A Study of the Capability of the Armed Forces of Thailand, the United Kingdom and the United States of America to Deliver Domestic Disaster Relief Operations as a Distinct Military Task

By

Colonel Roger Lewis

British Defence Attaché

British Army

Student of the National Defence College

The National Defence Course : Class 59

Academic Year 2016 – 2017

Preface

During my time in the British Army I have frequently witnessed, either first hand or vicariously, the armed forces of various nations being used to mitigate an imminent but predictable disaster or assist in the immediate aftermath. Rarely though have they been perfectly suited, equipped and resourced for the task assigned, and usually they have been given that task when every other avenue has been exhausted: a classic example of 'too little, too late'. The approach to deploying each armed forces has varied significantly by country but, nevertheless, normally follows similar principles allowing them to be compared.

Understanding the ability of an armed force to support the demands of its own nation is self-evidently of importance. Gen Charles H. Jacoby USA, a previous Commander United States Northern Command & North America Aerospace Defence Command, regularly stated that "it is too late to exchange business cards during a crisis", which is why an early consideration of the logic train from National Risk Register to military tasking will pay dividends. Understanding who can do what, when, where, how and, importantly, why, is always of significance and made even more germane during a period of national threat. Gaps in the logic train could prove hugely expensive in terms of both lives lost and opportunities missed. The purpose of this study, therefore, is to help prevent such a situation arising.

Choosing which countries to study was remarkably simple: the country I am from; the UK, the country in which I am currently living; Thailand, and the country in which, save my own, I have lived and worked the longest; the USA. Whilst the scope of the research was inevitably constrained by the availability of unclassified information and the challenge of language, experience gained from extensive exposure to the system employed in the UK and the USA, enabled a useful comparison to be made to the one in Thailand. I hope this paper, in some small way, helps others to assess their own system and, perhaps, make enhancements.

(Col Roger Lewis, British Army and Defence Attaché)
Student of the National Defence College
Course: NDC Class: 59
Researcher

Contents

		Page
Abstract		**i**
Preface		**ii**
Acknowledgement		**iii**
Contents		**iv**
Contents of Figures		**vii**
Chapter 1	**Introduction**	**1**
	Background and Importance of the Problem	1
	Objectives of the Research	4
	Scope of the Research	4
	Research Methodology	4
	Limitations and Delimitations of the Research	7
	Research Utilisation	7
	Definitions	7
Chapter 2	**National Threat Scenarios**	**9**
	Threat Types	9
	Individual	10
	Organisational	11
	National	16
	UK	17
	USA	23
	Thailand	28
	International	37
	Scale of Threat	37
	Rate of Occurrence	39
	The Most Likely Common Scenarios	40
	Down Selected Common Scenarios	42

Contents (Cont.)

		Page
Chapter 3	**National Tasking Mechanisms**	**43**
	National Tasking Procedures	43
	The UK	
	Ends	44
	Ways	47
	Means	50
	The USA	
	Ends	54
	Ways	58
	Means	63
	Thailand	
	Ends	66
	Ways	71
	Means	79
Chapter 4	**Meeting the requirement: Supply and Demand**	**83**
	Equilibrium – The quest for the Holy Grail	83
	Assessing Supply	84
	The Disaster Management Cycle	84
	Capability Management Frameworks	88
	UK Defence Lines of Development	88
	Assessing Demand	89
	Scenarios	90
	Six Honest Serving Men	90
	Supply and Demand	91
	The UK	92
	The USA	95
	Thailand	98
Chapter 5	**Conclusion and Recommendations**	**101**
	Conclusion	101
	Results	103
	Question 1	103
	Question 2	104
	Question 3	104

Recommendations 106

Contents (Cont.)

Page

Bibliography 108

Biography 114

Contents of Figures

Figure No.		Page
1 – 1	Research Methodology	6
2 – 1	Risk of Terrorist and Other Malicious Attacks	20
2 – 1	Other Risks	20
2 – 3	Likely Form of Central Government Engagement based on the Impact and Geographic Spread of an Emergency in England	23
2 – 4	SNRA National Level Events	24
2 – 5	UNDP Thailand Hazard Assessment	29
2 – 6	DDPM Disaster Rankings	30
3 – 1	Generic Command and Control Model for Resilience/Security Operations	48
3 – 2	Presidential Policy Directive 8	55
3 – 3	Core Capabilities	56
3 – 4	FEMA Regions	61
3 – 5	DSCA Phases	62
3 – 6	Disaster Risk Management Strategy	70
3 – 7	Disaster Risk Management Cycle	71
3 – 8	Activation Levels	72
3 – 9	Disaster Risk Management Mechanisms	76
3 – 10	Interagency Relationships and Collaborative Linkages for Emergency Management Operations	78
3 – 11	Military Disaster Relief Centres	79
4 – 1	The Ideal Relationship Between Supply and Demand – The ‘Holy Grail’	83
4 – 2	The 4-way Relationship Between Demand and Suppliers	84
4 – 3	The Disaster Management Cycle	85
4 – 4	Graphic Representation of UK’s Demand and Supply Balance	92
4 – 5	Graphic Representation of USA’s Demand and Supply Balance	95
4 – 6	Graphic Representation of Thailand’s Demand and Supply Balance	98

Chapter 1
Introduction

Background and problem

> *"Spectacular achievement is always preceded by unspectacular preparation".*[1]

> *"O it's Tommy this, and Tommy that, and Tommy 'ow's your soul? But it's thin red line of heroes when the drums begin to roll."*[2]

1. The language will vary, the tone differ and the rhetoric fluctuate but most nation states would probably agree that the primary purpose of meeting the significant expense of raising, equipping and maintaining an armed force is to protect and defend itself against threats to its safety and very existence. Whether those threats materialise from internal or external sources; whether they are enduring or contemporary; or whether, amongst other criteria, they are violent, virtual or environmental, the government-of-the-day must match the demands it places on its armed forces with the resources it allocates to achieve them. Demand will always outstrip supply and thus an amount of prioritisation will be required.

2. The challenge facing both central government and the Armed Forces themselves is how to balance the competing demands they face in such a way to ensure they can achieve an acceptable measure of success across a broad array of requirements. Is an army that spends its time training for a fight that never materialises the very acme of success – deterrence may have worked – or a significant failure – a waste of resources that could better have been spent elsewhere? The answer to that particular riddle will, no doubt, come down to a matter of perspective and vested interest; on which side of the fence the reader sits. Nevertheless, it hints neatly at an inability to be able to measure intangibles such as 'inaction' and the near impossibility to accurately predict the future. There is no 'one-size-fits-all' solution, no 'correct' answer to the question "What will we need, and when will we need it?" Each nation and each Armed

---

[1] Robert H. Schuller, 1979

[2] Rudyard Kipling, The Barrack-Room Ballads and Other Verses, 1892

Force must come to its own conclusion consistent with its own situation, resources and ambition.

3. The self-evident difference that sets military units apart from the vast majority of other collective national organisations is that they are armed. They are structured, equipped and trained, albeit to varying degrees, to exert violent force when required to do so, for a political purpose – Clausewitz's dialectic thesis 'war is merely the continuation of policy by other means' aptly applies. Yet, notwithstanding this remit, most have other non-violent tasks to fulfil including, for example, International Defence Engagement, Public Duties[3], and Humanitarian Assistance and Disaster Relief Operations (HADR). [Although classified here as non-violent it would be remiss not to acknowledge that military forces may be called upon to use violence during HADR Operations, not least for the purpose of self-defence.] In the case of most modern-world countries precisely what the list of tasks will be, and who specifically is responsible for carrying them out, can be derived from an examination of National interests, objectives and resultant strategy. It is less obvious, however, whether the allocation of resources to meet these tasks is similarly well defined.

4. In order to consider the relationship between domestic Disaster Relief Operations (DR Operations) and the role of the military three countries have been selected on the basis of:

a: The availability of information.

b: Their repeated and recent use in DR Operations.

c: Their scale.

d: The author's existing knowledge.

They are: Thailand, the United Kingdom and the United States of America. All three militaries have a standing remit to conduct domestic DR Operations when so tasked, but their scale, authority and priorities vary of necessity. The relationship between geographical area, population size,

[3] Public Duties is a UK military term that covers activity that usually has a ceremonial or historic significance rather than an overtly operational role.

density, military and gross domestic product (GDP) per capita provides a useful insight into the differing challenges they face.

Country	Area	Pop	Density	Armed Forces	GDP per cap
Thailand	0.51M km^2	68M	131/km^2	0.698M	$16.7k
UK	0.24M km^2	65M	255/km^2	0.255M	$43.9k
US	9.82M km^2	322M	34/km^2	2.35M	$49.9k

5. Each of the three subject countries faces a range of 'threat scenarios' against which they need to plan and organise. Even a cursory examination of the potential challenges, for example: environmental (e.g. pandemic), geographical (e.g. flood), man-made (e.g. chemical leak), demonstrates the significant complexity involved in preparing for such eventualities. Understanding the nature and scale of these threats is paramount, however, for without it the Armed Forces may be expected to achieve unrealistic levels of support and national planning assumptions will lack rigour, allowing capability gaps to develop.

6. Predicting an appropriate balance of capability development within the military is fraught with the potential for miscalculation and conflicting aims. Similarly, understanding which assets might have a dual-role capability is not always obvious or simple. By way of stark example, the impact of a Multiple Launch Rocket System (MLRS) on a battlefield is fairly obvious yet it is harder to envisage a direct role for it in an HADR Operation. Nevertheless, components of the system may indeed be of use because the system comes with, amongst other things, command & control assets, logistic vehicles and re-deployable personnel.

Problem Statement

7. Matching the appropriate allocation of resources to meet a domestic DR Operation is fraught with difficulty and made even more challenging because it is, usually, not the primary driver for raising and sustaining a standing armed force. The purpose of this research paper is, therefore, to consider the most likely domestic Disaster Response Operation demand signal that might be placed upon the armed forces of Thailand, the United Kingdom and the United States of America and,

using a capability development framework, analyse their ability to meet it. Put simply: what has the military been asked to do and can they do it?

Objectives of the research

8. The paper will address 3 primary questions:

a. What is the nature and scale of the most likely domestic DR Operation 'threat scenarios' in Thailand, the United Kingdom and the United States?

b. What have/will the armed forces of each country be asked to do?

c. To what extent can the armed forces of each country meet the requirement?

Scope of the research

9. The risk inherent in this research project is the sheer size and scope of potential disasters, man-made or otherwise, that could affect each country in the future; and the inability to accurately predict what will actually happen. As the primary aim of the paper is to assess the logic train each armed force is following and identify the capability development decisions they are taking, the threat scenario research will be confined to a manageable proportion designed to identify the most likely, rather than necessarily the most dangerous or apocalyptic situations.

10. Some of the details required to conduct this research would, of necessity, be classified and therefore unpublishable, and, in the case of Thailand and the USA, not made available to the author. To that end the research will concentrate on information freely and publically available.

Methodology (see Figure 1 below for the numbered Steps)

11. The primary questions will be analysed as follows:

a. In order to understand the challenge facing each armed force Question 1 will benchmark the potential threats in terms of their nature and scale relative to the country by both population and territory (Step 1.1). A representative selection of the most likely,

larger scale scenarios, common to all 3 countries will be identified. (Step 1.2) Where relevant reference will be made to unclassified versions of national risk registers.

b. A ‘Mission Analysis’ will be conducted in Question 2 in order to identify what the armed forces have been tasked to do, and the logic train behind that direction (Ends, ways and means). (Step 2.2) It will seek to identify in what way the assigned Military Tasks contribute to, and meet the respective National Strategy, and what comparisons can be drawn between the 3 countries. Any gaps identified at this point will be taken forward for discussion later in the paper. (Step 2.2)

c. Having extracted the defined military tasks, and any that are implied, the ability of each armed force to meet the requirement (Question 2) will be assessed against the back drop of the 5 threat scenarios (Question 1) through the prism of the Defence Lines of Development and the Disaster Management Cycle. (Step 3.1) Strengths, weaknesses and gaps, including those brought forward from Step 2.2, will be identified.

d. The paper will be drawn together at Step 4, and then make recommendations that can be used to update each nation’s approach to Humanitarian Assistance and Disaster Relief Operations.

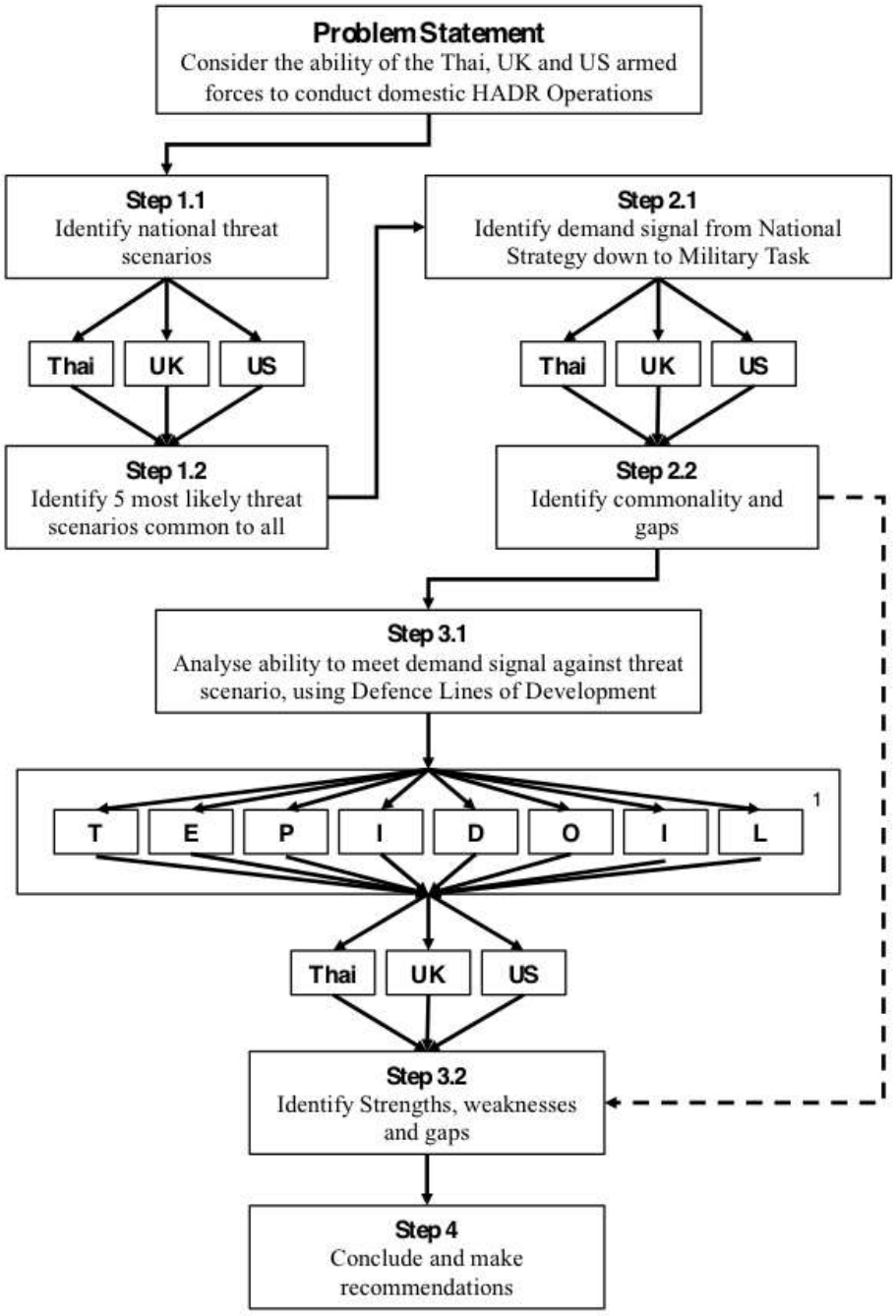


Figure 1. Research Methodology

[1]Training, Equipment, Personnel, Information, concepts & Doctrine, Organisation, Infrastructure, Logistics

Limitations and delimitations

12. The time frame for consideration of capability development will be limited to no more than 20 years due to the inability to accurately predict demand signals over a longer term.

13. The paper has specifically been delimited to consider only domestic DR Operations. The complexity involved in considering the ability to conduct similar operations abroad is just too broad to be dealt with in the time available. Although there is a significant moral component to providing Humanitarian Assistance, it is generally considered to be a secondary Military Task and thus it would be very unusual for overseas HADR operations to act as a driver for capability development.

Research utilisations

14. Understanding the ability of each armed force to support the demands of its own nation is self-evidently of importance. Gen Charles H. Jacoby USA, a previous Commander United States Northern Command & North America Aerospace Defence Command, regular stated that "it is too late to exchange business cards during a crisis". Understanding who can do what, when, where, how and, importantly, why, is always of significance made even more germane during a period of national threat. Gaps in the logic train could prove hugely expensive in terms of both lives lost and opportunities missed. The purpose of this study, therefore, is to make a comparative assessment of the 3 nations to help prevent such a situation arising.

Definitions

15. It is assumed that the three countries have a similar understanding of the type of operation addressed in this research paper but define it using different terms. In particular, differing terminology is often used depending on whether a relief operation is being conducted overseas (abroad) or domestically (within the sovereign territory of the troop supplying nation). For the purpose of this paper the UK definitions, taken from Joint Doctrine Publication 3-52 Disaster Relief Operations[4] serve as a suitable basis to enable discussion:

[4] UK JDP 3-52 Disaster Relief Operations (2nd Edition) published 21 Dec 12.

a. **Humanitarian Disaster**. A humanitarian disaster is a catastrophe the consequences of which put lives and/or livelihoods at risk, and exceeds the ability of the affected society to cope using only its own resources.

b. **Disaster Relief**. Disaster Relief is the organised response to alleviate the results of a catastrophe. The aims are to save life; relieve suffering; limit damage; restore essential services to a level that enables local authorities to cope.

c. **Disaster Relief Operations (DRO).** A DRO is a primary Military Task and contribution to a disaster relief response. It provides specific assistance to an afflicted population.

d. **Resilience**. The ability of the community services area or infrastructure to withstand the consequences of an incident. It should be noted that in military terminology resilience is defined as, 'the degree to which people and capabilities will be able to withstand, or recover quickly from, difficult situations. Wherever possible, capabilities, systems and munitions that have utility across a range of activities, high levels of reliability and robustness should be procured'.

e. **Military Aid to the Civil Authorities (MACA)**. The collective term given to the 3 types of operations which may take place in a civilian environment: Military Aid to the Civil Community (MACC), Military Aid to the Civil Ministries (MACM) and Military Aid to the Civil Powers (MACP).

Chapter 2
National Threat Scenarios

"Bad things do happen in the world, like war, natural disasters, disease. But out of those situations always arise stories of ordinary people doing extraordinary things".[1]

"We cannot stop natural disasters but we can arm ourselves with knowledge: so many lives wouldn't have to be lost if there was enough disaster preparedness."[2]

"If you can meet with Triumph and Disaster
And treat those two impostors just the same; ...
Yours is the Earth and everything that's in it"[3]

Threat Types

1. The nature of the threat scenarios facing each country will, by definition, drive the planning and the response to it. No two situations will be exactly the same and whilst history may mimic itself, it will never repeat identically. Understanding the characteristics and the scale of each threat scenario is therefore critical in order to make certain that an appropriate amount of resources is allocated ahead of time or made available once a crisis occurs. Too much, and the chances are that finite commodities are being wasted, too little, and the likelihood of systemic failure grows proportionally.

2. Henry Kissinger, the former US Secretary of State and National Security Advisor, once bemoaned that "there cannot be a crisis today; my schedule is already full"[4]. Most people in a position of responsibility would perfectly understand the sentiment of his comment and recognise that getting ahead of an emergency is therefore hugely beneficial to a successful outcome because once it strikes, quick decisions

---

[1] Daryn Kagan – News Anchor, 2012.
[2] Petra Němcová – Supermodel, 2011.
[3] Rudyard Kipling, Brother Square-Toes – Rewards and Fairies, 1910.
[4] RQA Inc, Crisis Control Newsletter, Vol U0110 Issue 1, Jan 2010.

will be necessary and time will be in short supply. Kissinger's remark does not, of course, define what constitutes a crisis, which can have an effect at an individual, organisational, national, or even international level.

3. **Individual**. In their article, 'Crisis Intervention[5]' Kneisl and Riley define 3 types of crisis that affect the individual:

> a. Situational (or unanticipated). Situational crises originate from three factors: material or environmental such as a fire or a natural disaster; personal or physical such as a heart attack, the diagnosis of a fatal illness, or bodily disfigurement; and interpersonal or social, such as the death of a loved one, divorce, or the loss of a job. These events are unplanned and unexpected.
>
> b. Traditional (or developmental). This type of crisis involves two major areas: developmental transitional states or situational transitional states.
>
> 1) Developmental states are composed of normal and expected life cycle changes based on predicted human development. Significant changes accompany these stages.
>
> 2) Situational transitional states include significant life events like marriage, the birth of a child, retirement or first-time employment. Though anticipated, the changes necessary for the transition create anxiety and tension
>
> c. Cultural and social (or adventitious). These crises involve such events as robbery, rape, incest, marital infidelity, physical abuse, and hostage situations. This form of crisis is unpredictable and not under the individual's control.

It is clear from their classification that what constitutes a crisis on a personal level is frequently unexpected, or, if predictable, for which the consequences have largely remained unplanned for. Similarly, what constitutes a crisis for one person may be more mundane, almost routine, for another. Taken to an extreme 'one man's crisis is another man's

---

[5] Kneisl, C & Riley, E. 'Crisis Intervention' Psychiatric Nursing (5th edition), 1996.

opportunity'[6] and thus not all would agree that for any given event it should be classified as a crisis at all: it is always a matter of personal perspective and perception.

4. **Organisational**. According to Seeger, Sellnow and Ulmer[7] there are 3 elements common to a crisis:

a. A threat to an organisation.

b. The element of surprise.

c. A short decision time.

Venette, however, adds a fourth, namely 'the need for change', arguing that crisis is a process of transformation where the old system can no longer be maintained. If change is not needed the event could more accurately be described as a failure [or simply] an incident[8]. The Management Study Guide[9] provides a complimentary but more detailed breakdown of potential crisis types articulating that crises are sudden unplanned events that cause major disturbances in an organisation and trigger a feeling of fear and threat amongst employees. They define crises as falling into the following types:

d. Natural Crisis

1) Disturbances in the environment and nature lead to natural crisis.

2) Such events are generally beyond the control of human beings.

---

[6] Slaves and Masters, Jerry Horne in Twin Peaks, Series 2, Episode 15, Slaves and Masters, 1991.

[7] Communication, organisation and crisis", Seeger, M. W.; Sellnow, T. L.; Ulmer, R. R. Communication Yearbook. 21: 231–275, 1998.

[8] Risk communication in a High Reliability Organization: APHIS PPQ's inclusion of risk in decision making. Ann Arbor, MI: UMI Proquest Information and Learning, Venette, S.J, 2003.

[9] Management Study Guide http://www.managementstudyguide.com/types-of-crisis.htm, retrieved Mar 2017.

3) Tornadoes, earthquakes, hurricanes, landslides, tsunamis, flood, drought all result in natural disaster.

e. Technological Crisis

1) Technological crisis arises as a result of failure in technology. Problems in the overall systems lead to technological crisis.

2) Breakdown of machines, corrupted software and so on give rise to technological crisis.

f. Confrontation Crisis

1) Confrontation crises arise when employees fight amongst themselves. Individuals do not agree with each other and eventually depend on non-productive acts like boycotts, strikes for indefinite periods and so on.

2) In such a type of crisis, employees disobey superiors; give them ultimatums and force them to accept their demands.

3) Internal disputes, ineffective communication and lack of coordination give rise to confrontation crisis.

g. Crisis of Malevolence

1) Organisations face crisis of malevolence when some notorious employees take the help of criminal activities and extreme steps to fulfil their demands.

2) Acts like kidnapping a company's officials, [or simply] false rumours, all lead to crisis of malevolence.

h. Crisis of Organisational Misdeeds

1) Crises of organisational misdeeds arise when management takes certain decisions knowing the harmful consequences of the same towards the stakeholders and external parties.

2) In such cases, superiors ignore the after-effects of strategies and implement them regardless, searching for quick results.

