons, drawn from the investigation into the \textit{Khobar Towers} bombing, was that the prevention of military or unconventional threats is dependent on effective intelligence and communication. Following the attack, the Pentagon Senate Armed Services Committee commissioned a report on the protection of US forces deployed abroad, which concluded that the unit was ‘ill-served’ by an intelligence arrangement that focused almost exclusively on the threat to air operations in the Region, and highlighted the potential difficulties arising from the necessary interface between deployed military commanders and ‘Host Nation’ military agencies and bureaucracies.\footnote{Downing, General W.A. (US Army Retd.), \textit{The Downing Investigation Report to the President and Congress on the Protection of US Forces Deployed Abroad} (30 August 1996).}

Where the perceived threat is directed against domestic targets, preventative measures involve targeting groups assessed as potential breeding grounds for terrorists; however, this inevitably stretches the limits on domestic intelligence activities and presents a tension between the maintenance of civil liberties and legitimate surveillance. The potential weakness of intelligence collation and communication in a domestic context is illustrated by the flawed Japanese response to the activities of \textit{Aum Shinrikyo} prior to the 1995 attack on the Tokyo subway; the Sect had used Sarin nerve agent in assaults on civilians nearly a year earlier but, although the Japanese national media had reported the incident, law enforcement agencies remained unaware of intelligence that other local organizations had uncovered. The parties did not share the expertise to prevent another attack and the world remained unaware of an incident which possibly represented the first terrorist use of WMD.\footnote{Carter \textit{et al}, \textit{op. cit.}, 83.}

Finally, preventative measures will also need to address the \textit{cyber}-threat to military C\textsuperscript{4}ISR systems and the NSI. The optimum solution appears to lie in the identification and protection of the MEII; however, despite complex technical measures to protect the confidentiality and authenticity of computer-processed information, solutions to ‘denial of service’ attacks remain elusive. One US suggestion proposes the formation of a National Information Assurance Institute to conduct research on security assessment tools, intrusion detection, data recovery, and restoration; and train key personnel on state-of-the-art (‘technical best-practice’) procedures.\footnote{\textit{Ibid.}, 87.}
Passive Defence (Protection)

Passive defence typically focuses on those protective measures designed to minimise the effects of successful strikes. For deployed military forces, this requires the protection of HVA and personnel from WMD and missile, ground or terrorist attack; and the shielding of critical C\(4\)ISR systems from EMP effects and cyber-attack. Considerable protection is provided by the routine emphasis on dispersal and physical measures, which reduce the impact of conventional attacks, and by the proficiency of most NATO forces in nuclear and chemical defence procedures. However, protection against biological attack is recognised as a general area of weakness\(^{201}\) and few navy, army or air forces possess dedicated defence forces specifically trained and equipped to protect against clandestine attacks, launched from the ‘stand-off footprint’ around high-value static facilities.\(^{202}\) The vulnerability of in-theatre accommodation to terrorist attack has focused attention on the selection and protection of suitable facilities; however, there is evident ‘institutionalised inertia’ against dispersal measures which minimise the risks of large-scale attacks but reduce the ‘quality of life’ for deployed personnel.\(^{203}\) Finally, the increasing reliance on ‘commercial off-the-shelf’ (COTS) C\(4\)ISR systems raises the vulnerability of the military’s essential information infrastructure to EMP and cyber-attack.

Notwithstanding the evident weaknesses in military protective measures, the truly asymmetric opponent will seek to exploit the optimum vulnerability - potentially the civil population. This has led Betts to argue for the implementation of protective measures to mitigate the consequences of a catastrophic attack, including:

‘[the] stockpiling or distribution of protective masks; equipment and training for decontamination; standby programmes for mass vaccinations and emergency treatment with antibiotics; wider and deeper planning of emergency response procedures; and public education about hasty sheltering and emergency actions to reduce individual vulnerability.’\(^{204}\)