Crisis of organisational misdeeds can be further classified into the following three types:

a) Crisis of Skewed Management Values

i. Crisis of Skewed Management Values arises when management supports short term growth and ignores broader issues.

b) Crisis of Deception

i. Organisations face crisis of deception when management purposely tampers data and information.

ii. Management makes fake promises and wrong commitments to the customers. Communicating wrong information about the organisation and products lead to crisis of deception.

c) Crisis of Management Misconduct

i. Organisations face crisis of management misconduct when management indulges in deliberate acts of illegality like accepting bribes, passing on confidential information and so on.

i. Crisis due to Workplace Violence. Such a type of crisis arises when employees [engage]in violent acts such as beating employees, [or] superiors in the office premises itself.

j. Crisis Due to Rumours

1) Spreading false rumours about the organisation and brand lead to crisis. Employees must not spread anything which would tarnish the image of their organisation.

k. Bankruptcy

1) A crisis also arises when organisations fail to pay their creditors and other parties.

2) Lack of fund leads to crisis.

l. Crisis Due to Natural Factors. Disturbances in environment and nature such as hurricanes, volcanoes, storms, flood; droughts, earthquakes etc. result in crisis.

m. Sudden Crisis

1) As the name suggests, such situations arise all of a sudden and on an extremely short notice.

2) Managers do not get warning signals and such a situation is in most cases beyond anyone's control.

n. Smouldering Crisis

1) Neglecting minor issues in the beginning leads to smouldering crisis later.

2) Managers often can foresee crisis but they should not ignore the same and wait for someone else to take action.

3) Warn the employees immediately to avoid such a situation.

Regardless of the type of crisis that unfolds, in order to achieve a successful outcome, Gonzales-Herrero and Pratt [10] articulate that organisations must have a crisis management plan consisting of 3 stages:

[10] Ibid.

o. Diagnosis of Crisis

1) The first stage involves detecting the early indicators of crisis. It is for the leaders and managers to sense the warning signals of a crisis and prepare the employees to face the same with courage and determination. Superiors must review the performance of their subordinates from time to time to know what they are up to.

2) The role of a manager is not just to sit in closed cabins and shout at his subordinates. He must know what is happening around him. Monitoring the performance of the employee regularly helps managers to foresee crisis and warn employees against the negative consequences of the same. One should not ignore the alarm signals of crisis but take necessary actions to prevent it.

p. Planning

1) Once a crisis is detected, the crisis management team must immediately jump into action. Ask the employees not to panic, devise relevant strategies to avoid an emergency situation and it is essential to take quick decisions.

q. Adjusting to Changes

1) Employees must adjust well to new situations and changes for effective functioning of the organisation in the near future. It is important to analyse the causes which led to a crisis at the workplace. Mistakes should not be repeated and new plans and processes must be incorporated in the system.

The main objective of crisis management at the organisational level is to protect employees, consumers and customers, as well as, company assets, brands and corporate image[11]. The key tenant is organisational survival and the ability to return to normalcy in the shortest possible time. Crisis management is a distinct concept separate from risk management,

[11] RQA, Inc.op.cit.

which involves assessing potential threats and seeking to avoid or mitigate them in advance. Crisis management deals with threats before, during and after they have occurred.

5. **National**. Whilst a crisis at a national level will inevitably contain many of the same elements as those taken into consideration by individuals and organisations the likely scale, impact and, frequently, loss of life involved only serves to increase the importance of preparation. In his book on Ongoing Crisis Communication Timothy Coombs highlights a wide-array of crises that should be planned for and managed[12]:

a. Natural Disasters: Tornadoes, earthquakes, hurricanes, floods, droughts, severe storms, etc.

b. Malevolence: Product tampering, sabotage, kidnapping, terrorism, malicious rumours.

c. Product Recall: Misbranded, adulterated, or violated product in the market.

d. Confrontation: Boycotts, picketing, protests, ultimatums.

e. Hazardous Materials: Spills, leaks, build-up of toxic materials, etc.

f. Technological Breakdowns: Software failures, hardware failures, infrastructure collapse, computer viruses.

g. Utilities Failure: Power outages, gas, water, sewer, garbage.

h. Human Error: Mistakes that cause significant damage or loss to a company.

i. Workplace Violence: Violent actions against other in the workplace.

---

[12] Ongoing Crisis Communication: Planning, Managing, and Responding", W. Timothy Coombs, 2007.

j. Medical Emergencies: Heart-attacks, broken bones, lacerations.

k. Organisational Misdeeds: Deception, management misconduct, misrepresentation, illegal actions.

Although Coombs' writing was aimed primarily at organisations much of his classification is applicable at the national level. There are, however, many additional events that should also be considered. Set out below, by country, are the major areas of concern to the UK, USA and Thailand.

l. **UK**. The Central Government arrangements for responding to an emergency, published by the Cabinet Office[13], describes an emergency (or disruptive challenge) as a situation or series of events that threatens or causes serious damage to human welfare, the environment or security in the United Kingdom. This definition covers a wide range of scenarios including, for example, adverse weather, severe flooding, animal diseases, terrorist incidents and the impact of a disruption on essential services and critical infrastructure. This is expanded upon in The Civil Contingencies Act 2004, which describes an emergency (i.e. a crisis) as:

1) An event or situation which threatens serious damage to human welfare in a place in the United Kingdom.

2) An event or situation which threatens serious damage to the environment of a place in the United Kingdom.

3) War, or terrorism, which threatens serious damage to the security of the United Kingdom.

Having pithily articulated what constitutes an emergency the National Risk Register of Civil Emergencies goes on to provide a catalogue of the highest priority risks facing the UK[14].

---

[13] UK Central Government Arrangements For Responding To An Emergency, An Overview – Published by The Cabinet Office, March 2010.

[14] 2015 National Risk Register of Civil Emergencies © Crown Copyright, 2015.

4) Pandemic influenza – This continues to represent the most significant civil emergency risk. The outbreak of H1N1 influenza in 2009 (‘swine flu’) did not match the severity of the scenario that was planned for and is not necessarily indicative of future pandemic influenzas. The 2009 H1N1 pandemic does not change the risk of another pandemic emerging (such as an H5N1 (‘avian flu’) pandemic) or mean that the severity of any future pandemics will be the same as the 2009 H1N1 outbreak.

5) Coastal flooding – The risk is of an event similar in consequence to the 1953 east coast flooding emergency caused by a combination of high tides, a major tidal surge and onshore gale force winds. The consequences of the storm surge in December 2013 were less serious even though sea levels were higher than in 1953. Our assessment is that the likelihood of such severe consequences as in 1953 is lower now due to the investment made in coastal flood defences and flood warnings. [It is worth noting here that the UK has followed its own advice and sought to mitigate the risk of a serious crisis by allocating resources ‘left of the event’. In other words, before a crisis occurs. The only way to measure the effectiveness of this approach is to note the absence of failure. Whether more resources were used than truly necessary is almost impossible to discern, however, should another major flood occur, it will be possible to identify an underspend.]

6) Widespread electricity failure – Previously a risk grouped within the major industrial accidents risk category, the risk of widespread electricity failure has been reassessed in light of an enhanced understanding of the risk’s impacts. As a result, is now assessed to be very high, and thus a priority risk. Although the UK has never before suffered a national loss of electricity, and this does not represent an increase in likelihood, the consequences of such an event could be significant. [Risk has been measured on two distinct but interconnected scales, namely the likelihood of an incident occurring and the impact on the country should it do so. Combining the effect of the two scales suggests, in this

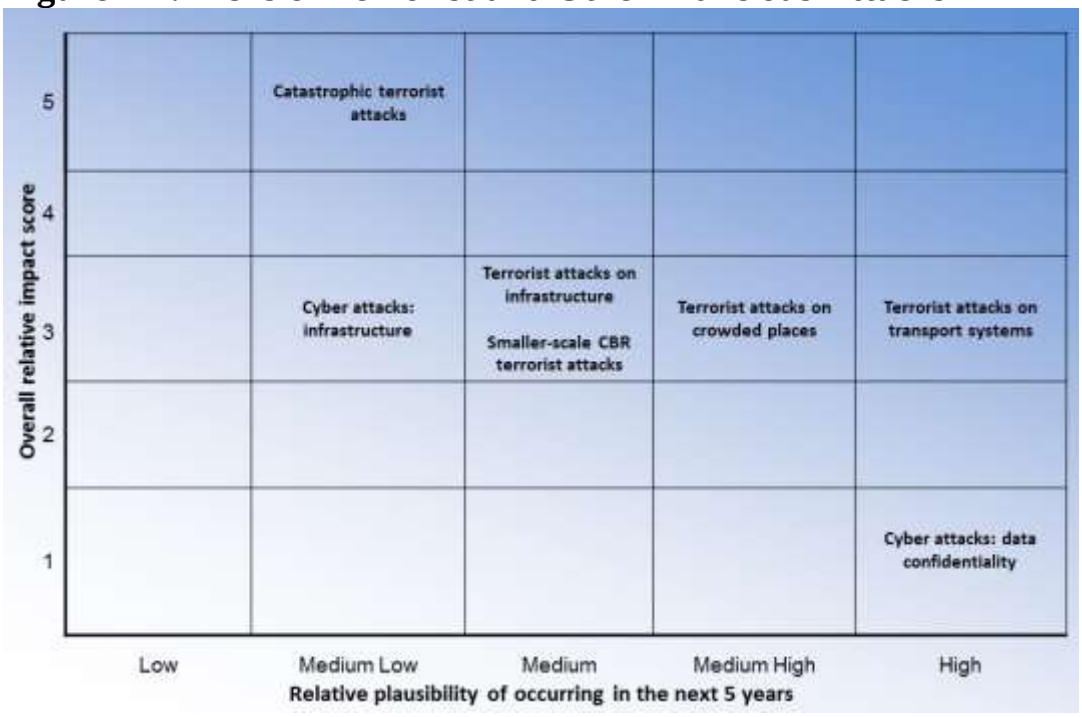
instance, that more resources than hitherto considered should be allocated to mitigate this threat.]

7) Catastrophic terrorist attacks – This type of attack causes long term mass impacts of a magnitude over and above conventional terrorist attacks such as those targeting crowded places or transport systems. Catastrophic terrorist attacks are assessed to be less likely that conventional terrorist attacks. Although catastrophic terrorist attacks are unlikely, they cannot be ruled out. The likelihood of terrorists obtaining effective mass impact biological agents or a functioning nuclear device remains low but not negligible, and the impacts are potentially very serious. [A catastrophic terrorist attack can be measured by occurrence or by an assessment of plots that have been detected, disrupted or defeated. Whether they have been successfully deterred is immeasurable and thus resource allocation is harder to judge.]

8) Poor air quality events – Air pollution harms the environment and can also lead to significant effects on health, particularly for those who suffer from respiratory or cardio-vascular conditions. Ozone and fine solid particles and liquid droplets suspended within the air are the two main causes of poor air quality events and are more likely to occur during heatwaves, as experienced in 2003, 2006 and 2011, when high temperatures and light winds helped to create the necessary conditions. Poor air quality may also occur at other times of the year, particularly in longer periods of settled weather, where high pressure dominates. [It is worth comparing the largely predictable (based on recurring instances) but 'slow burn' impact of poor air quality with that of far less predictable (based on infrequency) but shock impact and suddenness of a catastrophic terrorist attack. Relatively speaking it is much easier to measure the risk of the former on a daily basis (air quality measurement) and thus adjust the resources being allocated to prevention and mitigation than the latter.]

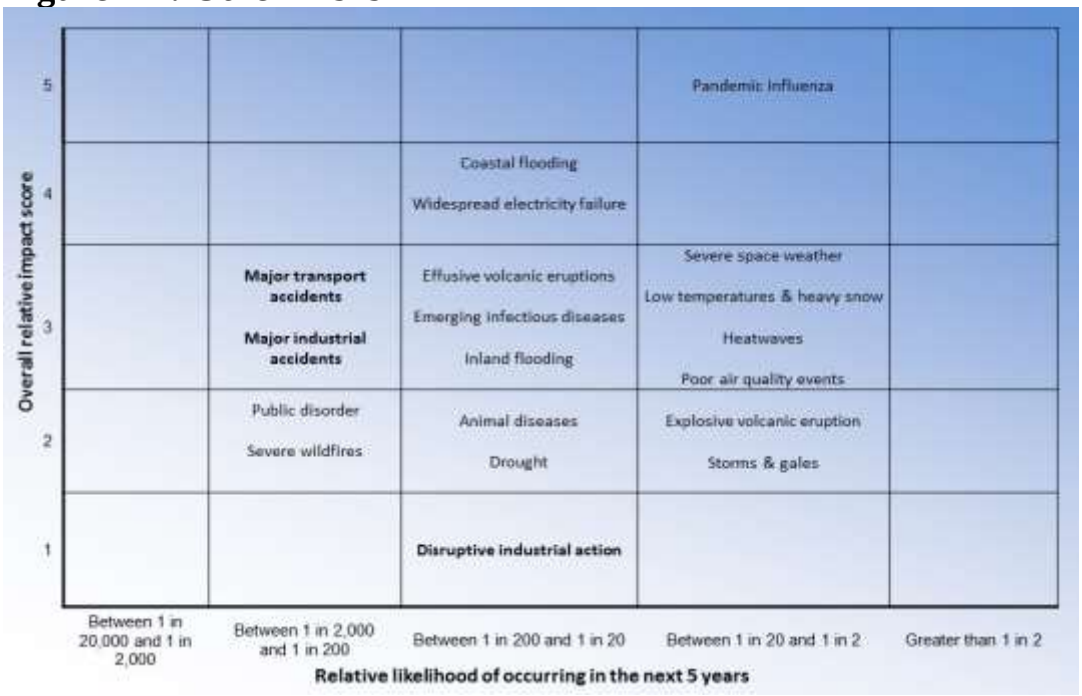
The Government's assessment of the key risks facing the country, set out by impact, plausibility and likelihood are shown in Figures 2-1 and 2-2 below.

Figure 2-1: Risks of Terrorist and Other Malicious Attacks



Source: UK National Risk Register, 2015: Page 12

Figure 2-2: Other Risks



Source: UK National Risk Register, 2015: Page 13

As well as setting out the risk, the Cabinet Office Concept of Operations for the UK Central Government Response to

Emergencies[15] the document sets out the Levels of Emergencies and narrows down what constitutes a National level scenario.

9) The principle of subsidiarity emphasises the importance of local decision making supported, where necessary, by co-ordination at a higher level. In order to aid planning, further understanding, and provide guidance to responders and central government planners on when they might expect central government involvement in responding to an incident, three broad types (or levels) of emergency have been identified which are likely to require direct central government engagement. These are:

a) **Significant emergency (Level 1)** has a wider focus and requires central government involvement or support, primarily from a lead government department (LGD) – or a devolved administration [such as Scotland or Wales], alongside the work of the emergency services, local authorities and other organisations. There is however no actual or potential requirement for fast, inter-departmental/agency, decision making which might necessitate the activation of the collective central government response. Examples of emergencies on this scale include most severe weather-related problems.

b) **Serious emergency (Level 2)** is one which has, or threatens, a wide and/or prolonged impact requiring sustained central government co-ordination and support from a number of departments and agencies, usually including the regional tier in England and where appropriate, the devolved administrations. The central government response to such an emergency would be co-ordinated from the Cabinet Office Briefing Rooms (COBR), under the leadership of the lead government department. Examples of an emergency at

[15] Responding To Emergencies, The UK Central Government Response, Concept Of Operations, 24 April 2013.

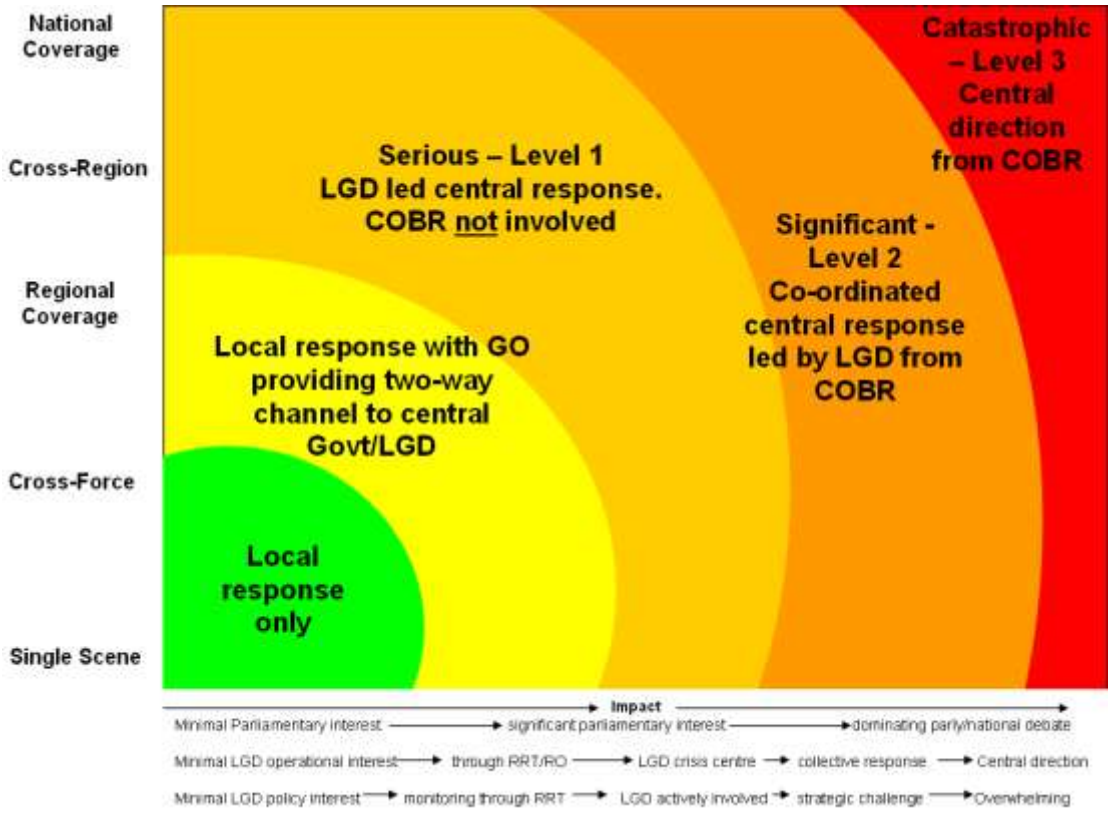
this level could be a terrorist attack, widespread urban flooding, widespread and prolonged loss of essential services, a serious outbreak of animal disease, or a major emergency overseas with a significant effect on UK nationals or interests. Further examples include the H1N1 Swine Flu pandemic, the 2007 summer floods, and the response to the 7th July [2005] bombings in London.

c) **Catastrophic emergency (Level 3)** is one which has an exceptionally high and potentially widespread impact and requires immediate central government direction and support, such as a major natural disaster, or a Chernobyl-scale industrial accident. Characteristics might include a top-down response in circumstances where the local response had been overwhelmed, or the use of emergency powers were required to direct the response or requisition assets and resources. The Prime Minister would lead the national response.

10) The majority of incidents are managed at the local level, with little or no involvement from central government nationally. However, the increasingly complex and inter-dependent nature of society means that there are sometimes significant knock-on consequences even from apparently straightforward events necessitating central government engagement. This could include, for example, providing guidance, co-ordination, people, expertise, specialised equipment, advice or financial support. These decisions will be taken on a case by case basis depending on the nature of the emergency and its impact. In practice, the level of central government engagement may change over time (both up and down) as the demands of the emergency change.

11) By way of illustration, at Figure 2-3 is a chart indicating the characteristics of different levels of emergency and the likelihood of central government engagement according to the actual or potential spread of an emergency and its effect in England.

Figure 2-3: LIKELY FORM OF CENTRAL GOVERNMENT ENGAGEMENT BASED ON THE IMPACT AND GEOGRAPHIC SPREAD OF AN EMERGENCY IN ENGLAND



Source: UK Central Government Arrangements For Responding To An Emergency, An Overview – Published by The Cabinet Office, March 2010, page 68.

m. **USA**. The US National Response Framework [16] provides a guide to how the Nation will respond to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System to align key roles and responsibilities across the Nation. The purpose of the framework is to describe the specific authorities and best practice for managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters[17]. It does not, in itself, set out what those events might be

[16] US Homeland Security, National Response Framework, Third Edition, June 2016.

[17] Ibid., p.3.

as they are captured in The Strategic National Risk Assessment (SNRA) in Support of Presidential Policy Directive 8 (PPD-8). The SNRA sets out a National Preparedness Goal, a National Preparedness System and a National Preparedness Report[18]:

1) To identify high risk factors that supported development of the core capabilities and capability targets in the National Preparedness Goal;

2) To support the development of collaborative thinking about strategic needs across prevention, protection, mitigation, response, and recovery requirements, and;

3) To promote the ability for all levels of Government to share common understanding and awareness of National threats and hazards and resulting risks.

The SNRA grouped threat scenarios into three categories namely Natural Hazards, Technological/Accidental Hazards and Adversarial, Human-caused Threats/Hazards set out in Figure 2-4 below. Notably, in contrast with the UK approach, the comparison of risk in terms of their likelihood of occurring and consequence level is classified.

Figure 2-4 SNRA National-Level Events

Threat/ Hazard Group	Threat/ Hazard Type	National-level Event Description
Natural	Animal Disease Outbreak	An unintentional introduction of the foot-and-mouth disease virus into the domestic livestock population in a U.S. state
	Earthquake	An earthquake occurs within the U.S. resulting in direct economic losses greater than $100 Million
	Flood	A flood occurs within the U.S. resulting in direct economic losses greater than $100 Million

[18] US Strategic National Risk Assessment, December 2011.

Figure 2-4 SNRA National-Level Events (Cont.)

	Human Pandemic Outbreak	A severe outbreak of pandemic influenza with a 25% gross clinical attack rate spreads across the U.S. populace
	Hurricane	A tropical storm or hurricane impacts the U.S. resulting in direct economic losses of greater than $100 Million
	Space Weather	The sun emits bursts of electromagnetic radiation and energetic particles causing utility outages and damage to infrastructure
	Tsunami	A tsunami with a wave of approximately 50 feet impacts the Pacific Coast of the U.S.
	Volcanic Eruption	A volcano in the Pacific Northwest erupts impacting the surrounding areas with lava flows and ash and areas east with smoke and ash
	Wildfire	A wildfire occurs within the U.S. resulting in direct economic losses greater than $100 Million
Technological /Accidental	Biological Food Contamination	Accidental conditions where introduction of a biological agent (e.g., *Salmonella*, *E. coli*, botulinum toxin) into the food supply results in 100 hospitalizations or greater and a multi-state response
	Chemical Substance Spill or Release	Accidental conditions where a release of a large volume of a chemical acutely toxic to human beings (a toxic inhalation hazard, or TIH) from a chemical plant, storage facility, or transportation mode results in either one or more offsite fatalities, or one or more fatalities (either on- or offsite) with offsite evacuations/shelter-in-place
	Dam Failure	Accidental conditions where dam failure and inundation results in one fatality or greater

Figure 2-4 SNRA National-Level Events (Cont.)

	Radiological Substance Release	Accidental conditions where reactor core damage causes release of radiation
Adversarial/ Human-Caused	Aircraft as a Weapon	A hostile non-state actor(s) crashes a commercial or general aviation aircraft into a physical target within the U.S.
	Armed Assault	A hostile non-state actor(s) uses assault tactics to conduct strikes on vulnerable target(s) within the U.S. resulting in at least one fatality or injury
	Biological Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponizes, and releases a biological agent against an outdoor, indoor, or water target, directed at a concentration of people within the U.S.
	Chemical/Biological Food Contamination Terrorism Attack	A hostile non-state actor(s) acquires, weaponizes, and disperses a biological or chemical agent into food supplies within the U.S. supply chain
	Chemical Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponizes, and releases a chemical agent against an outdoor, indoor, or water target, directed at a concentration of people using an aerosol, ingestion, or dermal route of exposure
	Cyber Attack against Data	A cyber attack which seriously compromises the integrity or availability of data (the information contained in a computer system) or data processes resulting in economic losses of a Billion dollars or greater
	Cyber Attack against Physical Infrastructure	An incident in which a cyber attack is used as a vector to achieve effects which are ―beyond the computer (i.e., kinetic or other effects) resulting in one fatality or greater or economic losses of $100 Million or greater

Figure 2-4 SNRA National-Level Events (Cont.)

	Explosives Terrorism Attack	A hostile non-state actor(s) deploys a man-portable improvised explosive device (IED), Vehicle-borne IED, or Vessel IED in the U.S. against a concentration of people, and/or structures such as critical commercial or government facilities, transportation targets, or critical infrastructure sites, etc., resulting in at least one fatality or injury
	Nuclear Terrorism Attack	A hostile non-state actor(s) acquires an improvised nuclear weapon through manufacture from fissile material, purchase, or theft and detonates it within a major U.S. population center
	Radiological Terrorism Attack	A hostile non-state actor(s) acquires radiological materials and disperses them through explosive or other means (e.g., a radiological dispersal device or RDD) or creates a radiation exposure device (RED)

Source: US Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation, published December 2011, pages 2-4.