In 1996, the US Defense Department implemented a programme to provide domestic emergency preparedness training and equipment for 120 cities;\(^{205}\) however, the UK has no parallel legislation and Betts observes that, since the threat has yet to register on the public agenda this in turn limits the inclination of politicians to pursue appropriate civil defence programmes. Nevertheless, opponents of civil defence argue that at best they promotes a false sense of security, at worst they alarm people and

---

\(^{201}\) See Roberts and Pearson, op. cit.
\(^{202}\) In the conclusion to their analysis of the evolving ground threat to US Air Force bases, Shlapak and Vick recommended that the USAF should consider the Royal Air Force approach to air base security, encapsulated in a dedicated infantry force - the RAF Regiment. Shlapak & Vick, op. cit., 71.
\(^{203}\) Four days into NATO’s Kosovo air campaign, a British broadsheet published an article which revealed that the British aircrew of the RAF Harrier Force were accommodated in ‘…one of the most luxurious hotels in Gioia del Colle [Italy].’, Hall, M., ‘Coffee and opera by day: bombing Serbia by night’, The Sunday Telegraph, (28 March 1999), 25.
\(^{204}\) Betts, op. cit., 37.
could even be destabilizing, provoking an attack in a crisis.\(^{206}\)

**CONCLUSION**

It is difficult to frame a useful definition which provides a comprehensive, yet concise, explanation of asymmetric threats; not least because of the disparate asymmetries which may exist within a conflict, and the broad spectrum of asymmetric means which the opponent may exploit - themselves dependent on his motives, intentions and opportunities. This paper offers the following explanation, as a conceptual framework within which to analyse the emerging challenges to military intervention:

‘Asymmetric conflict occurs when there exists, between the contending parties, any significant disparity with respect to their military or technical configuration; their degree of compliance with international legal conventions; or their respective ‘stake’ in a successful conflict resolution. Where asymmetries exist, the weaker party will endeavour to avoid the superior opponent’s strengths by focusing their military, technical and unconventional comparative advantages against his relative weaknesses. The aim of asymmetric strategy is to deter or disrupt military intervention; defeat the opponent’s will through exhaustion or attrition; or coerce the opponent, their coalition partners or allies, into withdrawing support for the use of military force.’\(^{207}\)

Several factors suggest that Britain will continue to ‘punch above her weight’\(^{208}\) in international affairs, even where the national ‘stake’ is minimal. As Towle observes, apart from humiliations at Singapore in 1941 and Suez in 1956, ‘British power has declined slowly rather than being shattered by some catastrophic defeat [as a result of which] the tradition of intervention, or of behaving like a Great Power, has been unbroken.’\(^{209}\) In addition to this underlying tradition, experience and national pride, Britain’s obligations as a ‘P5’ member of the UN Security Council, and the expectations of her allies and dependants, continue to compel a pro-interventionist stance. It is this, combined with the nation’s emerging\(^{210}\) power-projection capability, which contributes to Britain’s status as one of the advanced military powers and theoretically increases the nation’s vulnerability to asymmetric challenges by small, or relatively weak opponents. However, the aim of this paper has been to achieve a pragmatic assessment of the realistic, rather than the possible, risks and this has highlighted the tendency, in much of the contemporary literature concerning ‘asymmetric threats’ to connect vulnerabilities directly with ‘strategies, capabilities

\(^{206}\) Betts, *op. cit.*, 38.


\(^{208}\) Attributed to Douglas, Lord Hurd of Westwell (formerly British Secretary of State for the Foreign and Commonwealth Office) *Hinsley Memorial Lecture, St. John’s College, Cambridge, 4 March 1999.*

\(^{209}\) Towle, *op. cit.*, 94.