The US has identified a set of overarching themes that include:

> 4) Natural hazards, including hurricanes, earthquakes, tornadoes, wildfires, and floods, [which] present a significant and varied risk across the country.
>
> 5) A virulent strain of pandemic influenza [, which] could kill hundreds of thousands of Americans, affect millions more, and result in economic loss. Additional human and animal infectious diseases, including those previously undiscovered, may present significant risks.
>
> 6) Technological and accidental hazards, such as dam failures or chemical substance spills or releases, have the potential to cause extensive fatalities and have severe

economic impacts, and the likelihood of occurrence may increase due to ageing infrastructure.

7) Terrorist organisations or affiliates may seek to acquire, build, and use weapons of mass destruction. Conventional terrorist attacks, including those by "lone actors" employing explosives and armed attacks, present a continued risk to the Nation. [Set against a consideration of resource allocation it is interesting to note, in this context, the US's inability to agree on what they mean by 'weapons of mass destruction'. The surviving perpetrator of the Boston Marathon bombing in 2013, who employed two pressure cooker explosive devices, was charged with the use of a weapon of mass destruction. Clearly though, it is for each nation to decide what they consider to constitute a crisis in their own country.]

8) Cyber-attacks can have their own catastrophic consequences and can also initiate other hazards, such as power grid failures or financial system failures, which amplify the potential impact of cyber incidents[19].

n. **Thailand**. The Thai Department of Disaster Prevention and Mitigation (DDPM), Ministry of Interior and the Centre for Excellence in Disaster Management and Humanitarian Assistance (CFE-DMHA) are, arguably, the pre-eminent sources for articulating the nature of the threat facing Thailand. According to CFE-DMHA[20] Thailand is less susceptible to natural hazards than many of the countries in the Asia-Pacific region as it is largely protected from typhoons due to land masses in the east and does not lie on a tectonic plate boundary. These two aspects of its geography help insulate Thailand from many of the impacts of meteorological and geophysical natural disasters. However, Thailand is not immune to natural hazards. Many hazards become disasters because of the complex relationship between people and nature. In particular, Thailand is susceptible to flooding, drought, and landslides. Sources

[19] Ibid., p.4-5.

[20] Thailand Disaster Management Reference Handbook, Center for Excellence in Disaster Management & Humanitarian Assistance, 2015; p28.

tend to disagree about degrees of relative risk for other hazards like earthquakes, tsunamis, typhoons, and fires. Some rank these as significant threats and others point out that they almost never reach 'disaster' scale [The 2004 tsunami is an obvious and significant exception.] Instead, these hazards are just local emergencies. For example, an independent researcher found floods, landslides, and accidents to be Thailand's greatest source of risk. The Thai Department of Disaster Prevention and Mitigation (DDPM) determined floods, accidents, and explosions to be the greatest source of risk. The U.S. Agency for International Development Office of Foreign Disaster Assistance (USAIDOFDA) noted floods, storms, and droughts to be the greatest source of risk (see charts and tables below). It is likely that when aggregated, fires and accidents account for a significant portion of damage in Thailand annually. However, each incident is limited enough that the national disaster management structure is not needed.

There is little doubt that Thailand's most common and most catastrophic disasters emanate from natural hazards and flooding in particular. The impact varies by region but nowhere is immune. Typhoons, droughts, landslides, earthquakes and, thankfully very rarely, tsunamis also cause significant damage. Figure 2-5 below provides a useful representation of the comparative risks assessed by the United Nations Development Programme (UNDP), whilst Figure 2-6 captures information provided by Thailand's DDPM.

Figure 2-5 UNDP Thailand Hazard Assessment

Disaster	Severity	Vulnerability	Management	Tendency
Flood	High	Medium	Medium	High
Landslide/Mudflow	High	Medium	Poor	High
Windstorm	Medium	Medium	Medium	Medium
Drought	High	Medium	Medium	Medium
Fire	High	Medium	Medium	Medium
Explosive	High	Medium	Medium	Medium
Earthquake	Low	Low	Poor	Medium
Accident	High	Medium	Poor	High
Tsunami	High	Medium	Medium	Medium

Source: UNDP in 2002, DDPM Adjust in 2010

Figure 2-6 DDPM Disaster Rankings

Type of Disasters	Subjective Rank	Numeric Weight
Flood	high	2.39
Accident	high	2.37
Explosive	high	2.34
Typhoon	moderate	2.31
Drought	moderate	2.24
Fire	moderate	2.20
Land slide	moderate	2.15
Earthquake	moderate	1.97
Civil Unrest/Refugee Influx	moderate	1.87
Pests	moderate	1.77
Epidemic	low	1.63

Source DDPM Ranking,
http://www.adrc.asia/countryreport/THA/2011/FY2011B_THA_CR.pdf

Of significant note, the 2015 Thai National Disaster Risk Management Plan [21] references the Disaster Prevention and Mitigation Act B.E. 2550 (2007), which defines a 'disaster' as encompassing: fire, storm, flood, drought, human epidemic, animal epidemic, aquatic animal epidemic, plant epidemic, including any type of hazard that has a negative effect on [the] general public, be it induced by nature activities, human activities, accident or any other incident which is harmful to life, body of people or inflicts damage on property of people or of the State, and including air threat and sabotage actions [22]. The document does not make any relative assessment of likelihood, scale or impact of any particular form of disaster but does set out 14 types of hazard:

> 1) Fire Hazard: The threat triggered by uncontrolled burning of which the flame has continued to spread and engulfed the nearby areas where combustible materials are present. Fire condition can be intensified if it continuously receives augmented fuel or if there is a high discharge of rate of vapour of burning materials.

[21] National Disaster Risk Management Plan (2015) approved by Cabinet 31 March, B.E. 2558, 2015.

[22] Ibid., Appendix B: Illustration of Relevant Hazard Characteristics, p.131.

2) Storm Hazard:

a) Tropical Cyclone: A natural phenomenon capable of inflicting widespread destruction of residences and structures, vegetation, etc., caused by inward spiralling winds of storm. This threat occurs along the forward track of a storm, which extends as far as 50 – 100 kilometres. The most affected areas will be those located close to the track of the tropical cyclone eye wall where the most damaging winds and intense rainfall are found.

b) Storm Surge: The rising of sea levels due to low pressure high winds and high waves associated with a tropical cyclone with speeds reaching up to more than 100 kilometres per hour as it makes landfall. A storm surge often results in coastal inundation, which can cause significant damage to the areas adjacent to the shoreline particularly the windward side area.

c) Thunderstorms: A form of weather which usually occurs in summer months of a year particularly during the period of sweltering warm weather for several consecutive days. Thunderstorms are formed as a result of the collision between a cold front [coming] from China and the prevailing warm front in Thailand. The collision raises moist and unstable air vertically into the atmosphere, which subsequently matures into cumulonimbus clouds or a thunderstorm cell. Thunderstorms are accompanied by gusts, lightning, thunder and occasional hail. Generally, thunderstorms are short-lived and their coverage area is less than 20 – 30 kilometres.

d) Hail: A hazard triggered by a solid precipitation that falls as balls or irregular lumps of ice. Hail forms when super cooled droplets of rain in nimbus clouds collide with solid particles such as dust or existing ice pellets. The ice is suspended in the air by a strong updraft and will then fall back down. The

process will occur over and over adding layers upon layers of hailstones.

e) Thunderstorm force winds: Narrow area damage of residences, vegetation and other structures caused by a short period (approximately 10–15 minutes) of severe gusts or hailstones [often] associated [with] a thunderstorm with a sustained wind speed greater than 100 kilometres per hour. They occur most frequently during the transition period from the cool season to summer and before the start of monsoon season.

3) Flood Hazards:

a) Flooding: An overflow or accumulation of an expanse of water that submerges land. It is usually due to heavy rainfall events that produce a large volume of water within a body of water such as a river or canal, exceeding the total capacity of the body, and as a result, some of the water flows or sets outside the normal perimeter of the body. In addition, human activities such as blocking the natural flow of water either intentionally or unintentionally can produce flooding, often causing significant fatalities and material and environmental damage. Flooding can be classified according to inherent characteristics as follows:

i. Inundation/Overbank flow: Inundation is [the] gradual rising and spreading of water from continuous heavy downpour due to slow dissipation or [an] ineffective drainage system. Whereas overbank flow is a slow kind of flooding due to an excessive volume of rainfall navigating a river at a too rapid speed beyond the coping capacity of a river channel. These floods mainly occur in the river basins, urban areas and in the lowest reach area of a river.

ii. Flash flooding is a rapid or sudden flood in a poorly absorbent area and precipitous terrain due to a massive and sudden rainstorm. Flash flooding can also occur after a significant and unexpected event such as the collapse of a man–made structure such as a dam, reservoir, etc. Flash flooding most often occurs in normally dry areas that have recently received precipitation, but may be seen anywhere. Flash flooding is extremely dangerous due to its sudden nature and rapid flow that provides little protection or evacuation opportunity.

b) Landslide/Mudslide Hazard: A hazard triggered by a downslope movement of earth mass, rock or debris due to the force of gravity. Landslides can occur on any terrain given the right conditions of soil, moisture and the angle of slope. The rate of movement of landslide can range from extremely slow to extremely rapid owing to the types of materials, gradient, environment and volume of rainfall. In addition to water related factors, earthquakes and volcanic eruptions can also cause landslides. Landslides regularly cause severe property damage, injury and death, and adversely affect a range of resources.

4) Drought Hazard: A hazard triggered by a prolonged dry period of weather involving a deficit or no rainfall spanning over large areas. Periods of prolonged drought can trigger widespread and severe effects among people, animals [and] vegetation, including a shortage of water for drinking and household use as well as for agricultural and industrial purposes, substandard or highly limited crop or yield productions, death of livestock, etc. The causal factors of drought include:

a) Rainfall shortage/Dry spell: A drier than normal condition with abnormally low rainfall or no rainfall [at all] in locations [that] regularly receive substantial seasonal rainfall.

b) Break of downpour: A period during which the daily amount of rainfall is less than 1 millimetre for 15 consecutive days during normal monsoon season. June and July are most likely to experience a break of downpour.

5) Human Epidemic: A human health hazard occurs when a new case of certain diseases, in a single human population and during a given period substantially, exceed what is expected based on recent experience. The aforesaid disease is not required to be a communicable exposure, and is capable of affecting [the] wellbeing of people residing in stricken and neighbouring communities.

6) Animal Epidemic: The widespread outbreak of animal infectious diseases in domesticated or wild animals of a single kind, among multiple animal species and can be transmitted from animals to humans, during a given period substantially exceeding what was expected based on recent experience. Animal epidemic outbreaks are capable of causing socioeconomic consequences and public health problems.

7) Aquatic Animal Epidemic: Widespread outbreak of epidemic in aquatic animals of a single kind, among multiple aquatic animal species, and can be transmitted from aquatic animals to humans, during a given period that substantially exceeds what is expected based on recent experience. Aquatic animal outbreaks are capable of causing socioeconomic consequences and public health problems.

8) Plant Epidemic/Plant Pests: Those which are harmful to plants such as plant pathogens, insects, animals or plants which may harm plants, any part of a plant such as stems, buds, stocks, shoots, offshoots, branches, leaves, flowers, fruits, and cultures and spores of mushrooms, whether or not they can be propagated; including predators, parasites, silkworm eggs, silk cocoons, bees, beehives and micro-organisms, to the extent of inducing widespread negative effects on society, the economy and the general public.

9) Transport Hazard: An incident or condition created by land, maritime, and air travel. This includes large scale mass transportation incidents, chemical and hazardous material transportation incidents, oil spills and chemical spills into water bodies, as well as discharging oil or waste into rivers and the sea.

10) Forest Fire and Haze Hazard: A hazard triggered by any uncontrolled fire regardless of the cause of ignition, that occurs in the natural forest or forestry plantation areas which results in an accumulation of dust particles, smoke and airborne suspended particulate during cloudy sky conditions. Forest fires can create extensive damage to property including negative environmental and natural resources effects, and thick haze can cause negative health effects.

11) Earthquake Hazard and Building Collapse

a) Earthquake hazard: A natural hazard caused by the sudden release of accumulated strain energy within the interior of the earth. This release causes ground shaking and vibration at the surface of the earth. In cases where earthquake shaking is relatively weak, it may not pose any damage but in cases of intensive ground shaking, it can cause catastrophic consequences.

b) Building collapse hazard: A hazard triggered by an earthquake induced ground shaking, which is strong enough to cause the collapse of buildings and other structures, including edifices, houses, stores, warehouses, offices, floating houses, and the destruction of life and property.

12) Tsunami Hazard: A hazard induced by a series of extremely large waves. The original Japanese term literally translates as ‘harbour waves’. Tsunami can be classified as local tsunami and distance or regional tsunami. A local tsunami is a tsunami from a nearby source for which its destructive effects are confined to the coast within a short

(tsunami) travelling time from its origin. Distance tsunami are usually triggered by major undersea earthquakes and are capable of causing widespread destruction not only in the immediate region of its generation but across the entire ocean. Other natural phenomena that cause tsunami are volcanic eruption, large-scale landslides and large asteroids smashing into the ocean. The power created by tsunami can lead to large scale destruction of property and massive loss of life along coastal areas.

13) Air Threat: A harmful menace inflicted by air attack using aircraft, guided-missile, ballistic missile or any airborne vessel. Such an attack can substantially affect the life and property of people.

14) Sabotage Actions:

a) Sabotage: Any deliberate action that aims at destroying property of people or of a state, or public utilities, or at disrupting and delaying the functional system as well as causing bodily harm to people and which trigger national political, economic and social agitation with an intention to damage the stability of a state.

b) Terrorism threat: Any deliberate act intended to provoke a state of terror or instil fear in the general public, or intimidate or coerce the government or international organisation to act or abstain from acting, which will lead to bodily harm and vital property damage.

c) International terrorist threat: Any deliberate act of a person or group of persons with an intention to attain desired goals that are political, economic and social in nature. Acts of international terrorism are mostly carried out in a foreign county by individuals or groups who are not natives to that country. Such individuals or groups may act on their own without any support from any state or are supported by a state sponsor of terrorism. The

occurrence of international terrorism can exert direct effects on national interest, international commitment, national defence policy, political economic and psychological policies as well as national reputation and dignity.

6. **International**. An international threat, by definition, would affect more than one country either simultaneously or sequentially. The nature and characteristics of the threat are unlikely to be dissimilar to those already mentioned above but the reaction to them may have significant differences not least because they are likely to involve international authorities and organisations. An affected country might be near powerless to do anything about the threat (for example the radiation levels in neighbouring countries following the Chernobyl disaster in Ukraine in 1986) yet have to deal with the effects and clean-up. International scenarios fall outside the scope of this research paper and thus will not be considered further. They would, however, make for a productive follow on study.

7. **Scale of Threat**. Each of the three nations has set out in their various documents the nature and type of threat scenario they believe they will face over the near to mid-term. New threats could easily emerge, especially in areas of terrorism, cyber and pandemics, but the most recurring theme throughout history, namely natural disasters, is almost certain to remain largely constant over time. Predicting the scale, and thus impact, of each event though is very hard to do, not least because empirical data is illusive.

a. The UK approach to this challenge has been to make an assessment using both a 'low through medium to high risk scale', and the statistical 'odds' of something occurring based on past experience and a largely subjective analysis of future trends. The impact of each type of event has then been measured on a linear scale of 1 to 5. Whilst such a scale lacks fidelity it arguably compensates through simplicity. That said, when it comes to allocating resources, it could make prioritisation much more difficult especially when two types of event are judged to have similar impact.

b. The USA has taken a more generic approach setting benchmarks that would constitute a national level event and thus

indicate the degree of event impact. At the unclassified level though it has not been possible to identify which threats they see as relatively more likely. However, given the size of the country – territorial and population – it is not wholly unreasonable to conclude that most events on their threat list will occur somewhere in the country at some time. The sheer volume of events that take place was one of the seminal reasons for setting up the Federal Emergency Management Agency (FEMA) and United States Northern Command (USNORTHCOM). Both FEMA and USNORTHCOM run 24-7 operation rooms to coordinate the response to crisis events across the country[23]. The benchmarks are, arguably, much more political in their outlook than those of the UK because measuring, for example, 100 Million Dollars of damage is not a precise, quick or easy thing to do, especially during a crisis. It is also unclear as to who, ultimately, decides if the benchmark has been reached.

c. The Thai approach falls somewhere between that of the UK and the USA. The DDPM has made an assessment of the relative impact of a number of event types, although it has not been possible to determine the underlying data to support the numerical weighting. Nevertheless, their very existence indicates that some sort of scientific approach has been made to the assessment. There is not, however, any indication of the likelihood of occurrence. The UNDP lists 9 types of disaster, assigns a relative severity grading (low, middle, high) and makes a stab at suggesting their likely frequency. Almost curiously, nothing is given a low likelihood making the value and relativity of the scale more difficult to assess. There is also no mention of a pandemic so, again, it is difficult to discern the likelihood or impact of such an event or whether this was simply an oversight on the part of the authors. Given that pandemics for people, animals, marine and plant life are all included in the 2015 Thai National Disaster Risk Management Plan the chances of accidental omission seem plausible.

d. One issue that is common to all three nations is an increase in population density. It is a glimpse of the blindingly obvious to say that every type of disaster mentioned above is

[23] USNORTHCOM does not bear any responsibility (less Ballistic Missile Defence) for the State of Hawaii, which is looked after by United States Pacific Command (USPACOM).

considered a crisis based, ultimately, on having an impact on people. Whether the unit of measurement is lives lost, injury, inconvenience, financial cost or something else they all relate to degrees of human suffering. By way of a counter-example, an earthquake or landslide in the middle of nowhere will not be considered a crisis. Modern technology may make us aware of the event but if no, or only a few, people are, or will be, affected the situation will not be deemed an emergency. By deduction, it follows that there is a direct relationship between the scale (impact) of what constitutes a crisis and population density. The greater the density, the greater the impact and thus the greater the crisis. The challenge for all three nations is that as population density continues to grow so will the need for resource allocation and appropriate planning and preparation. The problem, however, is that higher densities do not, in themselves, ensure higher revenue.

8. **Rate of Occurrence**. If impact is relative to population density then it follows that there must also be a connection between density and incidence, albeit not quite so directly. In a low-density population, a crisis is less likely to occur because the thresholds described above may not be breached. (It does not automatically mean that the number of events will necessarily be less, especially for natural phenomena.) However, it is also logical for there to be a link between rate of event occurrence and geographical size; the bigger the country the more likely an event will take place. (Again, whether that event constitutes a crisis is dependent on the affect population density.) The rather imprecise definition of a disaster contained in the Thai Disaster Prevention and Mitigation Act B.E. 2550 (2007) pretty much guarantees there will be a disaster in Thailand every year due to the regular pattern of large scale flooding. Both the UK and the USA also suffer from a variable amount of flooding each year but, in most cases, it does not breach the disaster benchmark and thus classify as a crisis. Returning to the Organisational level definition of a disaster set out by Seeger, Sellnow and Ulmer there appears to be much value in defining a crisis as needing three common elements, namely:

a. A threat to an organisation (a country in this case).

b. The element of surprise.

c. A short decision time.

If an event is largely predictable it should not constitute a crisis. In the case of Thailand, it is easy enough to say that there will almost certainly be some large scale flooding every year, or, in the case of the USA that there will be some significant forest wildfires. However, it is the 'where?' and 'when?' questions that add the unpredictability factor and thus repeatedly turn these predictable events into crises.

9. **The Most Likely Common Scenarios**. As has already been established above, all three countries face a range of threat scenarios that manifest on a recurring but irregular schedule. For the purpose of this paper however, it is necessary to identify common themes that each country needs to plan against and it will utilise the most likely, rather than the most catastrophic, events for comparison.

a. **For the UK** based on the data above, the most likely scenarios, weighted for severity, are:

1) Catastrophic Terrorist attack (and probably on the transport system).

2) A pandemic influenza.

3) Weather extremes (including poor air quality, storms and gales).

4) Explosive volcanic eruption.

5) Widespread electricity failure.

6) Flooding (inland or coastal).

7) Animal diseases (such as Foot and Mouth).

8) Drought.

9) Disruptive industrial action.

b. **For the USA** it is a little harder to discern as they do not provide unclassified data on likelihood, however, based on the information provided above, it is assessed, subjectively, that the most likely scenarios are:

1) Natural hazards, specifically including hurricanes, flooding and wildfires. (Tornadoes, whilst frequent, tend to wreak local chaos rather than becoming a nationally significant event. Clearly, were one to occur in a higher density population this would not be the case but few major cities have, unsurprisingly, been built in major tornado alleys.)

2) A pandemic influenza.

3) Man-made hazards (whether accidental or technological including large-scale chemical spillage and infrastructure collapse).

4) Terrorist attack (including the use of a weapon of mass destruction (WMD) and more conventional methods).

5) Cyber-attack (which could include the initiation of a widespread electricity failure or financial meltdown).

c. **For Thailand**, combining the data extracted from Figures 2-4 and 2-5, it is assessed that the most likely scenarios are:

1) Flooding (including from tsunami albeit these occur very infrequently).

2) Landslides and/or mudflow

3) Windstorms (including typhoons).

4) Droughts.

5) Civil unrest and/or refugee influx

6) Epidemic (which should be considered to include a pandemic influenza).

10. **Down-selected Common Scenarios**. The scenarios common to all three countries, and thus down-selected for further consideration within this paper are:

a. Flooding (regardless of cause or location such as inland or coastal).

b. Weather extreme effects (regardless of cause).

c. Terrorist Attack (of a conventional style only as the impact of the use of a WMD is so significant that it automatically will become international and require a global response).

d. Pandemic influenza (even though the same terminology is not used by Thailand).

e. Cyber Attack is only mentioned by the US, but undoubtedly is applicable to all given that it recognises no borders or boundaries.

Chapter 3
National Tasking Mechanisms

"Do. Or do not. There is no try.".[1]

"You are what you do, not what you say you'll do."[2]

"Action expresses priorities."[3]

National Tasking Procedures

1. Every civilised and organised nation has a procedure for translating its *intent* and *will* into direction for its levers of power, whether they be diplomatic, economic or military. When it comes to planning, preparing and reacting to one of the national threat scenarios identified in the previous chapter this should be no different. As Henry Ford, the American Industrialist and founder of the Ford Motor Company said *"Vision without execution is just hallucination."*[4]. A failure to tell the military forces what to do will set them up for failure at the very moment they are, perhaps, needed most.

2. There is, of course, no one size fits all mechanism for issuing direction and each country will therefore do it differently. The most important point, however, is that what is communicated (i.e. the message sent) is clearly understood (i.e. the message received) by the recipient. Where there is a difference in intent on one part and understanding on the other (akin to Chinese Whispers theory[5]) there will be gaps in the process and thus another potential point of failure. To make certain these gaps do not materialise, there should be synergy between the Ends, Ways and Means of National Strategy and, additionally, a mechanism by which it can be measured and assessed.

3. In the case of the three countries under study in this paper they all have a different mechanism to convert national intent for disaster

---

[1] Yoda – Star Wars Trilogy, The Empire Strikes Back, 1980.

[2] C.G Jung, 1956.

[3] Mahatma Ghandi, 1947.

[4] Henry Ford, 1932.

[5] https://en.wikipedia.org/wiki/Chinese_whispers, accessed Apr 2017.

planning and response into military tasking. Given the difference in threat scale and military assets this is hardly surprising but it provides a useful opportunity for comparison of methodology.

The UK – Ends

4. **Strategic Background**. The context for military involvement in preparedness and response is set out in Joint Doctrine Publication (JDP) 02, (Edition 2)[6], as follows: Her Majesty's Government (HMG) is committed to, and continually improving the country's ability to respond to disruptive challenges at the national, regional and local levels. The Civil Contingencies Act (CCA) 2004 provides the core framework for civil protection; it defines how organisations, particularly local responders, prepare for emergencies. The Home Secretary has overall Ministerial responsibility for the safety and security of the population within the United Kingdom and, therefore, is responsible for emergency preparedness and response. Ministers in Lead Government Departments are responsible for contingency planning and response within their specific areas. Although the Devolved Administrations are responsible for coordinating many aspects of resilience within their respective jurisdictions, they work closely with the Cabinet Office to ensure a coherent approach.