\(^{210}\) The SDR highlighted the shortfall of dedicated strategic lift, to enable the timely deployment of the new Joint Rapid Reaction Forces, and identified specific requirements for additional container ships and strategic airlift. Additionally, the replacement of the existing *Invincible* class aircraft carriers with two larger new-generation carriers, and the acquisition of the ‘Future Carrier-Borne Aircraft’, are central to the Government’s force projection aspirations. *SDR, op. cit.* Para. 115.
and intentions of shadowy, unidentified “enemies.” This concern was elucidated by the Chairman of the US Army War College’s 1998 Annual Strategy Conference, who admonished that:

‘No nation, not even the United States, can eliminate all its vulnerabilities. Rather, we... must narrow our security focus to those particular vulnerabilities that correlate with the actual capabilities of real-world enemies.’

The first danger is that we over-estimate our opponents’ realistic resources and capabilities - in particular their degree of technical sophistication - and fail to assess the obstacles they first need to overcome. A 1996 paper, published in the Indian Defence Review, cautions that the less-advanced military force risks ‘...rush[ing] into rapid technological modernisation in such a way that desired military advances become a “technology trap,” leading to the nation’s battlefield demise against the very adversary it has attempted to emulate.’ The second is that we impugn too much cleverness in our adversaries; notwithstanding Iraq’s use of BMs against Israel in 1991, and Iraq and Serbia’s extensive use of unconventional strategies in their confrontations with the US-led coalition (Iraq: 1991-98) and NATO (Serbia: 1999) respectively, neither power resorted to the full range of conceivable asymmetric strategies. One possible explanation is offered by Preston, who suggests that the primacy of ‘regime survival’ may impose considerable limitations on the lengths to which opponents are prepared to go in order to coerce a superior challenger. Preston describes the Iraqi Leader, Saddam Hussein, as ‘...an aggressive, power maximizer who will pursue aggrandizement only until it threatens his own power position.’ Indeed, this assessment may be equally true of Serbian President, Slobodan Milosevic, and suggests that both leaders’ ambition and drive for power are rivalled only by their desire for self-preservation.

Just as there is a danger of overestimating potential opponents’ capabilities and intentions, the alternative arguably presents the greater dangers. Indeed the ‘Downing Commission’ investigation into the Khobar Towers bombing concluded that one of the factors which accounted for the inadequacy of FP measures in Dhahran in 1996, following a much smaller car bomb attack in Riyadh the previous November, was a simple ‘failure of imagination’. The commentary on the broader ‘emerging threats’ highlights two related areas where the West needs to adopt greater imagination: first, to expand its assessment of asymmetric warfare to consider the culturally distinct perspective of potential enemies; and, second, to anticipate the danger from opponents who pursue the ‘twin pillars’ of conceptual innovation and advanced military technology.

212 Ibid., 327.
214 Preston, op. cit., 104.
215 Downing, op. cit.
216 Dunlap in Matthews, op. cit., 12.
217 Beck et al, op. cit., 49.
In 1998, in its report on the SDR, Britain’s HCDC made the following observation:

‘The UK has largely avoided overseas interventions that have rebounded to our disadvantage, but the same is not true of our North American allies. Once a decision has been taken to intervene, the stakes are immediately raised for the UK, and the risk of diplomatic damage, or even some form of military or terrorist reprisal, are accordingly heightened.’

Therefore, Britain will need to decide when and where it can afford to back its policies by military intervention or the threatened use of force. In essence, there are three possible courses of action: isolationism; rampant interventionism; or a ‘third way’, based on a considered calculation of the merits of the decision to employ armed forces ‘...determined not only by the justice of the cause but also by their likely efficacy.’

Isolationism is discussed by Betts, who observes that activism to guarantee international stability is, paradoxically, the prime source of vulnerability; however, he qualifies this with the acknowledgement that:

‘[I]t is not automatically sensible to stop pursuing others’ interests for the sake of uncertain reductions in a threat of uncertain probability. Security is not all of a piece, and survival is only part of security.’

Rampant interventionism has some merit, if decisive and robust action against barbarism proves to be an effective strategy for deterring subsequent challenges to the international order; however, whilst this may be possible for unilateral intervention, the requirement for consensus makes it harder to achieve, or sustain, for coalition operations. Moreover, there is a danger - expressed by Dunlap in 1998, and exacerbated by the relatively painless NATO victory against Serbia the following year - that ‘...decisionmakers may delude themselves into thinking that the challenge of asymmetric warfare is exclusively technical.’ Indeed, in 1995 the Wall Street Journal reported military officers’ fears that civilian leaders who lack first-hand military experience might believe that ‘gadgets can somehow substitute for the blood and sweat of ground combat.’ Therefore, the sensible strategy appears to lie with the ‘third way’, restricting military intervention to circumstances where Britain has a particular stake, or where there is a consensus between the establishment and the general public that such involvement is desirable. In one respect, this will require exceptional political leadership, not least to banish the stranglehold that the media’s obsession with ‘casualty sensitivity’ has on the freedom to commit military forces. If the public is persuaded of the moral imperative for, and legitimacy of, military intervention then strong political leadership is likely to temper the strategic impact of the physical or psychological damage inflicted by the opponent who exploits asymmetric means. However, as Luttwak observes, ‘the routine functioning of a great

---

218 HCDC, op. cit., clxiv.
219 Towle, op. cit., 104.
220 Betts, op. cit., 28, 41.
221 Dunlap, in Matthews, op. cit., 11.
power cannot depend on the fortuitous presence of exceptional leadership.’

Where the stake is minimal, and an asymmetric backlash to intervention would risk a humiliating withdrawal, the options are stark; in Luttwak’s words, the public will need to ‘learn not to see, hear or feel much that would otherwise offend their moral sensitivities... to “step over the beggar in their path.”’

Assuming Britain continues to adopt a pragmatic approach to military intervention, it is important that the political-military leadership is prepared to defeat the asymmetric challenges that are likely to be encountered. RAND identify three factors which potentially detract from this readiness: first, a lack of strategic appreciation of the potential opponent’s capabilities; second, a lack of tactical and operational appreciation of their methods; and, finally, the inevitable time lag for, and inherent difficulty in, implementing the necessary responses. The responses, or countermeasures, were assessed in Chapter VI, and Britain’s requirements can be summarised as follows:

- A robust nuclear force, plus a precision-guided conventional weapons capability, for deterrence and counterforce purposes.
- A clear statement of deterrence policy with regard to adversary CBW use; potentially a doctrine of ‘no-first-use of WMD’; or, alternatively, a deliberately ambiguous declaratory policy.
- The deployment of a BM defence umbrella, with which to protect forward-deployed forces and allies, vulnerable dependent territories or symbolic domestic targets.
- A comprehensive NBC Defence Doctrine, which emphasises the emerging BW threat, for both military and civil defence.
- The enhanced protection of vital maritime assets against air, cruise missile and sub-surface attack.
- The provision of dedicated, specifically trained and equipped defence forces to protect static HVA (air bases, ports, logistics depots).
- A comprehensive ‘force protection’ doctrine targeted at the protection of personnel and HVA against terrorism and SPF operations.
- A robust domestic counter-terrorism strategy.
- A strategy to identify and protect both the military and national MEII against EMP and cyber-attack.

In Britain, many of these capabilities are in place or under development; however, in its report on the SDR, the HCDC concluded:

‘We find that the Review has ignored the questions of the protection against [WMD] of troops at home, and of liaison with civil defence facilities for the

---

223 Luttwak, E.N., ‘Where are the Great Powers? At Home with the Kids’ Foreign Affairs, (July/August 1994), 27.
224 ‘Richer inhabitants of the poorest countries learn from childhood how to step politely over the quadruple-amputee beggar in their path without ever actually looking at him... Blindness can be learned, and Americans will have to learn how to passively ignore avoidable tragedies and horrific atrocities.’ Luttwak, Ibid., 28.
protection of the civil population. It has confined its examination of protection against chemical and biological weapons to an expeditionary context. Nor has it made explicit the government’s policy for nuclear deterrence at the strategic and sub-strategic levels. We cannot afford to allow our reliance on the nuclear deterrence to become our only, or our first, line of defence against such threats.”