5. **The Constitutional and Legal Basis for UK Operations**. A helpful explanation of the Constitutional and Legal Basis for UK military forces to act within the UK is provided in an Addendum to JDP 02 (Edition 2)[7] as follows: Defence is exercised under Prerogative power. Letters Patent from Her Majesty carry delegation of some of the responsibilities for defence of the realm to the Defence Council. The Armed Forces are therefore under the direct command of Central Government and Armed Forces personnel do not have additional powers granted to them. They must operate within UK and international law at all times. Under certain specific situations, they can be granted additional powers under Part 2 of Civil Contingencies Act 2004 and the 1964 Emergency Powers Act. For constitutional reasons, any members of the Armed Forces deployed on operations must remain under military command at all times and are only ordered to undertake activity by

[6] Joint Doctrine Publication 02 (2nd Edition) – Operations In The UK: The Defence Contribution To Resilience, dated September 2007.

[7] JDP 02 (2nd Edition) Addendum – The Defence Contribution To Uk Resilience: A Guide For Civil Responders, dated February 2010.

Defence Ministers and the Defence Council. This represents a key tenet of democracy, whereby the Armed Forces remain under the control of Central Government – the representatives of the population. This also means that provision of Military Aid automatically involves the elevation of the response to Central Government and Defence Minister authorisation.

6. **The National Response Overview**. Whenever possible the initial response to the vast majority of emergencies will be provided by local, civilian, emergency services and authorities. However, should the scale, duration or impact of the event prove to be beyond their capabilities and capacity then they will seek assistance from elsewhere, potentially including the Ministry of Defence. At this point, the chain of command can become confusing if not articulated with care and consideration. A core principle within the UK is that the Police command chain is operationally independent of Government, which is a situation diametrically opposite to that of the Armed Forces for whom an operation must be approved by a Defence Minister.[8]

7. **Defence Involvement**. The National Security Strategy and Strategic Defence and Security Review 2015 sets out eight Defence Missions; Defence Task 1 is to Defend and contribute to the security and resilience[9] of the UK and its Overseas Territories. It requires the MoD to 'provide support to the UK civil authorities in strengthening resilience, helping in the response to natural disasters, accidents and terrorist attacks'[10]. Defence Strategic Direction 16 also directs that Defence should conduct its UK fixed tasks under Military Aid to the Civil Authorities (MACA).

8. **Military Aid to the Civil Authorities**. The MoD's role in MACA is concentrated on 2 main areas:

a. Providing niche capabilities, which MOD needs for its own purposes and which would not be efficient for the rest of

---

[8] Joint Doctrine Publication 02 (2nd Edition).op.cit.,p.1-3.

[9] Resilience is defined as the 'Ability of the community, services, area or infrastructure to detect, prevent, and, if necessary to withstand, handle and recover from disruptive challenges.' Cabinet Office, *UK Civil Protection Lexicon Version 2.1.1*, February 2013.

[10] Joint Doctrine Publication 02 (3rd Edition) – Operations In The UK: The Defence Contribution To Resilience and Security, p. 12, dated February 2017.

government to generate independently, for example Explosive Ordnance Disposal (EOD).

b. Standing ready to support the civil authorities when their capacity is overwhelmed. The armed forces provide this support from spare capacity, so it is subject to the availability of resources, without affecting core MOD objectives. (The MOD does not generate and maintain forces specifically for this task because the requirement is unpredictable in scale, duration and capability requirement; experience suggests that requirements can usually be met from spare capacity; and it would involve using the MOD budget to pay for other government departments' responsibilities, which would not normally happen.[11]

The provision of military assistance is governed by 4 principles[12] and MACA may be authorised when:

c. There is a definite need to act and the tasks the Armed Forces are being asked to perform are clear;

d. Other options, including mutual aid and commercial alternatives, have been discounted; and either

e. The civil authority lacks the necessary capability to fulfil the task and it is unreasonable or prohibitively expensive to expect it to develop one; or

f. The civil authority has all or some capability, but it may not be available immediately, or to the required scale, and the urgency of the task requires rapid external support from the MOD.

However, under exceptional circumstances, ministers can choose to temporarily waive these principles. This may happen when there are major events of national and international importance, or an event that is catastrophic in nature.

g. The 2016 MACA Policy Review increased the demand signal on the MoD, widening the scope for MACA to include the

[11] Policy paper: 2015 to 2020 government policy: Military Aid to the Civil Authorities for activities in the UK, p. 3, dated 4 August 2016.

[12] Joint Doctrine Publication 02 (3rd Edition).op.cit.,p. 27-28.

full range of resilience tasks. Defence assets can now expect to become involved in planning and preparation, and recovery tasks, as well as responding to emergencies. They may also be asked to assist civil authorities with training.

The UK – Ways

9. **Roles**. Following a request for assistance Defence assets may be used to contribute in 5 main roles or functions, namely:

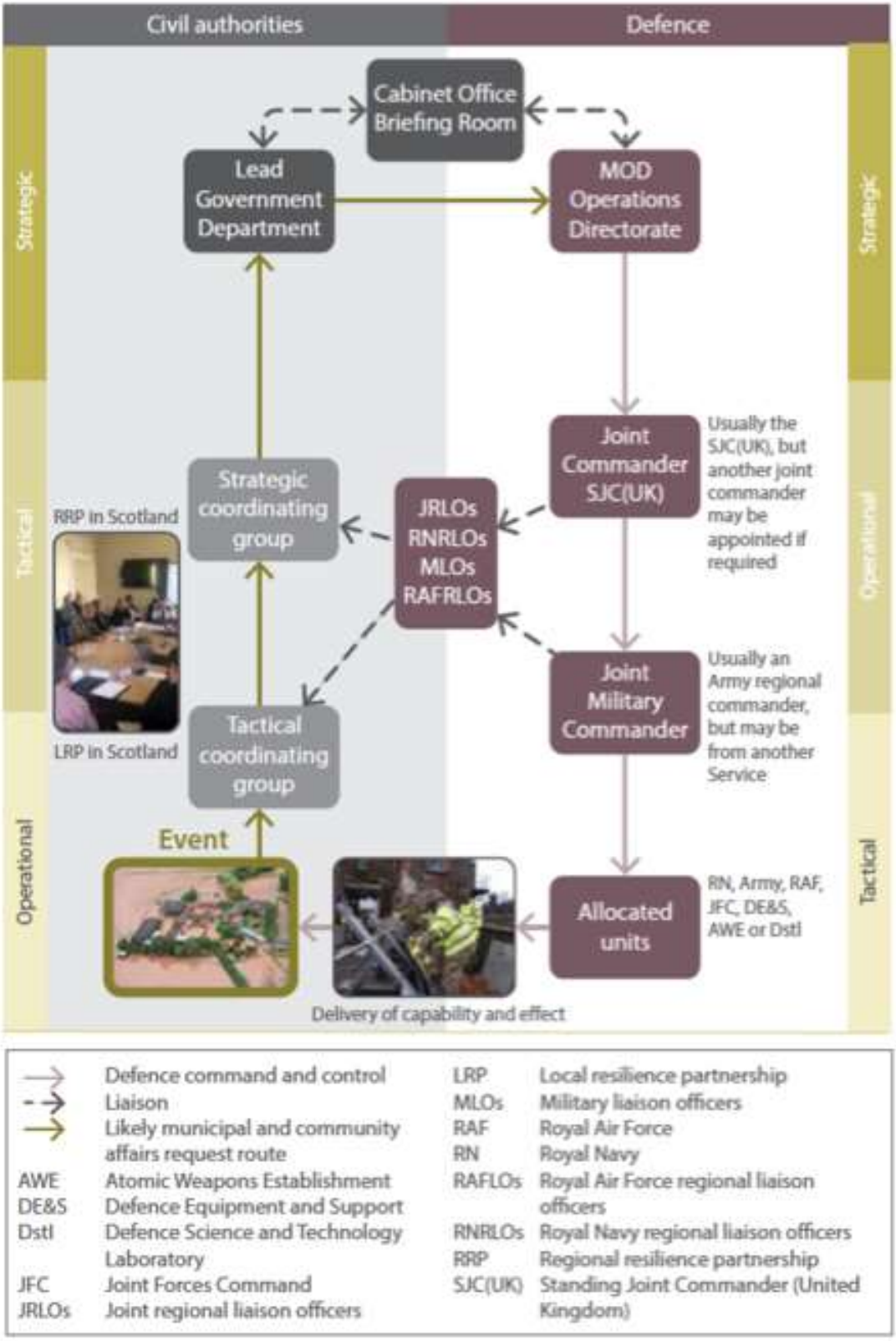
a. Command and control (C2). Military C2 is considered at the Strategic, Operational and Tactical levels. (This can be a little confusing when dealing with the civil Police as they use a Strategic, Tactical and Operational lexicon to describe the same functions.) A diagrammatic model of the process is set out in Figure 3-1 below.

1) Strategic. The MoD acts as both a military headquarters and a Department of State. The Deputy Chief of the Defence Staff (Military Strategy and Operations) along with the Director General Security Policy provide guidance to Defence ministers and other government departments, whilst the Operations Directorate leads on all operations activity within the UK.

2) Operational. The Army's Commander Home Command acts as the Standing Joint Commander (SJC(UK)) and is responsible for the planning and execution of the MoD's contribution to resilience operations (during peacetime).

3) Tactical. Regional Points of Command (RPoC) deliver Defence C2 across the UK and maintain strong links with civil authorities.

Figure 3-1: Generic Command and Control Model for Resilience/Security Operations



Source: Joint Doctrine Publication 02 (3rd Edition), p.49

b. Liaison. In order for Defence support to be effective it is dependent upon timely and relevant liaison with other government departments, civil authorities and, occasionally, commercial organisations. The network of Liaison Officers is depicted graphically in Figure 3-1 above.

c. Specialist Advice and Capability. There are 5 focus areas for specialist support:

1) Explosive Ordnance Disposal (EOD)

2) Specialist Scientific Support, primarily the Atomic Weapons Establishment and Defence Science and Technology Laboratory

3) Intelligence, surveillance and reconnaissance

4) Communications

5) Cyber

d. General and non-specialist support. The Operations Directorate in the MoD will task the most appropriate and available regular unit or Service personnel depending on the nature and likely duration of the task. This could include counter-terrorism operations (CTO) and use of the Army's three UK Standby Battalions.

e. Education and training. A wide range of collective and individual resilience training is provided by the MoD to meet demand as and when it arises.

10. **Tasks**. There are four generic defence resilience tasks set out in JDP-02[13], namely:

a. Fixed Tasks. Defence is liable, on a permanent and enduring basis to deliver an irreducible minimum level of tasks even in the event of a competing large-scale war-fighting operation. They can therefore be considered non-discretionary and are delivered by assigned forces. Most examples are classified but include CTO.

[13] Ibid.,p.51-53.

b. Enduring Tasks. Comprising of a broad range of tasks, usually on an open-ended basis, examples of Enduring Tasks include the Royal Navy's contribution to fishery protection and EOD.

c. Response Phase Tasks. Defence support during the Response Phase is designed to meet the UK Government's standing strategic priority to 'protect life and, as far as possible, property, and alleviate suffering'. The process followed depends on the circumstances at the time

1) Urgent Response. Local commanders' have a standing authority[14] to deploy assets under their command to meet an urgent response when there is an imminent threat to life, a need to alleviate distress or to protect significant property.

2) Routine Response. In all other circumstances where there is time to consult the higher chain of command a formal process must be followed in order to request, and receive, Defence asset support.

d. Recovery Phase Tasks. By definition, Recovery Phase Tasks will rarely be urgent and thus a request for assistance must be submitted, in writing, by the appropriate civil authority.

The UK – Means

11. When requested, the Operations Directorate, supported by HQ SJC(UK) work with the single-Services to identify the most appropriate and available military capability to meet the demand signal. Depending on the actual problem, a range of capabilities might then be tasked to provide support. Those means include, but are not limited to[15]:

a. **Explosive Ordnance Disposal and Search** (EOD&S). An explosive ordnance threat exists both on land and at sea and can include conventional munitions, improvised explosive devices and chemical, biological, radiological and nuclear (CBRN) devices. The

[14] Defence Council Order, dated 17 January 1983.

[15] Joint Doctrine Publication 02 (3rd Edition).op.cit.,p.81-83.

MoD's EOD&S capability is joint in nature, scalable, environment prioritised and rapidly deployable.

b. **Salvage and Maritime Operations**. Defence provides a specialist team for salvage and maritime operations (SALMO), which is held at very high readiness to support MoD and other government departments' marine salvage requirements including:

1) Carrying out first aid repairs to damaged or submerged vessels;

2) Recovering ditched aircraft from the sea or inland waters;

3) Clearing ports, facilities and approaches;

4) Locating and recovering objects from the seabed, including deep water; and

5) Providing specialist advice on salvage operations.

Given the nature of SALMO tasks they are unlikely to have a pivotal role in major disaster scenarios although there may be instances during flooding events that their niche capability may be called upon.

c. **Intelligence, Surveillance and Reconnaissance** (ISR). ISR is a critical capability that can provide both the MoD and other users with situational awareness to enable timely and effective decision making. Amongst other tasks, ISR can assist with:

1) Locating missing persons;

2) Wide area reconnaissance;

3) Infrastructure damage analysis and assessment;

4) Intelligence products to support MoD operations and other government department and civil authority decision-making.

d. **Mobility**. The MoD inevitably has a very wide array of mobility capability that can operate on water, land and in the air to move both people and materiel. It can be used to facilitate the movement of military forces and specialist equipment into, or out of, an affected area and, in extremis, to help evacuate civilians away from danger. Example platforms include ships, rigid inflatable boats, landing craft, bulk equipment and personnel lift vehicles, helicopters, mechanical handling equipment and freight planes such as C-130 Hercules aircraft.

e. **Planning Specialists**. Defence personnel can be used to reinforce planning and coordination efforts at the Strategic, Operational and Tactical levels. They bring a wide-range and depth of experience often gained from similar situations abroad.

f. **Command and Control** (C2). In a similar vein to planning specialists, Defence personnel are well versed in delivering C2 during demanding, stressful and, frequently, unsocial hours of operations. Each of the single-Services has particular experience operating in their own specialist environment and can make use of country-wide infrastructure and presence.

g. **Communications**. Frequently coupled with C2 above, the MoD has a robust communications suite that can exploit both static and deployable assets across all three environments (sea, land and air). Critically, they can communicate with each other, which is not always the case in multi-agency responses.

h. **Engineering**. Many disaster situations require significant engineering effort to prevent, mitigate or recover from. All three single-Services can contribute although, usually, the Army provides the bulk of the capability who normally are sourced from the Royal Engineers. They come with a distinct advantage of being able (and frequently highly experienced) to deploy in austere conditions. They capabilities include, but are not limited to engineer reconnaissance including detailed technical infrastructure reconnaissance and diving; survey and mapping; planning and design; logistic resourcing; construction; and demolition.

i. **UK Standby Battalion**. The UK keeps three UK standby battalions at extremely-high readiness to support operations

in the UK. They each have an assigned geographic area of responsibility but are able to operate elsewhere as required. Their key characteristics are:

1) Agile command able to plug into civil authority systems;

2) Adaptable and scalable force packages able to deploy large numbers (1 – circa 400) of trained, disciplined, military personnel to a wide range of roles;

3) Up-to-date situational awareness of the UK joint operations area; and

4) Self-contained logistics allowing sustainment for 48-hours anywhere in the UK.

j. **Air Logistics**. The RAF provides logistics support to air operations worldwide and is thus well placed to do the same at home. It encompasses a number of capabilities including, but not limited to: real-life support; aircraft recovery; rapid runway clearance; and mountain rescue.

k. **Defence Estate**. There is a tendency to think of a military capability needing to move to the area of a disaster but frequently the provision of secure real estate is of significant help. The MoD is one of the largest landowners in the UK with facilities that range from training areas and firing ranges through to naval bases, army barracks and airfields. It also owns a wide-array of accommodation units.

l. **Counter-Chemical, Biological, Radiological and Nuclear** (CBRN). In the event of an incident involving CBRN activity, the MoD would deploy assets to assist in the response. The details or precisely what that would entail are classified.

m. **Fire and Rescue**. The MoD maintains a professional fire and rescue capability used, primarily, in support of Defence Airfields. Defence Fire Risk Management Organisation units are based throughout the UK often in geographically remote locations.

They can be used to respond to MACA events subject to the same authorisation requirements mentioned above.

n. **Non-Specialist Capability**. In the event of a major incident Defence personnel can be made available as necessary to support an operation. They may comprise formed units or be sent as individual augmentees depending on the need.

o. **Medical Capability**. Although not mentioned specifically in JDP-02, the MoD owns and maintains a significant medical capability designed to be deployed on overseas operations. It is closely entwined with the National Health Service, nevertheless elements could be deployed independently within the UK if required. Although not a large-scale disaster, MoD specialist medical assets were used recently to transfer a patient suffering from the Ebola virus to appropriate medical facilities in another part of the country. Had the virus spread to the general public a major incident would almost certainly have ensued.

p. **Education and Training**. MoD assets are also used for education and training exercises relating to resilience and UK operations.

The USA - Ends

12. **Strategic Background**. The seminal authority for resilience[16] in the US is Presidential Policy Directive Eight (PPD-8)[17]. It was issued by President Obama in March 2011 and states:

> This directive is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters. Our national preparedness is the shared responsibility of all levels of government, the private and non-profit sectors, and individual citizens. Everyone can contribute to safeguarding the Nation from harm. As such, while this directive

[16] Resilience is defined in the US as 'the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies'.

[17] Presidential Policy Directive 8, dated 30 March 2011.

is intended to galvanize action by the Federal Government, it is also aimed at facilitating an integrated, all-of-Nation, capabilities-based approach to preparedness.

Therefore, I hereby direct the development of a national preparedness goal that identifies the core capabilities necessary for preparedness and a national preparedness system to guide activities that will enable the Nation to achieve the goal. The system will allow the Nation to track the progress of our ability to build and improve the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation.

The Assistant to the President for Homeland Security and Counterterrorism shall coordinate the interagency development of an implementation plan for completing the national preparedness goal and national preparedness system. The implementation plan shall be submitted to me within 60 days from the date of this directive, and shall assign departmental responsibilities and delivery timelines for the development of the national planning frameworks and associated interagency operational plans described below.

PPD-8 is aimed at the whole community and is organised around the key elements shown in Figure 3-2 below:

Figure 3-2: Presidential Policy Directive 8 (PPD-8)

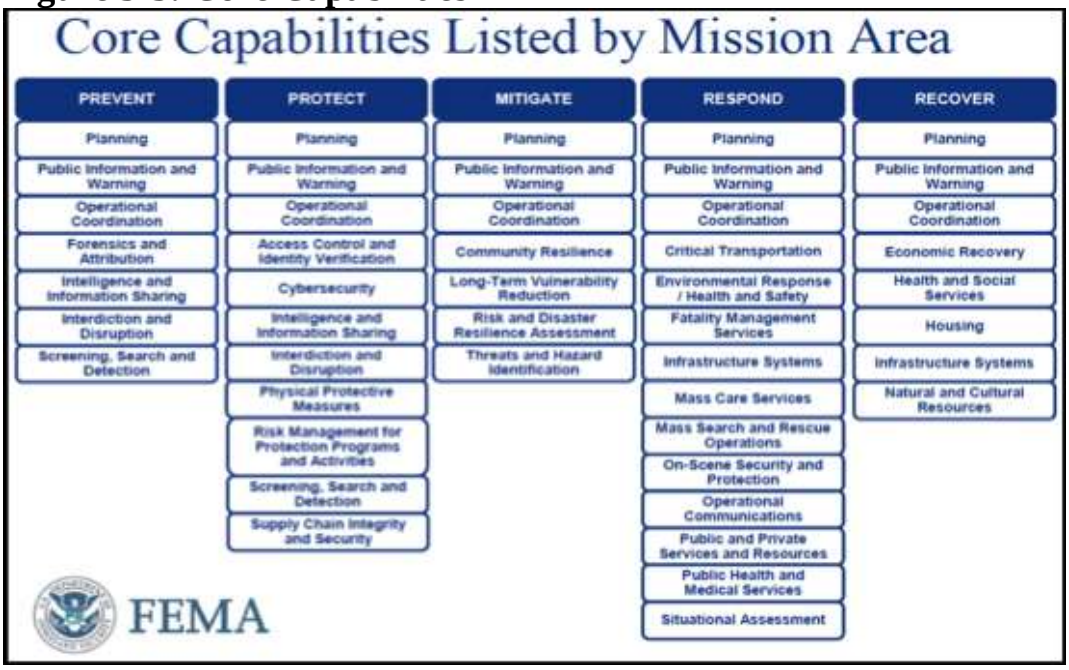
Source: http://eden.lsu.edu/Conferences/SCAP/Documents/Eric%20Runnels.pdf

13. **National Preparedness Goal** (NPG). PPD-8 sets out the Ends, Ways and Means of the US system with the former captured in the NPG:

> A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.

The NPG subsequently describes 31 core capabilities, as shown in Figure 3-3, needed to address the greatest risks. (Debatably, they are 'the Ways' rather than 'the Ends', but are shown here to conform with the way they are set out in PPD-8).

Figure 3-3: Core Capabilities



Source: http://eden.lsu.edu/Conferences/SCAP/Documents/Eric%20Runnels.pdf page 8

14. **Defence Involvement**. The National Military Strategy of the United States of America 2015 sets out the Strategic and Military Environments within which US forces will operate.[18] It confirms that the

[18] The National Military Strategy of the United States of America, p.1-4, June 2015.

purpose of the US military is to protect the Nation and win its wars setting out the National Military Objectives in the process, which are:

a. Deter, deny, and defeat state adversaries.

b. Disrupt, degrade, and defeat violent extremist organisations.

c. Strengthen our global network of allies and partners.

All of these objectives are outward looking in nature, rather than domestic. Curiously, the paper produces a fourth heading entitled 'Advance Globally Integrated Operations'[19] that contains a list of Joint Force Prioritised Missions that includes the following statement:

d. **Provide Support to Civil Authorities**. When man-made or natural disasters impact the United States, our military community offers support to civil authorities in concert with other U.S. agencies. As part of that effort, we integrate military and civil capabilities through FEMA's National Planning System and National Exercise Program. During domestic events, U.S. military forces — including National Guard and Reserve units — provide trained personnel, communications capabilities, lift, and logistical and planning support. They work alongside civilian first-responders to mitigate the impact of such incidents and keep our citizens safe.

15. **Defense Support of Civil Authorities** (DSCA). The National Military Strategy translates Presidential Policy Directives into Department of Defense (DoD) Directives and, in this instance, PPD-8 into DSCA, which will be covered in more detail under 'The Ways' below. However, it is useful at this point to understand that DSCA is governed by a uniquely complicated structure almost certainly unique to the US as a historical legacy. DSCA is defined in Joint Publication 3-28[20] as the:

Support provided by federal military forces, Department of Defense (DOD) civilians, DOD contract personnel, DOD component assets, and National Guard (NG) forces (when the

---

[19] Ibid.,p.10.

[20] US Joint Publication 3-28, Defense Support of Civil Authorities, p.vii, 31 July 2013.

Secretary of Defense (SecDef), in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, United States Code[21], status or when federalized) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.

DSCA in the US presents a unique challenge based on the history of the country and the interaction of the federal, state, local, territorial, and tribal governments and private and non-profit organizations. These relationships establish multiple layers and mutually reinforcing structures throughout the state and territorial governments for interaction based on the US Constitution, as well as on common-law and traditional relationships.

The US – Ways

16. **The National Preparedness System** (NPS) **and National Response Framework** (NRF). The US approach to preventing, mitigating and recovering from a disaster is codified in the NPS and set out by the US Department of Homeland Security in the NRF.[22] The Executive Summary of the latter states that:

The National Response Framework is a guide to how the Nation responds to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System to align key roles and responsibilities across the Nation. This Framework describes specific authorities and best practices for managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters. The National Response Framework describes the principles, roles and responsibilities, and coordinating structures for delivering the core capabilities required to respond to an incident and further describes how response efforts integrate with those of the other mission areas. This Framework is always in effect and describes the doctrine under which the Nation responds to

[21] The US Code is a consolidation and codification by subject matter of the general and permanent laws of the US. It is prepared by the Office of the Law Revision Counsel of the US House of Representatives. (Source: http://uscode.house.gov).

[22] National Response Framework, Third Edition, June 2016.

incidents. The structures, roles, and responsibilities described in this Framework can be partially or fully implemented in the context of a threat or hazard, in anticipation of a significant event, or in response to an incident. Selective implementation of National Response Framework structures and procedures allows for a scaled response, delivery of the specific resources and capabilities, and a level of coordination appropriate to each incident.

17. **Secretary of Defense** (SecDef). The SecDef does not, routinely, have the responsibility or authority to deploy National Guard assets as that honour falls to the relevant state governor. Instead, as the NRF sets out: [23]

a. SecDef has authority, direction, and control over the DoD. DoD resources may be committed when requested by another Federal agency and approved by the SecDef, or when directed by the President. However certain DOD officials and organizations may provide support under the immediate response authority[24], a mutual aid agreement with the local community, or pursuant to independent authorities or agreements. When DOD resources are authorized to support civil authorities, command of those forces remains with the SecDef. DOD elements in the incident area of operations coordinate closely with response organizations at all levels.

18. **Defense Support of Civil Authorities** (DSCA). JP 3-28 Defense Support of Civil Authorities published in July 2013 sets out the overarching guidelines and principles to assist military commanders and their staffs in planning, conducting and assessing DSCA. Of note, it is a joint doctrine publication and not an authority in itself; instead that rests with combatant commanders and other joint force commanders. The JP explains that the:

---

[23] Ibid., p.17-18.

[24] In response to a request for assistance from a civilian authority, under imminently serious conditions, and if time does not permit approval from higher authority, DOD officials may provide an immediate response by temporarily employing the resources under their control, subject to any supplemental direction provided by higher headquarters, to save lives, prevent human suffering, or mitigate great property damage within the United States. Immediate response authority does not permit actions that would subject civilians to the use of military power that is regulatory, prescriptive, proscriptive, or compulsory. Ibid.,p.18.

a. DOD has a large role in supporting the NRF. The NRF applies to all incidents requiring a coordinated federal response as part of an appropriate combination of federal, state, local, tribal, private sector, and nongovernmental entities. DSCA operations may occur in response to, or in anticipation of, a presidential declaration of a major disaster or an emergency, in coordination with the primary agency.

b. DSCA operations are consistent with the NRF in that they aim to supplement the efforts and resources of other US Government departments and agencies in support of state, local, and tribal governments, and voluntary organizations. When executing DSCA, the US military is in support of another USG department or agency that is coordinating the federal response. The President can direct DOD to be the lead for the federal response; however, this would only happen in extraordinary situations and would involve other DoD core mission areas. US federal and National Guard forces may also be conducting support at the state, local, or tribal levels.

19. **Command and Control in United States Northern Command** (USNORTHCOM) **Area of Responsibility**[25]. For DSCA operations SecDef designates a supported Combatant Commander (CCDR). Ordinarily, this will be CDRUSNORTHCOM for Continental United States (CONUS), Alaska, Puerto Rico, and the US Virgin Islands (and CDRUSPACOM for Hawaii, Guam, American Samoa, and the Northern Mariana Islands). Each CCDR provides, on a permanent basis, an Emergency Preparedness Liaison Officer (EPLO)[26] to each of the Federal Emergency Management Agency (FEMA) regions across the United States as shown in Figure 3-4 on the subsequent page. EPLOs are senior Reserve Component officers who are administered by and report to program managers within their respective Services that also provide EPLOs with training and equipment via appropriate sources. EPLOs are activated and employed by their Services at the request of the supported CCDR. They are trained in emergency management and DSCA operations. They advise civil authorities on military resources and capabilities and

[25] United States Pacific Command (USPACOM) has a distinct area of responsibility for DSCA roles but as the principles are the same as those for USNORTHCOM it is expedient to treat them here as a single entity.

[26] US Joint Publication 3-28.op.cit., Chapter 2, p.13.

facilitate coordination between civil authorities and DOD during state or federal exercises or DSCA operations.

Figure 3-4: FEMA Regions

Source: JP3-28, Chapter II, Page 13

20. **Operational Phases for DSCA**. It is usual for DSCA operations in the US to be carried out in six phases, namely: Shape, Anticipate, Respond, Operate, Stabilise, and Transition. They are designed to occur sequentially but some activities, inevitably, begin in a previous phase or continue into a subsequent one. Depending on the prevailing crisis condition multiple phases maybe occurring in one or more of the FEMA regions simultaneously. The specific phases, and the definitions are shown in Figure 3-5 on the next page.

Figure 3-5: DSCA Phases

a. **Phase 0 (Shape).** Phase 0 is continuous situational awareness and preparedness. Actions in this phase include interagency coordination, planning, identification of gaps, exercises, and public affairs (PA) outreach. These activities continue through all phases. Shaping operations are inclusive of normal and routine military activities and various interagency activities to assure or solidify relationships with partners, friends, and allies. This phase sets the conditions for expanded interoperability and cooperation with interagency partners via active engagements in planning, conferences, training programs and exercises, and coordination and interaction.

b. **Phase I (Anticipate).** Phase I begins with the identification of a potential DSCA mission, a no-notice event, or when directed by the President or SecDef. The phase ends with assigned response forces deployed or when the determination is made that there is no event requiring DSCA response. Phase I success is achieved when deployment of a DCO, EPLO, and other selected response forces is accomplished. These forces are postured to facilitate quick response after coordination with the primary agency PFO/JFO and coordination with state, local, and tribal officials.

c. **Phase II (Respond).** Phase II begins with the deployment of initial response capabilities. The phase ends when response forces are ready to conduct operations in the JOA. Phase II success is achieved when forces are deployed with sufficient capability to support civil authorities in accomplishment of the mission. DSCA operations are based on RFAs, which will be made at different times, and for missions that will be completed at different times. Consequently, forces will likely deploy into and out of the JOA during the entire DSCA operation.

d. **Phase III (Operate).** Phase III begins when DSCA response operations commence. Phase III ends when Title 10, USC, forces begin to complete mission assignments and no further requests for DOD assistance are anticipated from civil authorities. Phase III success is achieved when currently deployed DOD capabilities are sufficient to support civil authorities.

e. **Phase IV (Stabilize).** Phase IV begins when military and civil authorities decide that DOD support will scale down. Phase IV ends when DOD support is no longer required by civil authorities and transition criteria are established. Phase IV success is achieved when all operational aspects of mission assignments are complete.

f. **Phase V (Transition).** Phase V begins with the redeployment of remaining DOD forces. The phase ends when response forces have been relieved, redeployed, and OPCON is transferred to their respective commands. Phase V success is achieved when DOD forces have transitioned all operations back to civil authorities.

Source: JP3-28, Chapter II, Page 13

21. **Prohibited Direct Assistance**. A curiosity of the US legal system is that certain activities are prohibited for military forces acting under Title 10. They include[27]:

[27] Ibid., Chapter III, p.4.

a. Interdiction of a vehicle, vessel, or aircraft.

b. A search or seizure.

c. An arrest, apprehension, stop and frisk, or similar activity.

d. Use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators.

The US - Means

22. **The National Guard** (NG). As mentioned previously, the US Code system governs the use of NG assets (Title 32) in a distinctly separate way from those of Federal Defense assets (Title 10) and, as a result, they tend to be more readily deployable in the event of a domestic emergency. The NRF explains that[28]:

a. The National Guard is an important state and Federal resource available for planning, preparing, and responding to natural or manmade incidents. National Guard members have expertise in critical areas, such as emergency medical response; communications; logistics; search and rescue; civil engineering; chemical, biological, radiological, and nuclear response and planning; and decontamination.

b. The governor may activate elements of the National Guard to support state domestic civil support functions and activities. The state adjutant general may assign members of the Guard to assist with state, regional, and Federal civil support plans.

23. **The U.S. Army Corps of Engineers** (USACE). The NRF explains that[29]

The U.S. Army Corps of Engineers has independent statutory authorities regarding emergency management, such as Section 5 of the Flood Control Act of 1941 (Public Law 84-99) (e.g., providing

[28] National Response Framework.op.cit.,p.14.
[29] Ibid.,p.18.

> technical assistance; direct assistance such as providing sandbags, pumps, and other types of flood fight materials, emergency contracting; and emergency water assistance due to contaminated water source). In addition, the USACE urban Search and Rescue (SAR) programme provides technical and operational support to FEMA urban SAR and supports other state, local, and international urban SAR programmes.

24. **Defense Logistics Agency** (DLA). Similar to USACE, the DLA has an interagency agreement with FEMA to provide commodities including fuel to civil authorities responding to disasters.

25. **Explosive Ordnance Disposal** (EOD). DoD EOD personnel are authorised to provide immediate response in support of civilian authorities, when requested, in the mitigation, rendering safe, and disposal of suspected or detected UXO, damaged or deteriorated explosives or munitions, improvised explosive devices, other potentially explosive material or devices, or other potentially harmful military chemical munitions or devices, that create an actual or potential imminent threat to human health, including safety, or the environment, including property.

26. **Intelligence Support**. Again, due to existing laws DoD intelligence component personnel are limited in the mission set they are allowed to perform and anything that steps over those boundaries must be expressly approved by SecDef[30]. It is a legal minefield and needs lawyers to be involved nearly every step of the way. It acts as a significant barrier to their use.

27. **Logistics**. Contrary to the Intelligence Support nightmare, the Joint Publication is a triumph of freedom when it comes to logistics for it states, with eloquent simplicity:

> During times of crisis, DoD may provide vital logistics support to civil authorities.

Inevitably there are a whole host of authorities, responsibilities and details set out in support but the broad principle is one of enablement rather than restriction. That said, supply is largely aimed at self-sustainment and transportation requires approval by SecDef.

---

[30] US Joint Publication 3-28.op.cit., Chapter V, p.3.

28. **Engineering**. In general, DoD engineering forces are called upon once federal, state, tribal and local contract resources are fully engaged, exhausted, or timely action is necessary to save lives and prevent further human suffering and loss of property.[31] Emphasis is placed on using contractors whenever possible but after that general engineer priorities are:

a. Force bed-down with Force Protection considerations.

b. Emergency stabilization and repair of damaged critical infrastructure. Repairs/work-arounds to other critical public utilities, services, and facilities that will help restore the ability of the local authority to manage its own recovery efforts.

c. Emergency clearing of debris from streets, roads, bridges, airfields, ports, and waterways in support of recovery and humanitarian needs.

d. Immediate humanitarian needs of the dislocated populace, such as the construction of temporary shelters and support facilities.

e. Demolition of damaged structures and facilities that pose a significant risk to the public.

29. **Health Services**[32]. As a supporting agency to the Department of Health and Human Services, the DoD coordinates mission assignments involving health services through the relevant FEMA region Defence Coordinating Officer. DoD employs and integrates medical response through the following joint medical capabilities: first responder care; forward resuscitative care; en route care; and theatre hospitalization. The focus of DoD medical support is to restore essential health services in collaboration with the state and local health authorities. The scope of the medical response will vary with the type and scale of emergency. A clear focus remains on transition to other medical support organizations.

30. **Animal and Plant Disease Eradication**. The DoD is authorised to provide assistance to the US Department of Agriculture

[31] Ibid., Chapter V, p.7.
[32] Ibid., Chapter V, p.11.

(USDA) to contain and eradicate an actual or imminent outbreak of plant or animal disease. USDA will receive priority support including, when appropriate, DoD veterinary support activity.[33]

31. **Cyberspace Support**. During DSCA operations, DoD forces may be required to assist state and local networks to operate in a disrupted or degraded environment including the remediation and creation of critical emergency telecommunication networks. They also may be required to provide cyberspace support services to secure critical information infrastructure.[34]

32. **Chemical, Biological, Radiological, Nuclear and High-Yield Explosive (CBRNE) Consequence Management (CM)**. Direction for DoD CBRNE response is contained in the Chairman of the Joint Chiefs of Staff (CJCS) CBRNE Executive Order (EXORD) 2011[35]. The purpose of the EXORD is to delegate limited approval authority to the supported CCDR in order to provide a rapid and flexible federal response for potential or actual CBRNE emergencies or disasters within the US in order to save lives and minimise human suffering.

Thailand – Ends

33. **Strategic Background**. The Disaster Prevention and Mitigation Act 2007 provides the main legal basis and framework for disaster risk management in Thailand. Article 44 requires the National Disaster Prevention and Mitigation Plan (NDPMP) to be revisited every 5 years by the Department of Disaster Prevention and Mitigation (DDPM)[36]. The NDPMP was cleared by the National Disaster Prevention and Mitigation Committee (NDPMC) on 9 February 2015 and subsequently endorsed by the Thai Cabinet on 31 March 2015. The current plan underwent a participatory planning process, where related sectors were engaged, including public, private and civil society and all relevant agencies, including the military, are required to use it as a blueprint, framework and guidelines in handling national disaster management actions. They are to implement the plan, to develop their own action plan

[33] Ibid., Chapter V, p.13.

[34] Ibid.

[35] CJCS CRBNE EXORD, dated 21 Jun 2011.

[36] Thailand's National Disaster Prevention and Mitigation Plan 2015 Tri-fold (2.อังกฤษ(ชิดซ้าย).pdf), p.1.

and to incorporate projects and programmes on disaster risk management into their annual plan. The Cabinet also urged the Budget Bureau, concerned agencies and local governments to allocate sufficient budget to projects and programmes on disaster risk reduction, emergencies response and recovery in a sustained manner[37].

34. **Policy and Strategy on Disaster Risk Management** (DRM). The essential components of policy and strategy for DRM are set out in the NDPMP. An abridged version is as follows[38]:

a. **Disaster Risk Management Target**.

1) To ensure overall readiness of the national disaster risk management system to deal with potential disaster incidents through integrated and coordinated collaboration with stakeholders across multiple sectors and countries to timely provide disaster relief and emergency assistance to disaster affected people.

2) To cultivate a lifelong learning culture amongst, and boost the natural disaster immunity of, all sectors of society in Thailand aiming to gain a better grasp of the ways to manage disaster risk.

3) To increase public safety awareness through highlighting the creation of body of knowledge, awareness, and safety culture as well as developing local and community capacity gearing towards building community resilience to disasters.

b. **Objectives of National Plan**.

1) To provide consistent nationwide concept of operations to enable national and local governments, private sector, and other sectors of society to collectively implement disaster management activities in an integrated and systematic manner, and in the same direction.

---

[37] Ibid.

[38] National Disaster Risk Management Plan 2015, p.15-19.

2) To compile the current internationally recognized guidelines and directions and are used worldwide for disaster risk management that can be applied to disaster risk management in a Thai context.

3) To develop and enhance capacities for disaster risk management which encompasses disaster risk reduction, emergency management and building back better and safer at community, local, national and international levels to further minimize the potential losses from disasters.

b. **National Disaster Management Policy**. The NDPMC laid down the following four national disaster management policy framework's focus areas.

1) Improving and promoting disaster risk reduction by means of boosting the efficiency of disaster prevention, preparedness, and reducing disaster impacts.

2) Synergizing multi-sectoral partnerships' efforts to develop and enhance the capacities necessary for more effective, efficient and coherent emergency management.

3) Developing disaster recovery system that ably handles the demand for recovery assistance of disaster victims.

4) Developing and promoting the standards on international cooperation for disaster risk reduction between and among partnerships and networks at both national and international levels.

c. **Disaster Risk Management Strategy**. The strategies for DRM are:

Strategy 1: Focusing on disaster risk reduction

Strategy 2: Applying integrated emergency management system.

Strategy 3 Strengthening and enhancing the efficiency of sustainable disaster recovery.

Strategy 4 Promoting and strengthening international cooperation on disaster risk management.

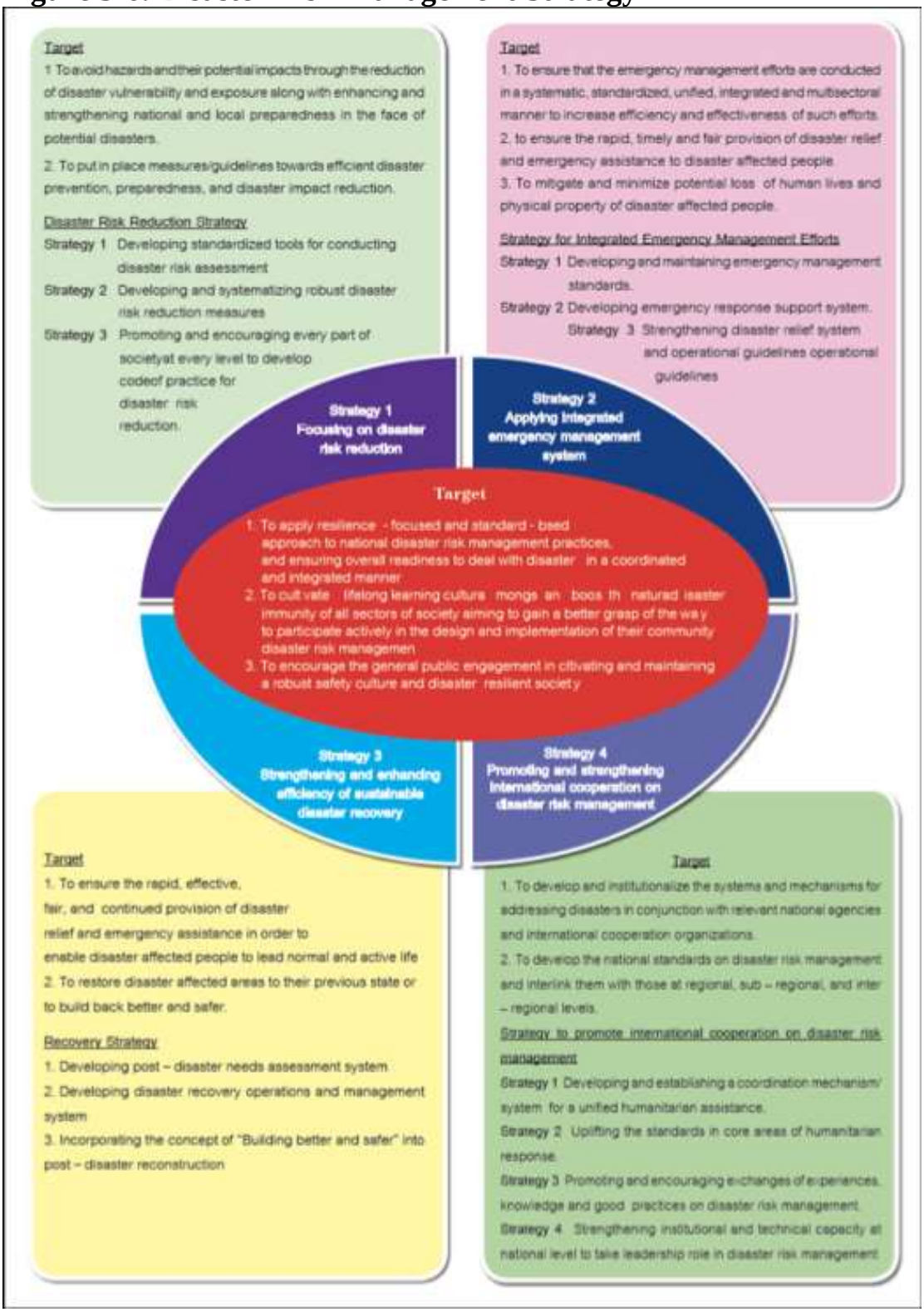
In his speech on 13 September 2015, Deputy Interior Minister Sutee Markboon explained that:

> At the national level, relevant agencies have adopted the National Disaster Prevention and Mitigation Plan 2015 for their operations. The plan consists of four strategies. In the first strategy, emphasis is placed on prevention and the reduction of impacts from disasters. The second strategy seeks to integrate disaster management in emergency situations. The third strategy seeks to enhance the efficiency of rehabilitation on a sustainable basis. In the fourth strategy, Thailand will step up cooperation with the international community in disaster risk reduction.
>
> Thailand has also incorporated the priorities for action in the Sendai Framework for Disaster Risk Reduction 2015-2030 into the National Disaster Prevention and Mitigation Plan. The priorities include understanding of all aspects of disaster risk, improved risk governance, investment in disaster risk reduction and better preparedness. The Sendai Framework was adopted in March 2015 at the Third United Nations World Conference on Disaster Risk Reduction, held in Sendai, Japan[39].

The Strategies and their supporting Targets are set out diagrammatically in Figure 3-6 below:

[39] http://thailand.prd.go.th/ewt_news.php?nid=2148&filename=index.

Figure 3-6: Disaster Risk Management Strategy



Source: National Disaster Risk Management Plan, page 20

Thailand – Ways

35. **Disaster Risk Management Cycle**. The DDPM has been implementing the NDPMP through Disaster Risk Management (DRM) and "Build Back Better and Safer" approaches to guide the country's disaster management efforts in a more proactive and sustained manner. In doing so, the emphasis has been put on developing collaboration among sectors in enhancing DRM capacity, strengthening community disaster preparedness, enhancing efficiency of recovery system and promoting international cooperation for DRM[40]. A change in disaster management thinking and practice has been brought about towards taking a more proactive and sustainable approach that includes prevention, mitigation of disaster impacts and preparedness in parallel with emergency management. The cycle is set out diagrammatically below:

Figure 3-7: Disaster Risk Management Cycle

Source: National Disaster Risk Management Plan, page 27

[40] http://122.155.1.143/en/cdetail-2779-news-134-1/DDPM+implements+National+Disaster+Prevention+and+Mitigation+Plan+2015+Moving+forward+towards+disaster+risk+management+for+building+resilience+in+Thailand.

36. **Disaster Risk Management Mechanisms (1)**. The NDPMP sets out how a disaster should be managed at various different levels, which would come into play depending on the scale of the incident[41]. Details are provided in two separate sections, which, confusingly, both use the term 'Level' to codify their hierarchy. Logic suggests that it makes more sense to deal with them in reverse order to how they are set out in the plan because the second one (articulated here) makes reference to the first one.

37. **Level of Emergency and Incident Management**[42]. An emergency and incident management in a Thai context is classified into four levels based on a wide range of parameters, including area affected, size, severity level and complexity, number of population, existing capacity for emergency management as well as the availability and capability of resources. Those who have legal authority must take these parameters into account when making decisions to assume the role of Incident Commander. The levels are shown in Figure 3-8 below.

Figure 3-8: Activation Levels

Level	Management of	Person Authorized
1	Small – scale disaster	District Incident Commander, Local Government Incident Commander and/or Bangkok Metropolitan Assistant Incident Commander is responsible for directing and/or controlling functions
2	Medium – scale disaster	Provincial Incident Commander or Bangkok Metropolitan Incident Commander is responsible for directing controlling and commanding functions
3	Large – scale disaster	National Incident Commander is responsible for directing, controlling and commanding functions
4	Catastrophic disaster	The Prime Minister or the Deputy Prime Minister whom assigned by the Prime Minister is responsible for directing, controlling and commanding functions.

Source: Source: National Disaster Risk Management Plan, page 51

38. **Disaster Risk Management Mechanisms (2)**. Details on the Disaster Risk Management Mechanisms are articulated below along with a diagram at Figure 3-9.

[41] National Disaster Risk Management Plan 2015. p.28-32.
[42] Ibid., p.50.

a) **Policy Level**. There are 2 organisations with a pivotal role at the top level, namely the NDPMC and the National Safety Council (NSC). The former has been tasked to formulate national disaster management policy and integrate public-private partnerships as stipulated under the provisions of Article 6 and 7 of Disaster Prevention and Mitigation Act B.E. 2550 (2007). The role of the NSC is to propose national safety policy and practice guidelines as well as to undertake interagency coordination. The composition and functions of the NSC were set out in the Prime Minister's Office Regulation on National Safety B.E. 2538 (1995), and addendum.

b) **Operational Level**. The plan sets out the management centre structure as follows:

1) **National Disaster Command Headquarters** (NDCHQ). As a national command and control facilities this headquarters has responsibilities to direct, oversee, and coordinate the emergency management practices of all lower disaster management centres. The Minister of Ministry of Interior has been designated as the National Incident Commander, and the Permanent Secretary for the Ministry of Interior as the Deputy National Incident Commander. In the event of a very large scale event either the Prime Minister or his/her nominated Deputy Prime Minster will assume the National Incident Commander's role and responsibility.