Moreover, with respect to the White Paper’s single paragraph devoted to BM defence, that: ‘...it would, at this stage, be premature to decide on acquiring such a capability’ the HCDC condemned the government’s ‘reticence’, noting that:

‘It may take a decade or more to develop and field a new air defence system. Policy in this area needs to be clear, kept under constant review, decisions on research on options for responses to these threats need to be made in the near future, and the research needs to be adequately funded.’

Subject to the publication of the 1999 Defence White Paper there remains no clear public statement on these issues.

The paradox of making the first move in deploying countermeasures which deter, pre-empt or defend against potential asymmetric challenges is that this strategy cedes the second-move advantages to the opponent by simply shifting the ‘cone of vulnerability’. However, it is important to keep the threat in perspective; as RAND judiciously points out:

‘Few asymmetric CONOPs are “silver bullets”... however, a synergy of asymmetric efforts may prove decisive in major conflicts and a single asymmetric act may be a “silver bullet” against less-than-vital interests.’

In short, there are few answers, but there is one certainty; that it is in Britain’s interest to have the debate about emerging asymmetric challenges and then to put necessary policies, doctrine and budgets in place to ensure the adequate defence and security of the country and its national interests as we enter the new Millennium.

226 HCDC, op. cit., clxiv.
227 Ibid., lxxxiv.
228 Bennett et al., op. cit., 7.
BIBLIOGRAPHY

Books


Journals


*French Defence Monitor* (Vol. 1, No. 1, August 1994).

*Programme for Promoting Nuclear Non-Proliferation: Newsbrief*, (No. 30, 2nd Quarter 1995).


Articles


Butcher, T., ‘US air cavalry to the rescue - but when will it attack?’, Sunday Telegraph (25 April 1999).

Cameron, G., ‘Nuclear Terrorism: a real threat?’ Jane’s Intelligence Review (September 1996).


Croddy, E., ‘Putting the lid back on the chemical box’ Jane’s Intelligence Review (January 1998).


Graves, D., ‘CIA thought British computer boy was more harmful than the KGB’ Daily Telegraph, (22 March 1997).


Luttwak, E.N., ‘Where are the Great Powers? At Home with the Kids’ Foreign Affairs, (July/August 1994).


Venter, A., ‘Biological warfare: the poor man’s atomic bomb’ Jane’s Intelligence Review (March 1999).

Walker, M., ‘Europe takes the first steps to common defence policy’ The Guardian (3 June 1999).


‘CIA chief fears “cyber attacks”’, BBC On-line, (published at 05.05 GMT 25 June 1998).

‘Terror Times Two’ Newsweek (17 August 1998).


Unattributed ‘British put on TV by Serb army: UN captives labelled ‘prisoners of war’ as injured soldiers are shown in Bosnian hospital’ The Daily Telegraph (30 May 1995).

Government Papers


• Garden, Sir Timothy, cited in ‘Minutes of Evidence Taken Before The Defence Committee (22 July 1998)’

• ‘Memorandum submitted by Dr. Philip Sabin on the Strategic Defence Review’


Papers/Reports

Badsey, S., ‘Modern Military Operations and the Media’ The Occasional No. 8 (Strategic and Combat Studies Institute, 1994).


Miscellaneous


Interviews/Conference Proceedings

Gouré, D., Deputy Director Political-Military Studies, Center for Strategic and International Studies (CSIS), Washington, in an interview 5 May 1999).


The following interviews are not specifically cited in this dissertation; however, the discussions proved invaluable in informing the author’s broader understanding of the issues concerned:


Collins, Dr. J. Senior Fellow (Political-Military Studies), Center for Strategic and International Studies (CSIS), Washington, in an interview 5 May 1999.

Hoffman, Dr. B., Director, RAND Washington Office, in an interview 11 May 1999.


Matarazzo, Colonel D.T. USAF, Deputy Director of Security Forces, Headquarters Air Mobility Command (and Security Forces Directorate staff) in interviews 5-6 May 1999.