2) **Central Disaster Management Centre** (CDMC). The Department of Disaster Prevention and Mitigation is required to set up the CDMC, and the Director General has been designated as the Central Incident Commander. Its functions and authority are set forth as follows:

i. In a non-emergency situation it coordinates and integrates emergency response information, resources, and plans of all relevant government agencies in order to ensure the overall state of readiness for handling any type of potential disaster.

ii. When a disaster is likely, it undertakes a full scale preparation for potential response operations, keeps a close watch on the disaster situation, conducts data analysis and rapid situation assessment, disseminates early warning message as well as reporting and providing recommendations to the National Incident Commander.

iii. During a disaster it directs, integrates, and coordinates the joint response operations for small – (level 1) and medium scale (level 2) disasters. In this context, the Central Disaster Management Centre is required to take responsibilities for directing, conducting disaster situation assessment and providing technical support and assistance to the National Incident command Headquarters, keeping a close watch on the disaster situation and disseminating early warning messages; and providing information and recommendations to the National Incident Commander for the purpose of making a decision on raising the level of the disaster incident to level 3 (large – scale incident).

iv. The CDMC is required to continue acting as the constituent part of the Emergency Response Coordination Centre under the National Disaster Command Headquarters in case of an upgrade to level 3 and level 4.

3) **Provincial Disaster Management Centre** (PDMC). This centre has been tasked to direct, control, provide support for and coordinate disaster risk management efforts within the respective provincial jurisdiction. The Provincial Governor has been designated as the Provincial Incident Commander with the Vice Provincial Governor as his deputy. A representative will be assigned to the PDMC from the MoD amongst other organisations and agencies.

4) **Bangkok Metropolitan Disaster Management Centre** (BMDMC). This centre has been tasked to direct, control, and coordinate disaster risk management efforts

within its jurisdiction; to develop action plans based on its vulnerability and exposure to specific hazards in line with the Bangkok Metropolitan Disaster Risk Management Plan and function as an emergency response unit when an actual disaster occurs within its jurisdiction. The Governor of Bangkok Metropolitan Administration will be the Bangkok Metropolitan Incident Commander and has been tasked to perform duties and responsibilities as stipulated in item (3) of Disaster Prevention and Mitigation Act B.E. 2550 (2007).

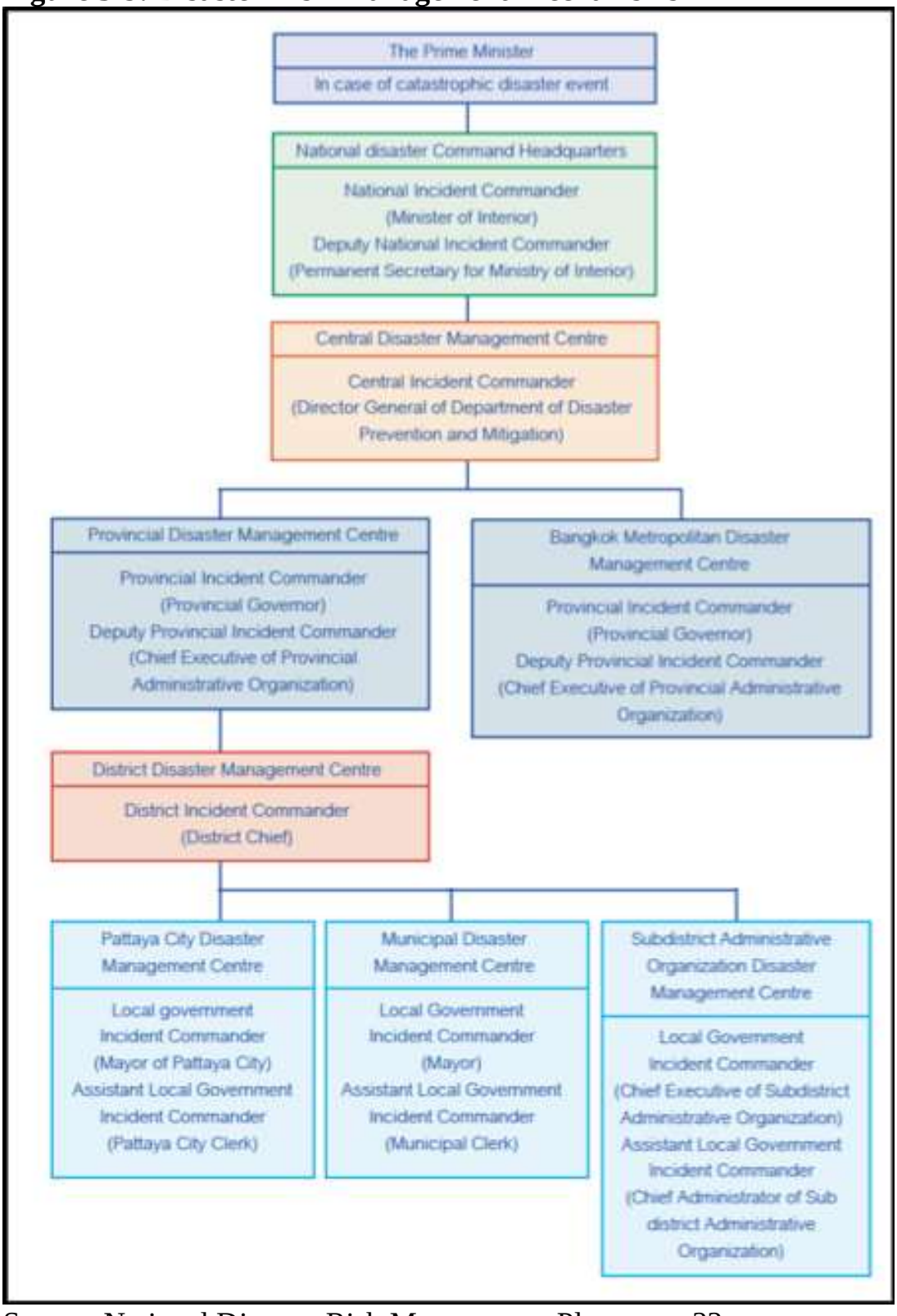
5) **District Disaster Management Centre** (DDMC). The DDMC has been tasked to direct, provide support for, and coordinate disaster management efforts of local administrative organizations located in its jurisdiction, as well as performing any function assigned by the Provincial Governor or by the PDMC. The Chief District Officer has been designated as the District Incident Commander and a representative from the MoD will also by assigned.

6) **Other Disaster Management Centres**. Along similar lines to those set out above, there are DMCs for Pattaya City, Municipal DMCs (city, town and Sub-district Administrative Organisations).

Much more detailed information, including legal authorities and guidelines for responsibilities and action plans are contained in the NDRMP[43].

[43] Ibid., p.51-124.

Figure 3-9: Disaster Risk Management Mechanisms



Source: National Disaster Risk Management Plan, page 33

39. **Role and Functions for the Military**. The specific roles and responsibilities for the Ministry of Defence are set out, very succinctly, as follows[44]:

a. To provide support and assistance to national efforts for disaster prevention and for addressing disaster situations in conformity with Article 8(3) of the Ministry of Defence Administrative Arrangements Act B.E. 2551 (2008).

b. To disseminate information and disaster warnings to Disaster Management Centres in the locality and the civilian government agencies located in the areas at risk, in case of imminent threat of war or airstrike of sabotage actions.

40. **Civil-Military Collaboration**. The NDRMP sets out[45] how the civil and military response to a disaster should collaborate together. It states that Civil–Military collaborative efforts in emergency management operations require very close coordination to promote an increase in mutual understanding and, in order to provide emergency management support to the NDCHQ, local DMCs at all levels, the military entity may consider setting up a Civil-Military coordination or operations centre. The centre can serve as a coordinating mechanism and venue for meetings and an exchange of information in order to gain and maintain situational awareness and share a common operating picture. It should also conform to international standard operating framework and the Disaster Prevention and Mitigation Act 2550 (2007) as follow:

a. To perform the duties in conformance with Article 46 of the Disaster Prevention and Mitigation Act B.E. 2550 (2007).

b. To perform the duties in accordance with the guidelines for Civil-Military collaborative efforts in a disaster.

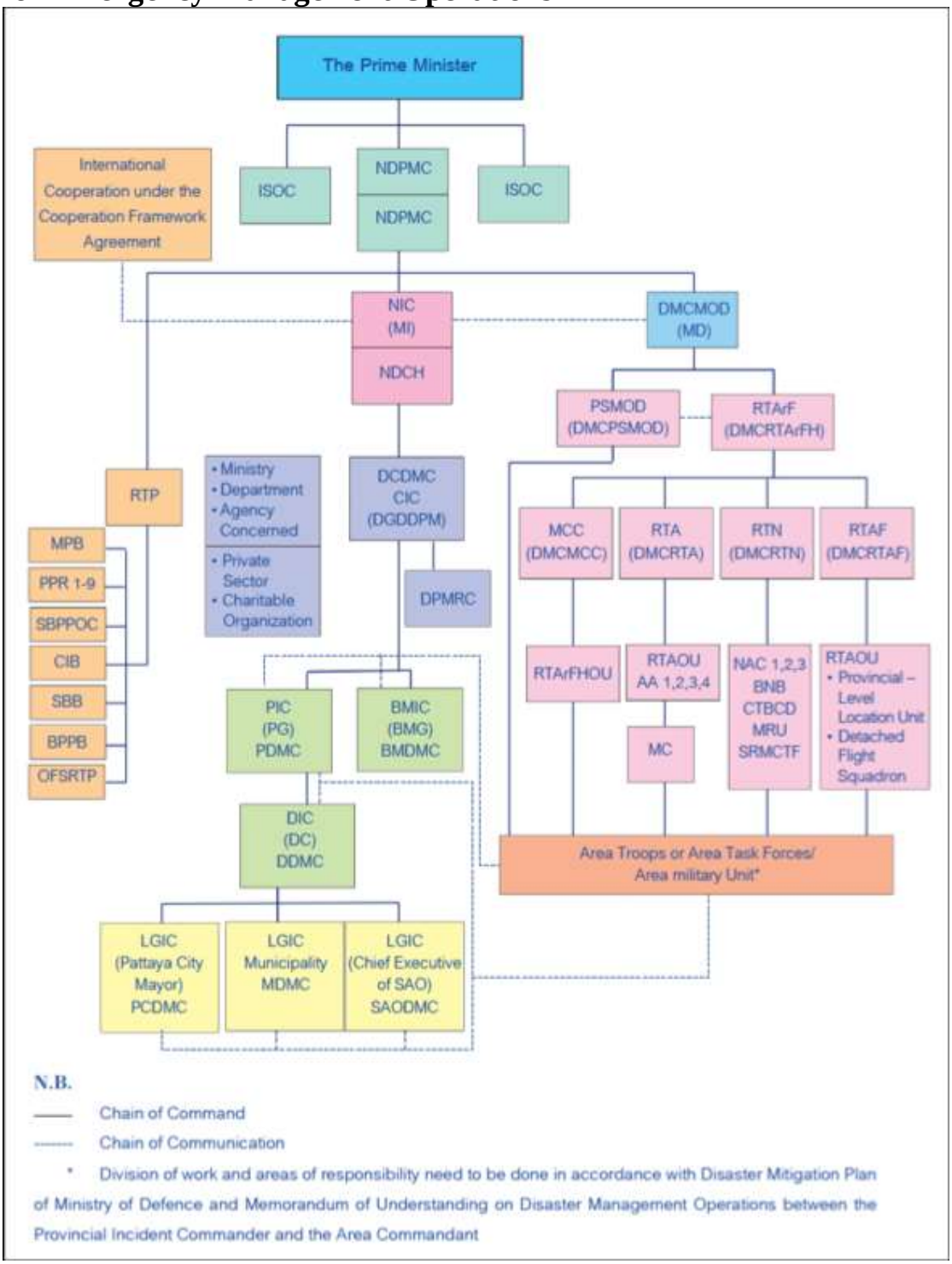
c. To maintain close contact and close coordination between civil and military actors.

A diagram showing the relationship between the various civil and military chains of command is shown at Figure 3-10 below.

---

[44] Ibid., p.34.
[45] Ibid., p.49.

Figure 3-10: Interagency Relationships and Collaborative Linkages for Emergency Management Operations



Source: National Disaster Risk Management Plan, page 48

Thailand – Means

41. **Thailand Disaster Relief Organisations**. Speaking at the 17th ASEAN Regional Forum Defence Officials' Dialogue (ARF DOD) held in New Delhi on 9 November 2009, Maj Gen Srisaran Dhiradhamrong (Special Advisor, MoD, Kingdom of Thailand), explained through his presentation entitled 'Armed Forces and Disaster management: Experience Sharing in Coordinating Humanitarian Assistance and Disaster Relief'[46], that Thailand has 3 main organisations involved with disaster relief:

a. **Department of Disaster Prevention and Mitigation**, Ministry of Interior: a hub of updating and policy making related to disasters and reliefs.

b. **Ministry of Foreign Affairs**: contacting international embassies in Thailand or overseas counterparts in case Thailand wants to deploy personnel.

c. **Ministry of Defence Disaster Relief Centres**. (DRC) (Also referred to as Disaster Management Centres (DMC)). The establishment of DRCs conformed to the Acts of Defence Department Civilians 2522 (1979), Civilian Defence Plan 2548 (2005) and Ministry of Finance Regulation on Advance Budget for State owned sector in assisting victims from emergency disasters 2546 (2003). A diagrammatic representation is at Figure 3-11.

Figure 3-11: Military Disaster Relief Centres

Source: Thai MoD Order 234/52 dated 28 Jul 2009

[46] Presentation: Armed Forces and Disaster Management, Maj Gen Dhiradhamrong.

42. **Military Disaster Relief Centres** (DRC). As can be seen by the representations in Figures 3-10 and 3-11, the application of military capability and resources are organised and controlled through a hierarchy of DRCs. The MoD DRC sits at the top and passes direction and resource (primarily financial authority) down to the single-Services and the Office of the Permanent Secretary for Defence. The Defence Minister acts as the Head of Operations, the Permanent Secretary and the Chief of the Royal Thai Armed Forces are Deputy Heads and each of the service chiefs becomes and Assistant Head. Below the DRCs Emergency Operations Centres (EOC) are set up close to the affected area. It has not been possible (in the English language and at the unclassified level) to discern precisely what orders, tasks, responsibilities and authorities have been passed down this chain, however, research into recent activity gives a good indication of the Means deployed to various situations. The MoD and RTArF DRCs do not appear to be heavily resourced and most of the responsibility thus falls to the single-Service DRCs.

43. **Military Tasks**. According to Maj Gen Srisaran, the following tasks were carried out by Thai military forces following the 2004 tsunami:

a. Searching for survivors and gathering bodies (Search & Rescue)[47].

b. Area improvement: removing and dismantling debris and obstacles out of the area and dumping them in the province's designated area.

c. Aircraft flew 432 flights totalling 616 hours of flight duration.

d. Support aircraft were used to transport patients and concerned staff and transport relief bags. (CASEVAC)

e. Distribution of relief bags and usable and consumable goods.

f. Repairing and building houses. (Engineering)[48]

[47] http://www.globalsecurity.org/military/world/thailand/navy-missions.htm.
[48] Ibid.

g. Medical care and mental rehabilitation (Medical support)

h. Provision of liaison officers.

i. Establishment of Donation Centres.

More recently, during the floods in 2016 the services:

j. Dispatched 12 Military Corps consisting of 3 Divisions of troops to assist[49]. (Non-specialist manpower support)

k. Provided ground transport to help evacuate flood victims and their property.

l. Reinforced flood defences using sandbags (General engineering).

m. Distributed survival bags

n. Built a temporary bridge to replace a collapsed bridge (Specialist engineering).

o. Provided information [50] and early warning [51] (Public Affairs).

p. Conducted route reconnaissance.

q. Traffic control.

r. Provided water, food, medical supplies and at times, emergency shelter for those affected. (In cold weather, blankets and clothing were distributed.)[52]

---

[49] https://www.thaivisa.com/forum/topic/957153-royal-thai-army-dispatches-12-military-corps-to-help-flood-victims-in-lower-south/.

[50] http://newsreleases.submitpressrelease123.com/2015/10/21/royal-thai-army-disaster-relief-center-to-cope-with-heavy-rain-and-floods/.

[51] http://www.globalsecurity.org/military/world/thailand/navy-missions.htm.

[52] Ibid.

s. Provided ships, boats, punts[53].

t. Provided towing mechanic teams to assist drivers.

A recent exercise also highlighted some additional tasks that the military were prepared to fulfil[54]:

u. Restoration of public services (Line of Communication).

v. Epidemic prevention (Water Treatment, Sanitation, Forensic, Mortuary Affairs)

w. Immediate relief aids (Temporary Shelter, Food and Water Supply).

x. CBRN Capability.

[53]http://www.globalsecurity.org/military/world/thailand/rtaf-intro.htm.

[54]https://ache-pko.blogspot.com/2015/02/asean-humanitaian-exercise-part-1-of-2.html.

Chapter 4
Meeting the requirement: Supply and Demand

"Efficiency is doing things right; effectiveness is doing the right things."[1]

"One cannot buy, rent or hire, more time."[2]

"The supply of government exceeds demand."[3]

Equilibrium – The quest for the Holy Grail

1. In an ideal world there would be a precise balance between the demand for support generated by a crisis and the response (supply) to meet it, as represented simply in Figure 4-1 below. Such an equilibrium may be described as the 'Holy Grail' for whilst it is the aiming point it is also wholly unachievable due to the unpredictable nature of both demand and supply.

Figure 4-1: The ideal relationship between Supply and Demand – The 'Holy Grail'

2. In reality there are a host of factors that have a bearing upon both the demand signal and the resource supply to meet it. Many of those elements have been discussed in previous chapters and the complexity of the relationship between them is compounded by their significant variance over time. The challenge therefore faced by crisis management planners is to define and quantify the various components of the most likely demand

---

[1] Peter F. Drucker, American Educator and Writer, 1980.

[2] Ibid., 1976

[3] Lewis H. Lapham, American Writer, 2001.

signal and then predict the 'who, what, when, and how' of the supply needed to achieve a balance. Arguably, demand can be considered as a single entity in this equation whilst supply may be defined as coming from three primary sources: The Whole of Government (WoG), the military and the community (which will include the business sector). The relationship between them all can be represented by a 4-way balance, as shown in Figure 4-2 below, because at any given moment each will vary in their size yet the overall aim is to achieve some measure of equilibrium. (Whilst, technically, supply could outweigh demand this would be a waste of resources and thus, over time, supply would naturally reduce especially, within the community sector.)

Figure 4-2: The 4-way relationship between Demand and Suppliers

As planners set about designing a system to get as close as they can to achieving a balance they can place a burden on the military (as discussed in Chapter 3) and the WoG but they can only predict what share the community will pick up. Each 'share' will also vary over time and by phase within a Disaster Management Cycle.

Assessing Supply

3. **The Disaster Management Cycle**. There is a tendency by the uninitiated to think that there will only be a demand signal during a crisis or, perhaps, during and after. In reality, demand exists before, during and after a crisis albeit the quantity and nature will vary. Many countries classify the various stages in similar terminology using a Disaster Management Cycle as depicted in Figure 4-3 below. The major components of the cycle are Mitigation and Preparation, which come before the crisis; the event or crisis itself; and then the Response and Recovery phases. The obvious risk to using such classification is it implies that each phase is easily defined, they run sequentially and that an

event has a clear initiation point; and it can be defined. In reality this is rarely the case and each phase will overlap meaning there will be concurrent demand and supply affecting each phase.

Figure 4-3: The Disaster Management Cycle

Source: http://globalasiablog.com/2016/12/06/disaster-asean-through-the-disaster-management-cycle/

4. The Global Development Research Center (sic) describes the Disaster Management Cycle and its component parts as follows[4]:

> a. Disaster management aims to reduce, or avoid, the potential losses from hazards, assure prompt and appropriate assistance to victims of disaster, and achieve rapid and effective recovery. The Disaster management cycle illustrates the ongoing process by which governments, businesses, and civil society plan for and reduce the impact of disasters, react during and immediately following a disaster, and take steps to recover after a disaster has occurred. Appropriate actions at all points in the cycle lead to greater preparedness, better warnings, reduced vulnerability or the prevention of disasters during the next iteration of the cycle. The

[4] Corina Warfield. The Disaster Management Cycle, p. 1-2, https://www.gdrc.org/uem/disasters/1-dm_cycle.html, undated.

complete disaster management cycle includes the shaping of public policies and plans that either modify the causes of disasters or mitigate their effects on people, property, and infrastructure.

b. The mitigation and preparedness phases occur as disaster management improvements are made in anticipation of a disaster event. Developmental considerations play a key role in contributing to the mitigation and preparation of a community to effectively confront a disaster. As a disaster occurs, disaster management actors, in particular humanitarian organizations, become involved in the immediate response and long-term recovery phases. The four disaster management phases illustrated here do not always, or even generally, occur in isolation or in this precise order. Often phases of the cycle overlap and the length of each phase greatly depends on the severity of the disaster.

1) **Mitigation** - Minimizing the effects of disaster. Examples: building codes and zoning; vulnerability analyses; public education.

2) **Preparation** - Planning how to respond. Examples: preparedness plans; emergency exercises/training; warning systems.

3) **Response** - Efforts to minimize the hazards created by a disaster. Examples: search and rescue; emergency relief.

4) **Recovery** - Returning the community to normal. Examples: temporary housing; grants; medical care.

5. **Crisis Management Considerations for the Military**. From a military perspective, there are a number of key headings that must be considered within each component phase of the Disaster Management Cycle in order to consider if an armed force can meet the requirement.

a. **Authority**. Before a military can act, in each phase of the Disaster Management Cycle, it must have the authority to do so. That authority should be defined in law and be transparent to the nation and the public. There must also be a recognised procedural

process to enable them to act, which should set out from where the authority is derived and over whom they have authority.

b. **Responsibility**. Having the authority to do something though is different from holding the responsibility to actual do it. In some instances, a military might hold a statute responsibility to act, meaning it must do it, the task is non-discretionary. An example might be provision of Explosive Ordnance Disposal. Other responsibilities might be assigned, amongst other reasons, for a specific geographic area, timeframe or scale of event.

c. **Structure**. A mechanism must exist for the military to be able to receive the task (the demand signal) and respond (the supply). The structure should be pre-determined but flexible enough to adapt to the circumstances. Orders might be passed downwards but, simultaneously requests for support might come in sideways (from other government departments) or upwards from those affected by a crisis.

d. **Resources**. As discussed in Chapter 3, the military must have the capability to respond. That capability will require consideration of the physical area of need, the scale of the demand, the nature of the demand (i.e. the type of support needed), the duration and, crucially, how it is to be financed.

e. **Affected versus Effective**. Depending on the particular crisis, and which phase of the Disaster Management Cycle is under consideration, a military component might itself have been affected by the event and thus no longer be effective. Redundancy is therefore essential to ensure that an effective response to the demand can be generated.

f. **Suitability and Sustainability**. Depending on the specific demand the military may not be the most appropriate or available resource to act. They may lack the expertise or the appropriate asset may already be performing a higher priority task from which it should not be diverted. Before committing to meet the demand, a military response must therefore be assessed for its suitability. Similarly, a decision must be taken on the likely duration of a task and whether military assets should be tasked for a limited time only, or whether it can be made available to complete

the task all the way through to completion of the recovery phase. Frequently a military asset will prove to be the most suitable during the response phase but, as time progresses and the situation moves back towards normal, it will be more appropriate to bring in a replacement asset from either the WoG or the community.

6. **Capability Management Frameworks**. There are a number of models available to assist in defining military capability and how it should be procured, managed and sustained. The US military uses 'DOTMLPF', which stands for Doctrine, Organisations, Training, Materiel, Leader Development, Personnel and Facilities. NATO has the same basis but includes an additional 'I' for interoperability. The UK MoD follows a similar principle but employs a different model known as 'TEPIDOIL'.

7. **The UK Defence Lines of Development (DLOD)**. The MoD Acquisition Operating Framework sets out 8 DLODs that make up TEPIDOIL and are defined as[5]:

a. **Training**. The provision of the means to practise, develop and validate, within constraints, the practical application of a common military doctrine to deliver a military capability.

b. **Equipment**. The provision of military platforms, systems and weapons, (expendable and non-expendable, including updates to legacy systems) needed to outfit/equip an individual, group or organisation.

c. **Personnel**. The timely provision of sufficient, capable and motivated personnel to deliver Defence outputs, now and in the future.

d. **Information**. The provision of a coherent development of data, information and knowledge requirements for capabilities and all processes designed to gather and handle data, information and knowledge. Data is defined as raw facts, without inherent meaning, used by humans and systems. Information is defined as

[5] UK MoD Defence Lines of Development, http://trak-community.org/index.php/wiki/Defence_Line_of_Development, undated.

data placed in context. Knowledge is Information applied to a particular situation.

e. Concepts & **Doctrine**. A Concept is an expression of the capabilities that are likely to be used to accomplish an activity in the future. Doctrine is an expression of the principles by which military forces guide their actions and is a codification of how activity is conducted today. It is authoritative, but requires judgement in application.

f. **Organisation**. Relates to the operational and non-operational organisational relationships of people. It typically includes military force structures, MoD civilian organisational structures and Defence contractors providing support.

g. **Infrastructure**. The acquisition, development, management and disposal of all fixed, permanent buildings and structures, land, utilities and facility management services (both Hard and Soft facility management) in support of Defence capabilities. It includes estate development and structures that support military and civilian personnel.

h. **Logistics**. Logistics is the science of planning and carrying out the operational movement and maintenance of forces. In its most comprehensive sense, it relates to the aspects of military operations which deal with; the design and development, acquisition, storage, transport, distribution, maintenance, evacuation and disposition of materiel; the transport of personnel; the acquisition, construction, maintenance, operation, and disposition of facilities; the acquisition of furnishing of services, medical and health service support.

Assessing Demand

8. In order to assess the size, duration and nature of the demand signal it would be helpful to identify objective and measurable indicators that can be applied to each situation. Regrettably, that is the scourge of the Crisis Management Planner and just not possible due to the unpredictability of what might happen. Nevertheless, there are some generalisations that can be made and will assist in codifying demand against a particular threat arising in a specific scenario.

9. **Scenarios**. A wide-range of scenarios were identified and discussed in Chapter 2 before the most likely threat scenarios for the three subject countries (UK, USA and Thailand) were down-selected to:

a. Flooding (regardless of cause or location such as inland or coastal).

b. Weather extreme effects (regardless of cause).

c. Catastrophic Terrorist Attack (of a conventional style only as the impact of the use of a Weapon of Mass Destruction (WMD) is so significant that it automatically will become international and require a global response).

d. Pandemic influenza (even though the same terminology is not used by Thailand).

e. Cyber Attack is only mentioned by the US, but undoubtedly is applicable to all given that it recognises no borders or boundaries.

10. **Six Honest Serving Men**. In his poem 'The Elephant's Child', written as part of the his 'Just So Stories'[6], Rudyard Kipling set out what he considered to be the most useful questions to ask in any given situation. He described them as his 'Six Honest Serving Men' and went on to explain how they should be used.

I keep six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who.
I send them over land and sea,
I send them east and west;
But after they have worked for me,
I give them all a rest.

11. When seeking to assess the demand likely to arise from each of the most likely threat scenarios it would be an ideal if we were able to

[6] Rudyard Kipling. Just So Stories for Little Children. 1st ed (London : Macmilian, 1902).

just use Kipling's 6 honest serving men (What, Why, When, How, Where and Who?) however, reality tends to lead us towards to a far more detailed analysis appropriately seeking underpinning data. Such an approach would far outstrip the mechanism of this paper but provides a flavour of the challenge facing Crisis Management planners. The task is compounded by the lack of access to data that is of a classified nature. A subjective approach must therefore be taken to assess the potential scale of demand within each scenario and, in this instance, it is based on the author's experience of living in and researching each of the three subject countries. Critically though, the purpose of this paper is to assess if the military are able to meet the tasks they have been given, rather than seeking to assess if the combined endeavours of the WoG, the community (including business) and the military can meet the demand signal and thus achieve a balance. The demand signal is therefore the tasks laid upon the military as set out in Chapter 3.

Supply and Demand

12. The relationship between the demand signal and the military response (supply), by country, can be considered against each of the 5 scenarios using the DLODs and Crisis Management Considerations set out above, against the phases of the Crisis Management Cycle. Doing so provides an indication of strengths, weaknesses and some gaps that need addressing given the potential impact on each of the countries and lead to a number of recommendations, which are set out in the next Chapter. What follows are a series of graphic representations of each country's situation and a description of the good, the bad and the downright ugly. A traffic light system has been employed to provide a visual indication of the relative representation. Areas shaded green suggest that there is a good relationship between supply and demand; that the issue has been considered in the nation's plan throughout all, or at least most, stages of the Disaster Management Cycle and the various Defence Lines of Development. Orange indicates that there are some areas for concern with the demand and supply balance and, perhaps, some issues with some of the DLODs. Red indicates significant cause for concern with the demand and supply balance and some glaring deficiencies with relevant DLODs.

13. **The UK**. Figure 4-4 sets out a subjective view of how well placed the UK military is to deal with the scale and nature of the subject threat scenarios.

Figure 4-4: Graphic Representation of UK's Demand and Supply Balance

UK	Significant Flooding	Weather Extremes	Terrorist Attack	Pandemic Influenza	Cyber Attack
Training					
Equipment					
Personnel					
Information					
C & D					
Organisation					
Infrastructure					
Logistics					
Authority					
Responsibility					
Structure					
Resources					
A v E					
S & S					

Key:

Green: Supply and demand in reasonable balance; DLODs mainly covered.

Orange: some cause for concern between supply and demand balance; some DLODs out of kilter.

Red: Significant variance between supply and demand; DLODs deficient and in need of addressing.

14. **Subjective Analysis**.

a. **Significant Flooding and Weather Extremes**. From Chapter 2 it can be seen that the UK does not tend to suffer regularly from devastating flooding or weather extremes although the potential does exist and the 1953 coastal flooding emergency is a case in point. In this context, the most damaging scenario would be a flood of the eastern seaboard leading to flooding in London and the east counties. When (rather than if) that happens again the impact will be significant and the military will struggle to meet the

demand. A WoG effort to improve coastal defences (Mitigate and Prepare) will help but, when the military are tasked to support, a lack of numbers, equipment, infrastructure, logistics and resources will significantly reduce the effectiveness of the response. Military units are spread across the country, therefore the numbers of military caught up in the problem should be easily manageable although their ability to operate for sustained periods will be reduced due to a lack of redundancy. Direction on Authorities and Responsibilities have been clearly set out, as are Concepts and Doctrine but there is little room for an increase in capacity during the Response and Recovery phases. The area for greatest risk lies with the tendency for politicians to task the military far too late in the process and always after the event, making the response itself less effective.

b. **Terrorist Attack**. The UK has suffered from various forms of terrorist attack for a significant length of time. For the majority of the last century the threat came from a domestic insurgency but more recently it has morphed into a broader international based threat. The consistency and regulatory of such occurrences, coupled with significant experience gained from overseas operations, means that, within defined parameters, the British Military is well prepared, equipped and trained to contribute to the solution when asked to do so. Concepts and Doctrine are well articulated and authorities and responsibilities are enshrined in law. The greatest threat to the UK military not being able to meet its tasks lies with the potential for it to be a target itself and thus some of its response and, to a much more limited extent, recovery capability might be severely denuded. The particular challenge that must be addressed is the impact that could occur from a catastrophic terrorist attack (even a conventional one as opposed to an NBC attack).

c. **Pandemic Influenza**. The UK has classified a pandemic influenza outbreak as the most significant civil emergency risk. Whilst the H1N1 influenza in 2009 did not come anyway close to the worst predictions it has no effect on the likelihood a similar or worse outbreak occurring. The WoG is putting significant effort into preparing for and mitigating a major event but resources are already stretched and many of them ‘double-tap’ to cover off both civilian and military tasks. Surge capacity is therefore minimal. Similarly, military resources and equipment are geared towards

providing medical cover on deployed operations rather than for a domestic emergency. Responsibilities are less well defined than in other areas and there is a very strong possibility that many members of the military would themselves become victims of an outbreak. In a recent potential example, military resources were used to help respond to the risk of an Ebola outbreak but, thankfully, the numbers of victims were very few meaning that the military were able to meet the demand. It would not have needed much of an increase before that capability would have been overwhelmed. What is less clear is precisely what the military will be asked to do during response and recovery phases and thus, unsurprisingly, what they are doing during mitigation in order to prepare (training and Concepts & Doctrine).

d. **Cyber Attack**. It is curious to note that whilst a cyber attack is classified as being highly plausible during the next 5 years its relative impact is defined as being low. As recently as May 2017, the Wannacry Ransomeware virus attack had a significant effect on the running of at least one government department (the National Health Service) in the UK. (Similar effects were experienced by many countries around the world.) The military response to such events in the future may prove to be both direct and indirect. Direct, in that they will have to contribute to dealing with the cyber attack, especially if it is against military cyber architecture, but also indirect, in dealing with the subsequent symptoms. (In the example of the Ransomeware above, military assets might have been used to support the NHS in delivering its service (i.e. healthcare provision). At present, the allocation of resources across the DLODs is minimal although the military is working very hard to address the situation. Concepts and doctrine are being drawn up, new specialist personnel have been recruited and are being trained. Simultaneously a review is being conducted to identify direct vulnerabilities. The risks posed by a major attack are significant and, seemingly, not dissipating. It is self-evident that the UK is 'behind the curve' and is having to adjust during the preparation phase in order that it is better placed for the response phase and, if necessary, for subsequent recovery.

15. **The USA**. Figure 4-5 sets out a subjective view of how well placed the US military is to deal with the scale and nature of the subject threat scenarios.

Figure 4-5: Graphic Representation of USA's Demand and Supply Balance

USA	Significant Flooding	Weather Extremes	Terrorist Attack	Pandemic Influenza	Cyber Attack
Training					
Equipment					
Personnel					
Information					
C & D					
Organisation					
Infrastructure					
Logistics					
Authority					
Responsibility					
Structure					
Resources					
A v E					
S & S					

Key:

Green: Supply and demand in reasonable balance; DLODs mainly covered.

Orange: some cause for concern between supply and demand balance; some DLODs out of kilter.

Red: Significant variance between supply and demand; DLODs deficient and in need of addressing.

16. **Subjective Analysis**.

a. **Significant Flooding and Weather Extremes**. The US suffers from a range of natural hazards on a daily basis. Whether it is forest fires, tornados, mudslides or something in between there is always something going on. It is unsurprising, therefore, the tasks placed upon the US military to help are significant and they have set up a large command – United States Northern Command – to deal with it through all phases of the Crisis Management Cycle. The size and scale of the geography and topography involved is reasonably

well matched by the strength and depth of the US military organisation although it brings with it some of the drawbacks of scale too. There can be little doubt that the bureaucracy involved frequently delays the military response and the fundamental principles enshrined in Title Law deliberately restricts many assets from being used in many circumstances. All that said, when it wants to, there is nearly always a way to get around the problem. Fairly recent crises such as Hurricane Katrina and Superstorm Sandy led to a vast improvement in training, information, concepts and doctrine. Many authorities were re-written and responsibilities defined more accurately. It is highly unlikely that the US military would not have sufficient assets somewhere to overcome the challenge of those who have become directly affected by an event and, with the exception of certain specialist capabilities, their sheer volume means they will be able to sustain their commitment throughout the response and recovery phases. The biggest challenge to a significant flood or weather extreme event will come when the incident takes places in a major population area, making it hard to get sufficient resources into place.

b. **Catastrophic Terrorist Attack**. The US suffered, arguably, the most significant and catastrophic terrorist attack in history on 11 September 2001. For those involved it was truly calamitous and led to worldwide repercussions, however, the actual events themselves were in a relatively small area and thus the direct military response was comparatively compartmentalised and on a limited scale. It is, sadly, very possible that the next catastrophic terrorist attack could directly affect a much larger percentage of the population requiring far more military involvement in the response and recovery phases. 9/11 did, however, act as a catalyst for the US to increase its training, equipment and personnel assets focussed on combatting terrorism. Their authorities and responsibilities are clear and they have a structure in place to act. Significant effort has been made during the mitigation and preparation phases and there is little doubt that the US military has the capacity to endure. The greatest risk to their ability to meet the demand signal lies in the risk of key assets being the target. That said, they enjoy far greater redundancy than most countries around the world and are thus still likely to be able to respond extremely well.

c. **Pandemic Influenza**. If scale and dispersion are a strength when dealing with a Terrorist Attack they may well prove to be the exact opposite when considering a pandemic influenza. As noted in Chapter 2, the US have recognised that a virulent strain could kill hundreds of thousands of Americans and affect millions more. An incident on such a scale will most likely overwhelm not just the WoG but the community response as well. The military would have to get involved on a vast scale whilst also, almost certainly, having larger numbers of its own people affected as well. Training for such an event is very difficult as, similarly, is an ability to prepare appropriate concepts and doctrine. US Title 10 versus Title 32 laws will also act as a potential hindrance to the immediate response.

d. **Cyber Attack**. There are millions of cyber attacks around the world every day and the US receives more than its fair share. It is unsurprising, therefore, that the US military is heavily involved in combatting them. The scale, purpose and effect of those acts varies considerably however, and it is the challenge of defining the authorities and responsibilities falling to the US military in a highly fluid environment that makes it hard to guarantee success. Recruiting and training sufficient people is proving hard as is procuring the appropriate assets. That said, the US arguably, has the greatest knowledge and experience in this field and is thus probably best placed to respond and lead the recovery. It is, nevertheless, much harder to define what is a military task versus one that should fall to WoG or the community at large.

17. **Thailand**. Figure 4-6 sets out a subjective view of how well placed the Thai military is to deal with the scale and nature of the subject threat scenarios.

Figure 4-6: Graphic Representation of Thailand's Demand and Supply Balance

THAILAND	Significant Flooding	Weather Extremes	Terrorist Attack	Pandemic Influenza	Cyber Attack
Training					
Equipment					
Personnel					
Information					
C & D					
Organisation					
Infrastructure					
Logistics					
Authority					
Responsibility					
Structure					
Resources					
A v E					
S & S					

Key:

Green: Supply and demand in reasonable balance; DLODs mainly covered.

Orange: some cause for concern between supply and demand balance; some DLODs out of kilter.

Red: Significant variance between supply and demand; DLODs deficient and in need of addressing.

18. **Subjective Analysis**.

a. **Significant Flooding and Weather Extremes**. Like most of South East Asia, Thailand suffers from a wide variety of natural hazards predominantly from flooding and weather extremes. As shown in Chapter 2, the National Disaster Risk Management Plan (2015) lists a significant number but places flooding at the top of the list. The tsunami of 2004 is, sadly, a prime example of the sheer scale of an event that can occur, but there are far more regular and disruptive floods nearly every year. Thailand benefits from

having a large military for the size of its population and its well dispersed across the country meaning it can be brought into action quickly. Authorities are reasonably well defined although not entirely clear, and there seems to be some stove-piping between the single-Services. Nevertheless, the basic tenants of responsibility seem to be well understood. Where Thailand perhaps fairs less well is the equipment and resources available for use at any given moment. The nation's strength appears to lie in the response phase with some notable effort being put into preparation. Mitigation and, recovery in particular seem to be less of a focus.

b. **Catastrophic Terrorist Attack**. Thailand has yet to experience a large-scale terrorist attack although many would deem it only a matter of time. The country has gained much experience from the ongoing insurgency in the Deep South of the country, which spills over into other areas fairly regularly. Thankfully, outwith that geographic region, attacks have been comparatively limited in their scale and design. Authorities and responsibilities have been assigned to a number of specialist units who would deal with most incidents and they are heavily involved in the preparation phase. More work is needed to mitigate threats and an attendant increase in resources, training, concepts & doctrine and relevant logistics.

c. **Pandemic Influenza**. Given prevailing climatic conditions the potential for a large-scale pandemic influenza is significant. Thailand is unique amongst the three subject countries in that it recognises the potential for such an epidemic to occur amongst a range of flora and fauna and has, as part of its mitigation and preparation phases, considered the nature of the potential impact. Unfortunately, it is probably the least well placed to deal with such an outbreak however, especially in the less developed areas of the country. The Thai military has a large number of personnel who could be particularly useful in dealing with the indirect challenges of a pandemic influenza. They are, however, less well equipped than their compatriots in the other 2 countries meaning they may be less able to deliver an effect during the response phase. That said, they are perhaps more experienced at working with very limited resources so may turn out to be the best suited.

d. **Cyber Attack**. Thailand is less well prepared to deal with a significant cyber attack than the other two countries although it may prove more resilient in terms of dealing with the impact. A large part of the population is less reliant on modern technology and thus will probably recover more quickly. The military capability to deal with a significant attack is not obvious and it has not proved possible to find underlying information in this sensitive area making even a subjective assessment difficult. Concepts & Doctrine, authorities and a personnel skill level are not easy to identify and thus it is presumed they are scarce.

Chapter 5
Conclusion and Recommendations

"To succeed, jump as quickly at opportunities as you do to conclusions."[1]

"Enough research will tend to support your conclusions."[2]

"I don't want happy-face conclusions. I want the truth."[3]

Conclusion

1. **Context**. No nation on earth can afford to raise, equip and maintain an armed force purely for show; they are too expensive. Their purpose, therefore, must me to protect and secure the country and the people they serve but precisely what they do and how they do it will vary by State. It is axiomatic that armed forces will be assigned tasks requiring the application of violence but most developed nations also ask their military to perform non-violent tasks including the conduct of Disaster Relief Operations. In order to achieve success there must be a corresponding and proportional relationship between the tasks assigned and the resources provided to achieve them. Such a transactional relationship should be identifiable and assessable otherwise the military are being set up for failure at the very moment that they are needed most.

2. **Research Objectives**. The paper set out to address 3 primary questions in order to consider if the relationship between assigned tasks and allocated resources is in balance for 3 particular countries, namely the UK, the USA and Thailand. Those countries were selected as the benchmark for consideration based upon their scale, the author's experience and because they all use their armed forces regularly on DR Operations. The questions were:

a. What is the nature and scale of the most likely domestic DR Operation 'threat scenarios' in Thailand, the United Kingdom and the United States?

---

[1] Benjamin Franklin, American Politician, 1780.

[2] Arthur Bloch, Author, 2012.

[3] Elizabeth Warren, US Senator, 2014.

b. What have/will the armed forces of each country be asked to do?

c. To what extent can the armed forces of each country meet the requirement?

3. **Relevance**. The paper, and the 3 specific questions are of importance because whilst the number of crises seems, anecdotally at least, to be increasing, so too are the demands being placed on military forces and their attendant budgets. The combination of competing factors makes it critical to ensure that what a government expects their military forces to underwrite is realistic, achievable and relevant. By addressing this notion, the paper goes some way towards conducting an audit of capability.

4. **Methodology**. The initial task, in Chapter 2, was to benchmark the potential crisis scenarios facing each country in terms of their nature and scale. Through open source literature and documents produced by national bodies is was possible to identify a representative selection of the most likely, larger scale scenarios, common to all 3 countries. National risk registers were particularly relevant in this regard. Having characterised the common threat scenarios the next undertaking was to confirm, in Chapter 3, what each armed force had been tasked to do through the identification of national Ends, Ways and Means. Chapter 4 then subjectively addressed the ability of the armed forces to achieve their tasks using Defence Lines of Development, the Disaster Management Cycle and Crisis Management Considerations for the Military as the basis for classification.

5. **Limitations**. The sheer size of the task became increasingly apparent during the research phase and the difficulty in accessing useable data, either for reasons of language or, more often, classification, meant that an objective assessment was unachievable. For similar reasons, it was not possible to accurately plot a timeframe over which the assessment might prove valid. The paper also specifically delimited itself not to consider the conduct of DR operations overseas, which would place yet another burden on the armed forces.

6. **Results**. The following results were discerned from the research.

a. **Question 1 – The nature and scale of the most likely threat scenarios.** The first discovery from the research was the similarity between many of the crisis scenarios but also some notable differences. The former is, perhaps, not unexpected given that 'there is no new thing under the sun'[4] whereas the latter gives rise for some concern.

1) All three nations had similar definitions for what constituted a crisis and also how they classified the seriousness and 'level' (national, regional, local), which drove the decision on how to respond.

2) The UK saw the likelihood of a major cyber attack as being high yet thought the relative impact would be low – this seems at odds with many recent events. The USA also recognises the threat but, as with its whole system, did not seem to assign any unclassified indices to the potential scale of risk or likelihood or occurrence making it impossible to codify. It was possible to find detail on subjective ranks and numeric weight pertaining to Thailand, however the risk of a cyber attack did not feature in the list of possible crises – an area that must be addressed.

3) All nations recognise the potential impact of a pandemic influenza with the UK assigning it the second highest likelihood, after a catastrophic terrorist attack. The USA placed it second after natural hazards, which is understandable given the fact that they suffer from some form of hazard every day. Thailand placed it further down the order but formally recognised more potential forms of an outbreak across flora and fauna thus more accurately articulating the risk in the process.

4) Thailand understandably concentrated its effort on various forms of natural disaster but seemed far less concerned about the risk of a significant terrorist crisis – an area that should be addressed.

[4] The Holy Bible, King James Version, Ecclesiastes 1:9, verse 9.

b. **Question 2 – What have/will the armed forces of each country be asked to do?** All three nations have a well-defined mechanism to translate national interest into military tasks – an Ends, Ways and Means mechanism.

1) The UK mechanism is very clearly defined in law but also enables a 'fast-track' override system if required to enable rapid deployment of forces. Constitutionally it was less inclined to ask the military to step in to meet new requirements until very late in the process and then it was usually driven by political motives. It could learn lessons from the US system, forged on the disaster of the response to Hurricane Katrina and who are now much more likely to engage early and ask questions later.

2) If the UK approach is too late, the US system is overly bureaucratic held back by, in the views of many, legacy laws written for a bygone era. The amount of time spent discussing rules and procedures under Title 10 and Title 32 could be much better spent dealing with an incident. That said, the existence of a full-time DR Operations Headquarters provides a clear benefit over the other two countries.

3) Thailand enjoys the benefit of a clearly articulated Disaster Risk Management Strategy but there appears, prima facie, to be some disconnect between it and the tasks assigned to the military. It maybe that they are indeed enshrined in a more helpful way but they were not discernible to the author. The Disaster Risk Management Mechanism seemed a particular strength but whether it actually worked in practice was less obvious. Finally, tasks seemed very much focussed on activity following an incident rather than trying to get out in front.

c. **Question 3 – To what extent can the armed forces of each country meet the requirement?** It was a source of significant frustration to the author that he was unable to provide a more empirical assessment of this question. Nevertheless, the research provided some useful subjective outputs.

1) **The UK**. It was clear that the UK enjoys the benefit of a well thought through system that shows a demonstrable path from National interest and likely threat scenario through to the tasks it has placed upon its military forces. Its greatest challenge, however, is that the force is now so small that, stand fast niche and specialist capabilities, it will not be in a position to underwrite large or significant events. It is, perhaps, best prepared for a significant terrorist attack but at its weakest for a pandemic and cyber attack. The former is, again, due to a lack of assets, the latter is similar but also is a new area for which concepts and doctrine are evolving rapidly. An increased willingness by politicians to lean into the problem would allow the military to become more involved earlier in the Crisis Management Cycle but, as the military will also point out, it is not their primary purpose for existence.

2) **The USA**. Like the UK, the USA military is reasonably well prepared to deal with its assigned tasks relating to significant flooding and weather extremes. It also enjoys, if that is not too much of a positive statement, the opportunity to test itself regularly due to the near daily occurrence of such events somewhere in the country. Scale is both a blessing and a curse in that military assets are well dispersed, however, as a result, they have a long way to move when needed, which increases the financial costs involved in sending them. Where the US suffers most is, arguably, in their potential to deal with a major pandemic influenza outbreak due to the sheer quantity of people that could be affected. They are the best trained and equipped of the three nations when it comes to dealing with a major cyber attack. The tasks and responsibilities that would fall to the military, however, need better articulation and clearer delineation.

3) **Thailand**. Of the three subject countries, Thailand is the least wealthy yet is, arguable, most likely to suffer from truly devastating flooding or weather extremes. As a result, the tasking mechanism needs to be the most responsive and resilient; currently it is not. A truly joint command and control mechanism would improve the situation through all phases of the Crisis Management Cycle and enable

better advice to be provided to political decision makers. The potential response to a catastrophic terrorist incident is considered mixed, largely dependent on where it takes places. A pandemic response could well be similar although as it is likely to endure over a longer time, resources will inevitably be stretched further, possibly beyond breaking point. Thailand's weakest area is considered to be a response to a cyber attack, which could bring the country to a standstill quite quickly. Almost ironically, however, Thailand may be the most resilient to such attack on the grounds that much of its population is seemingly less dependent on cyber related systems. As the country moves towards Thailand 4.0 it must, however, build in greater redundancy to prevent and respond to such attacks.

7. **Implications**. It is clear from the research conducted that the available information has precluded a detailed analysis of each country's situation. Much more detail is needed to make certain that the Ends, Ways and Means will deliver the requirement. Supply and demand are not, and probably never will be, in equilibrium – the search for the Holy Grail continues. The paper has demonstrated that each nation takes the various threats very seriously and are doing their level best to prepare for 'the worst', however, the situation changes rapidly and the military will always struggle to keep up to date.

8. **Further Research**. An opportunity exists for each nation to review the information contained in this paper and, using classified information not available to the author, review their particular circumstances – they owe it to their population to be as ready as they can for what is about to come.

Recommendations

9. It is recommended that:

a. Each nation reviews the scenarios more regularly to make certain they are germane and that their attendant plans are kept up to date and meet evolving threats – especially in the cyber domain.

b. The UK better recognises the need to get the military involved earlier in the process rather than tasking too little, too late.

c. The UK increases the manpower numbers of the military in order to deal with expected scenarios.

d. The US should more clearly define and delineate the military tasks, through all phases of the Crisis Management Cycle, appertaining to cyber attacks.

e. Thailand must consider the impact of cyber attacks in more detail and make a corresponding plan to deal with them.

f. Thailand must consider the wider ramifications of a significant terrorist attack and make a corresponding plan to deal with them.

g. Thailand should more clearly define its tasking mechanism and support it with appropriate resources. Incident command and control should be simplified.

h. As the country gets closer to delivering Thailand 4.0 the Thai military must be more proactive in preparing for cyber attacks. Only in this way will it be able to respond and recover in an appropriate timeframe.

Bibliography

Books

Army Doctrine Publication. Operations. Swindon, UK : British Army, 2010.

ASEAN-UN Joint Strategic Plan of Action on Disaster Management. Phnom Penh : ASEAN-UN, 2015.

Cabinet Office. National Risk Register. London : The Cabinet Office, 2008.

Cabinet Office. National Risk Register of Civil Emergencies. London : The Cabinet Office, 2015.

Center for Excellence in Disaster Management and Humanitarian Assistance (CFE-DMHA). Thailand Disaster Management Reference Handbook. Hawaii : CFE-DMHA, 2015.

Directorate of Force Development. AGILE WARRIOR 12 Summary of Insights. Andover : British Army, 2013.

HFA. Implementing the Hyogo Framework for Action in Europe: Advances and Challenges 2005 – 2015. Geneva : HFA, 2004.

Joint Doctrine Publication 02. Operations in the UK: The Defence Contribution to Resilience (2nd Edition). Swindon : The Development, Concepts and Doctrine Centre, 2007.

Joint Doctrine Publication 02. UK Operations: The Defence Contribution to Resilience and Security (3rd Edition). Swindon : The Development, Concepts and Doctrine Centre, 2017.

Joint Doctrine Publication 02. Operations in the UK: A Guide for Civil Responders (2nd Edition) - Addendum. Swindon : The Development, Concepts and Doctrine Centre, 2010.

Joint Publication 3-28. Defense Support of Civil Authorities. Washington

DC : Department of the Joint Chiefs of Staff, 2013.

Kneisl, C.R. and Riley, E. Crisis Intervention. In Wilson, H. and Kneisl, C.R. Psychiatric Nursing (5th ed., pp. 711-731). Menlo Park, California, 1996.

Library of Congress. History of the Unified Command Plan 1946 – 2012. Washington D.C. : Library of Congress Cataloguing-in-Publication Data, 2013.

Library of Congress. Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress. Washington D.C. : Library of Congress Congressional Research Service, 2011.

Ministry of Finance, Royal Thai Government and The World Bank. Thailand Flooding 2554: Rapid Assessment for Resilient Recovery and Reconstruction Planning. Bangkok : Royal Thai Government, 2012.

Pezard, Stephanie; Thaler, David E; Grill, Beth; Klein, Ariel; Robson, Sean. The Centre for Excellence in Disaster Management and Humanitarian Assistance (CFE-DMHA): An Assessment of Roles and Missions. Santa Monica : Rand Corporation, 2016.

National Disaster Prevention and Mitigation Committee. The National Disaster Risk Management Plan. Bangkok: Deputy Prime Minister, 2015.

National Economic and Social Development Board. The Eleventh National Economic and Social Development Plan (2012 – 2016). Bangkok : Office of the Prime Minister, 2011.

Rerngnirunsathit, Phatsita. Thailand Country Profiles 2011. Bangkok: Department of Disaster Prevention and Mitigation, 2012.

United Nations. Global Assessment Report on Disaster Risk Reduction 2015. New York, 2016.

United Nations. Sendai Framework for Disaster Risk Reduction 2015 – 2030. New York, 2014.

US Department of Homeland Security. National Response Framework (Third Edition). Washington D.C. : Homeland Security, 2016.

US Department of Homeland Security. Overview of the National Planning Frameworks. Washington D.C. : Homeland Security, 2016.

Venette, S.J. Risk Communication in a High Reliability Organization. Ann Arbor, Michigan, 2003.

Vigneri, Marcella and Lombardini, Simone. Resilience in Thailand: Impact Evaluation of the Climate Change Community-based Adaptation Model for Food Security Project. Oxford : Oxfam GB, 2015.

Journals and Newspapers

Cabinet Office. UK Central Government Arrangements for Responding to an emergency – An Overview. London : The Cabinet Office, 2010.

Department of Disaster, Prevention and Mitigation. Roles and Responsibilities of Department of Disaster Prevention and Mitigation. Ministry of Interior, 2015.

Department of Disaster, Prevention and Mitigation. Thailand's National Disaster Prevention and Mitigation Plan. Ministry of Interior, 2015.

Department of Health. Health Emergency Preparedness, Resilience and Response from April 2013. London : Department of Health, 2012.

Khan, Himayatullah; Vasilescu, Laura Giurca; Khan, Asmatullah. Disaster Management Cycle – A Theoretical Approach. Romania : Management and Marketing Journal Vol 6, Issue 1, Pages 43-50, 2008.

Home Office. Have you got what it takes? Police, risk and resilience. The Home Office, 2012.

Sawada, Yasuyuki and Zen, Fauziah. Disaster Management in ASEAN. Jakarta, Indonesia : Economic Research Institute for ASEAN and East Asia, 2014.

Seeger, M.W., Sellnow, T.L., Ulmer, R.R. Communication, Organisation and Crisis. Annals of the International Communication Association Vol 21, Issue , 1998.

Electronic Data Base

2015 to 2020 Government Policy: Military Aid to the Civil Authorities for Activities in the UK. (2016). Gov.uk, https://www.gov.uk/government/publications/2015-to-2020-government-policy-military-aid-to-the-civil-authorities-for-activities-in-the-uk/2015-to-2020-government-policy-military-aid-to-the-civil-authorities-for-activities-in-the-uk

Coombs, Timothy W. Crisis Management and Communications. http://www.instituteforpr.org/crisis-management-and-communications/ 2007.

Federal Emergency Management Agency : National Planning Frameworks Update: What's New. Accessed 29 Jan 17. http://www.fema.gov/national-planning-frameworks

Federal Emergency Management Agency : National Response Framework (Third Edition) Information Sheet. Accessed 29 Jan 17. http://www.fema.gov/national-response-framework

Federal Emergency Management Agency : Presidential Policy Directive 8 / PPD-8 National Preparedness. Accessed 12 Apr 17. http://www.fema.gov/pp8

Federal Emergency Management Agency : Strategic Plan. 2014. https://www.fema.gov/fema-strategic-plan

Global Security.org: National Planning Scenarios: Executive Summaries. http://www.globalsecurity.org/security/library/report/2004/hsc-planning-scenarios-jul04.htm

Management Study Guide: Types of Crisis. Guide http://www.managementstudyguide.com/types-of-crisis.htm.

PreventionWeb – Thailand: National Progress Report on the

Implementation of the Hyogo Framework for Action (2013-2015). 2014. http://www.preventionweb.net/english/professional/policies/v.php?id=41674

PreventionWeb – UK: National Progress Report on the Implementation of the Hyogo Framework for Action (2013-2015). 2014. http://www.preventionweb.net/english/hyogo/progress/reports/v.php?id=31804&pid:223

PreventionWeb – USA: National Progress Report on the Implementation of the Hyogo Framework for Action (2013-2015). 2014. http://www.preventionweb.net/english/hyogo/progress/reports/index.php?o=pol_year&o2=DESC&ps=50&hid=0&cid=185&x=10&y=8

Risk Assessment: How the Risk of Emergencies in the UK is Assessed. (2013). Gov.uk, https://www.gov.uk/guidance/risk-assessment-how-the-risk-of-emergencies-in-the-uk-is-assessed

Risk Management Agency : The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation. https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf

Retail Quality Audits (RQA) Crisis control Newsletter Vol U0110 Issue 1. https://www.rqa-inc.com/newsletters/Catlin_US_U0110.pdf

Structural Policy Country Notes: Thailand (2014). http://dx.doi.org/10.1787/saeo-2014-en.

Warfield, Corina. The Disaster Management Cycle. https://www.gdrc.org/uem/disasters/1-dm_cycle.html

Non-Published Documents

Chairman of the Joint Chiefs of Staff (USA). CBRNE Executive Order. 21 June 2011.

Chairman of the Joint Chiefs of Staff (USA). Defense Support of Civil Authorities (DSCA) Executive Order. 07 June 2013.

Chittmittrapap, Prof. Dr. Soottiporn. National Adaptation Planning and Actions in Thailand: The Watershed-Based Adaption To Climate Change Initiative. Presented in Japan, date unknown.

Dhiradhamrong, Maj Gen Srisaran Special Advisor, Ministry of Defence, Kingdom of Thailand. Armed Forces and Disaster Management: Experience Sharing in Coordinating Humanitarian Assistance and Disaster Relief. Presented at a Workshop on Thailand-initiated Concept Paper on: Humanitarian Assistance and Disaster Relief, 2009.

Iglesias, Gabrielle. Lessons on Resilience from the 2011 Central Thailand Floods. Presented by Asian Disaster Preparedness Center, date unknown.

Paksuchon, Amornthip (Visiting Researcher). Thailand on Disaster Risk Management 2011. Department of Disaster Prevention and Mitigation, Ministry of Interior, 2011.

Termpittayapaisith, Arkhom (Secretary-General, Office of the National Economic and Social Development Board). The Eleventh National Economic and Social Development Plan. Presentation to the British Chamber of Commerce Thailand, Bangkok, 2 October 2014.

Royal Thai Army. The Roles that Land Forces Should Play in CIMIC/Interagency Cooperation Building in DRO. Thailand, 2010.

Sreechumpol, Captain RTN Pisutsak. ASEAN Humanitarian and Disaster Relief Exercise. 2013

The National Military Strategy of the United States of America - 2015. http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf

World Conference on Disaster Reduction Report. Hyogo Framework for Action 2005 – 2015. Presented at the World Conference on Disaster Reduction : Kobe, Hyogo, Japan, 2005.

Biography

Name:	Colonel Roger Lewis
Date of Birth:	11 February 1965
Educational Background:	Masters of Military Studies, Cranfield University, United Kingdom
Military Courses:	British Army Junior Division, Staff College, Warminster, United Kingdom
	Military Technology Course, Royal Military College, Shrivenham, United Kingdom
	Advanced Command and Staff Course, Joint Services Command and Staff College, Bracknell, United Kingdom
	Directing Staff, Advanced Command and Staff Course, Joint Services Command and Staff College, Watchfield, United Kingdom
Military Experience:	Royal Military Academy, Sandhurst
	Troop Commander at Regimental Duty and Staff Officer, Grade 3
	Staff Officer, Grade 2, HQ United Nations Protection Force, Bosnia
	Manager, United Nations Mine Action Centre Mostar, Bosnia
	Deputy Chief of Staff, HQ 19 Mechanzied Brigade

Chief of Staff, HQ British Forces, Kosovo

Officer Commanding, 3 Armoured Engineer Squadron

Officer Commanding Engineer Squadron, North, Kosovo

Officer Commanding Engineer Squadron, Basra, Iraq

Military Assistant to the Deputy Supreme Commander (NATO) Allied Command Transformation

Commanding Officer, 38 Engineer Regiment

The Joint Force Engineer, Helmand, Afghanistan

Assistant Director, Force Development, Army Headquarters

British Liaison Officer to United States Northern Command and North American Aerospace Command (NORAD)

Current Position: British Defence Attaché, Bangkok, Thailand

SUMMARY

Field Strategy

Title: A study of the capability of the Armed Forces of Thailand, the United Kingdom and the United States of America to deliver domestic Disaster Relief Operations as a distinct Military task.

Name: Colonel Roger Lewis (*Tommy*) **Course** NDC **Class 59**

Position: Defence Attaché, British Embassy

Background and importance of the problem

1. The language will vary, the tone differ and the rhetoric fluctuate but for most nation states the primary purpose of raising, equipping and maintaining an armed force is to protect and defend itself against threats to its safety and very existence. Whether those threats are violent, virtual or environmental, the government-of-the-day must match the demands it places on its armed forces with the resources it allocates to achieve them. Demand will always outstrip supply and thus an amount of prioritisation will be required.

2. The challenge facing both central government and the Armed Forces themselves is how to balance the competing demands they face in such a way to ensure they can achieve an acceptable measure of success across a broad array of requirements. There is no 'one-size-fits-all' solution, no 'correct' answer to the question "What will we need, and when will we need it?"

3. In order to consider the relationship between domestic Disaster Relief Operations (DR Operations) and the role of the military three countries have been selected on the basis of their repeated and recent use in DR Operations; their scale; and the author's existing knowledge. The countries are: Thailand, the United Kingdom and the United States of America. All three militaries have a standing remit to conduct domestic DR Operations when so tasked but their scale, authority and priorities vary.

4. Each of the three subject countries faces a range of 'threat scenarios' against which they need to plan and organise. Even a cursory examination of the potential challenges, for example: environmental (e.g. pandemic), geographical (e.g. flood), man-made (e.g. chemical leak), demonstrates the significant complexity involved in preparing for such eventualities. Understanding the nature and scale of these threats is paramount however, for without it the Armed Forces may be expected to achieve unrealistic levels of support and national planning assumptions will lack rigour, allowing capability gaps to develop.

Objectives of the research

5. The purpose of this research paper is to consider the most likely domestic DR Operations demand signal that will be placed upon the armed forces of Thailand, the UK and the USA and, using a capability development framework and Disaster Management Cycle, analyse their ability to meet it. Put simply: what has the military been asked to do and can they do it? The paper addresses 3 primary questions: a) What is the nature and scale of the most likely domestic DR Operation 'threat scenarios?' b) What have/will the armed forces of each country be asked to do? c) To what extent can the armed forces of each country meet the requirement?

Scope of the research

6. The risk inherent in this research project was the sheer size and scope of potential disasters that could affect each country and the inability to accurately predict what will actually happen. As the primary aim was to assess the logic train each armed force is following the threat scenario research was confined to a manageable proportion designed to identify the most likely, rather than the most dangerous or apocalyptic situations. In addition, as some of the detail required to conduct this research is classified and therefore unpublishable, the research was confined to publically available sources.

Methodology[1]

[1] See Figure 1 in the paper for an explanation of the numbered Steps

7. The primary questions were analysed as follows: Question 1 benchmarked the potential threats in terms of their nature and scale relative to the country (Step 1.1). A representative selection of the most likely, larger scale scenarios, common to all 3 countries was then identified (Step 1.2). Question 2 identified what the armed forces have been tasked to do, and the logic train behind that direction (Ends, ways and means). (Step 2.2) It sought to identify in what way the assigned Military Tasks contribute to, and meet the respective National Strategy, and what comparisons can be drawn between the 3 countries (Step 2.2). Having extracted the defined military tasks the ability of each armed force to meet the requirement was assessed against the 5 threat scenarios through the prism of the Defence Lines of Development and Disaster Management System (Step 3.1). The paper was then drawn together at Step 4, and made recommendations that can be used to update each nation's approach to Humanitarian Assistance and Disaster Relief Operations.

Results

9. **Question 1 – The nature and scale of the most likely threat scenarios.** All three countries face a range of threat scenarios that manifest on a recurring but irregular schedule. For the purpose of this paper however, it is necessary to identify common themes that each country needs to plan against and using the most likely, rather than the most catastrophic, events is a logical approach for the purpose of comparison. For the UK, the most likely scenarios, weighted for severity, were: 1) Catastrophic Terrorist attack; 2) A pandemic influenza; 3) Weather extremes; 4) Widespread electricity failure; 5) Flooding (inland or coastal); 6) Animal diseases (such as Foot and Mouth); 7) Drought; 8) Disruptive industrial action. For the USA it was a little harder to discern as they do not provide unclassified data on likelihood, however, based on the information provided it was assessed, subjectively, that the most likely scenarios are: 1) Natural hazards, specifically including hurricanes, flooding and wildfires; 2) A pandemic influenza; 3) Man-made hazards; 4) Terrorist attack; 5) Cyber-attack (which could include the initiation of a widespread electricity failure or financial meltdown). For Thailand, it was assessed that the most likely scenarios are: 1) Flooding (including from tsunami); 2) Landslides and/or mudflow; 3) Windstorms; 4) Droughts; 5) Civil unrest and/or refugee influx; 6) Epidemic (including a pandemic influenza).

10. **Down-selected Common Scenarios**. The scenarios common to all three countries, are 1) Flooding (regardless of cause or location); 2) Weather extreme effects (regardless of cause); 3) Terrorist Attack (of a conventional style only as the impact of the use of a WMD is so significant that it automatically will become international and require a global response). 4) Pandemic influenza (even though the same terminology is not used by Thailand). 5) Cyber Attack is only mentioned by the US, but undoubtedly is applicable to all given that it recognises no borders or boundaries.

11. All three nations had similar definitions for what constituted a crisis and also how they classified the seriousness and 'level' (national, regional, local), which drove the decision on how to respond. The UK saw the likelihood of a major cyber attack as being high yet thought the relative impact would be low – this seems at odds with many recent events. The USA also recognises the threat but, as with its whole system, did not seem to assign any unclassified indices to the potential scale of risk or likelihood of occurrence making it impossible to codify. It was possible to find detail on subjective ranks and numeric weight pertaining to Thailand however the risk of a cyber attack did not feature in possible crises.

12. All nations recognise the potential impact of a pandemic influenza with the UK assigning it the second highest likelihood after a catastrophic terrorist attack. The USA placed it second after natural hazards, which is understandable given the fact that they suffer from some form of hazard every day. Thailand placed it further down the order but formally recognised more potential forms across flora and fauna than the other two nations more accurately articulating the risk in the process. Thailand understandably concentrated its efforts on various forms of natural disaster but seemed far less concerned about the risk of a significant terrorist crisis – an area that should be addressed.

13. **Question 2 – What have/will the armed forces of each country be asked to do?** All three nations have a well-defined mechanism to translate national interest into military tasks – an Ends, Ways and Means mechanism.

a. The UK mechanism is very clearly defined in law but also enables a 'fast-track' override system if required to enable rapid deployment of forces. Constitutionally it was less inclined to

ask the military to step in to meet new requirements until very late in the process and then it was usually driven by political motives. It could learn lessons from the US system, forged on the disaster of the response to Hurricane Katrina, but now much more likely to engage early and ask questions later.

b. If the UK approach is too late, the US system is overly bureaucratic and is held back by, in the views of many, legacy laws written for a bygone era. The amount of time spent discussing rules and procedures under Title 10 and Title 32 could be much better spent dealing with an incident. That said, the existence of a full-time DR Operations Headquarters provides a clear benefit over the other two countries.

c. Thailand enjoys the benefit of a clearly articulated Disaster Risk Management Strategy but there appears, prima facie, to be some disconnect between it and the tasks assigned to the military. It maybe that they are indeed enshrined in a more helpful way but they were not discernible to the author. The Disaster Risk Management Mechanism seemed a particular strength but whether it actually worked in practice was less obvious. Finally, tasks seemed very much focussed on activity following an incident rather than trying to get out in front.

14. **Question 3 – To what extent can the armed forces of each country meet the requirement?** It was a source of significant frustration to the author that he was unable to provide a more empirical assessment nevertheless, the research provided some useful subjective outputs.

a. **The UK**. It was clear that the UK enjoys the benefit of a well thought through system with a demonstrable path from National interest and likely threat scenario, through to the tasks it has placed upon its military forces. Its greatest challenge, however, is that the force is now so small that, apart from niche and specialist capabilities, it will not be in a position to underwrite large or significant events. It is, perhaps, best prepared for a significant terrorist attack but at its weakest for a pandemic and cyber attack. The former is, again, due to a lack of assets, the latter is similar but also is a new area for which concepts and doctrine are evolving rapidly. An increased willingness by politicians to

lean into the problem would allow the military to become more involved earlier in the Crisis Management Cycle but, as the military will also point out, it is not their primary purpose for existence. Figure 4-4 sets out a subjective view of how well placed the UK military is to deal with the scale and nature of the subject threat scenarios.

Figure 4-4: Graphic Representation of UK's Demand & Supply Balance[2]

UK	Significant Flooding	Weather Extremes	Terrorist Attack	Pandemic Influenza	Cyber Attack
Training					
Equipment					
Personnel					
Information					
C & D					
Organisation					
Infrastructure					
Logistics					
Authority					
Responsibility					
Structure					
Resources					
A v E					
S & S					

b. **The USA**. The USA military is reasonably well prepared to deal with its assigned tasks relating to significant flooding and weather extremes. It also gets the opportunity to tests itself regularly due to the near daily occurrence of such events somewhere in the country. Scale is both a blessing and a curse in that military assets are well dispersed but, as a result, they have a long way to move when needed, which increases the costs involved in sending them. Where the US suffers most is, arguably, in their

[2] **Key**:

Green: Supply and demand in reasonable balance; DLODs mainly covered.

Orange: some cause for concern between supply and demand balance; some DLODs out of kilter.

Red: Significant variance between supply and demand; DLODs deficient and in need of addressing.

potential to deal with a major pandemic influenza outbreak due to the sheer quantity of people that could be affected. They are the best trained and equipped of the three nations when it comes to dealing with a major cyber attack. Figure 4-5 sets out a subjective view of how well placed the US military is to deal with the scale and nature of the subject threat scenarios.

Figure 4-5: Graphic Representation of USA's Demand & Supply Balance

USA	Significant Flooding	Weather Extremes	Terrorist Attack	Pandemic Influenza	Cyber Attack
Training					
Equipment					
Personnel					
Information					
C & D					
Organisation					
Infrastructure					
Logistics					
Authority					
Responsibility					
Structure					
Resources					
A v E					
S & S					

c. **Thailand**. Thailand is the least wealthy country yet is, arguably, most likely to suffer from truly devastating flooding or weather extremes. As a result, the tasking mechanism needs to be the most responsive and resilient; currently it is not. A truly joint command and control mechanism would improve the situation through all phases of the Crisis Management Cycle and enable better advice to be provided to political decision makers. The potential response to a catastrophic terrorist incident is considered mixed largely dependent on where it takes places. A pandemic response could well be similar although, as it is likely to endure over a longer time, resources will inevitably be stretched further, possibly beyond breaking point. Thailand's weakest area is considered to be a response to a cyber attack, which could bring the country to a standstill quite quickly. Almost ironically, however, Thailand may be the most resilient to such attack on the

grounds that it is seemingly less dependent on such systems. As the country moves towards Thailand 4.0 it must, however, build in greater redundancy to prevent and respond to such attacks. Figure 4-6 sets out a subjective view of how well placed the Thai military is to deal with the scale and nature of the subject threat scenarios.

Figure 4-6: Graphic Representation of Thailand's Demand & Supply Balance

THAILAND	Significant Flooding	Weather Extremes	Terrorist Attack	Pandemic Influenza	Cyber Attack
Training					
Equipment					
Personnel					
Information					
C & D					
Organisation					
Infrastructure					
Logistics					
Authority					
Responsibility					
Structure					
Resources					
A v E					
S & S					

Recommendations

15. It is recommended that: 1) Each nation reviews the scenarios more regularly to make certain they are germane and that their attendant plans are kept up to date and meet evolving threats – especially in the cyber domain. 2) The UK better recognises the need to get the military involved earlier in the process rather than tasking too little, too late; there is an increase in military manpower numbers in order to deal with the expected scenarios. 3) The US should more clearly define and delineate the military tasks, through all phases of the Crisis Management Cycle, appertaining to cyber attacks. 4) Thailand must consider the wider ramifications of a significant terrorist attack and make a corresponding plan to deal with them; should more clearly define its tasking mechanism and support it with appropriate resources. Incident command and control should be simplified; As the country gets closer to delivering Thailand 4.0 the Thai military must be more proactive in preparing for cyber

attacks. Only in this way will it be able to respond and recover in an appropriate timeframe.