The securitisation of the United Kingdom’s maritime infrastructure during the ‘war on terror’

James A. Malcolm

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Politics and International Studies

University of Warwick, Department of Politics and International Studies

September 2011
Table of Contents

List of Figures, Tables and Images................................................................. iii
Acknowledgements...................................................................................... iv
Declaration.................................................................................................. v
Abstract...................................................................................................... vi
List of Abbreviations................................................................................... vii

Introduction - Counter-terrorism and the United Kingdom’s maritime infrastructure......................................................... 1

The study..................................................................................................... 1
Contribution................................................................................................. 5
Central argument......................................................................................... 7
Thesis structure......................................................................................... 10

Chapter One – Reorienting towards the ‘post-securitised environment’: utilising the Copenhagen School’s securitisation theory as an analytical framework................................................................. 14

Introduction............................................................................................... 14
Contextualising the Copenhagen School’s securitisation theory............... 17
The Copenhagen School............................................................................. 28
The Copenhagen School’s securitisation theory......................................... 32
  The speech act....................................................................................... 34
  A securitising move.............................................................................. 35
  Securitisation – a successful securitising move..................................... 38
  Macrosecuritisation and security constellations................................... 40
Reorienting securitisation theory towards the ‘post-securitised environment’ .......................................................... 43
The Copenhagen School’s securitisation theory and its critics.................. 51
The case study – the securitisation of the UK’s maritime infrastructure..... 60
Research methods and sources................................................................. 70
Conclusion.................................................................................................. 74

Chapter Two – Contextualising the case study: the ‘war on terror’ and the emergence of the ISPS code................................................................. 78

Introduction............................................................................................... 78
The construction of the ‘war on terror’ discourse of counter-terrorism........ 82
The ‘war on terror’ in the UK................................................................. 90
The securitisation of UK maritime infrastructure during the ‘war on terror’.... 107
Conclusion.                                                                                                      126
| Chapter Three – From introduction to institutionalisation: the next phase in implementation | 131 |
| Introduction | 131 |
| Resistance and reiteration – the stability of the ‘war on terror’ discourse | 135 |
| UK maritime infrastructure as a ‘site of securitisation’ | 144 |
| UK maritime infrastructure – the post-securitised environment | 150 |
| Legislation and regulations | 156 |
| Institutional changes and infrastructure developments | 164 |
| Working practices | 167 |
| Conclusion | 185 |

| Chapter Four – Beyond the ISPS code: securing UK maritime infrastructure after the London 2005 terrorist attacks | 192 |
| Introduction | 192 |
| Reflection and renewal – the ‘war on terror’ after the London 2005 terrorist attacks | 197 |
| UK maritime infrastructure as a ‘site of securitisation’ | 212 |
| UK maritime infrastructure – the post-securitised environment | 220 |
| Legislation and regulations | 224 |
| Institutional changes and infrastructure developments | 232 |
| Working practices | 241 |
| Conclusion | 247 |

| Chapter Five – Staying the course: securing UK maritime infrastructure after Blair | 255 |
| Introduction | 255 |
| New Prime Minister, little change – Gordon Brown and the ‘war on terror’ | 258 |
| UK maritime infrastructure as a ‘site of securitisation’ | 271 |
| UK maritime infrastructure – the post-securitised environment | 278 |
| Legislation and regulations | 280 |
| Institutional changes and infrastructure developments | 285 |
| Working practices | 295 |
| Conclusion | 306 |

| Conclusion – Continuity and change: the securitisation of UK maritime infrastructure during the ‘war on terror’ | 313 |
| The thesis’ argument | 313 |
| Key findings | 321 |
| Future research avenues | 341 |

| Appendix A – Interview Strategy | 346 |
| Appendix B – Project Kraken member survey | 348 |
| Bibliography | 353 |
Figures, Tables and Images

Figure 1 - The securitisation process................................................................. 49 & 322
Figure 2 - Terrorist Risk Factors from Shipping..............................................115
Figure 3 – The spatial dimension to securitisation..........................................334
Table 1 – The TRANSEC approach to compliance..........................................170
Image 1 – Security level sign...........................................................................173
Image 2 – Port security poster..........................................................................175
Image 3 – Port personnel search......................................................................181
Image 4 – Port vehicle search..........................................................................182
Image 5 – Port entry/exit point..........................................................................182
Image 6 – Big Mac...........................................................................................222
Image 7 - Project Kraken paraphernalia............................................................302
Image 8 – Coast Watch branding.....................................................................302
Image 9 – Project Kraken poster......................................................................305
Acknowledgements

Writing this PhD thesis has been a time consuming, yet rewarding experience. I have been very lucky to have had the opportunity to spend a number of years reading, thinking, discussing and writing about issues that interest me. I am particularly grateful to the Department of Politics and International Studies here at Warwick for having the faith in me to offer an ESRC scholarship. I also want to thank my PhD colleagues, too numerous to mention individually, for contributing towards building a friendly and supportive atmosphere in which research could take place. I wish to thank Matthew Watson for his support on a number of different occasions over the past four years, helping me to navigate various demands of the PhD process. To my supervisors I am eternally grateful. Matt McDonald helped me to find focus with my research, asking probing questions which effectively challenged me. Stuart Croft kept me on the straight and narrow, demonstrating reserves of patience I did not think were possible, constantly guiding me with insightful comments and encouragement. This thesis would not have been possible without the support of the staff at the International Maritime Organization archives. The IMO Knowledge Centre is a wonderful resource and one which I hope to return in the future. To all those anonymous individuals with responsibility for the security of UK maritime infrastructure, I thank you for welcoming me in to your places of work and for answering my very many questions. It is your insights which give the case study added depth. Most importantly I wish to thank my family for their love and support. You have been with me throughout the highs and lows of this journey and never stopped believing in me. This thesis is dedicated to you.

The responsibility for any errors of fact or judgement in the material contained in this thesis is ultimately my own.
Declaration

I declare that this thesis is entirely my own work other than where I have clearly indicated it is the work of others or as the result of collaboration.

Quotation from this thesis is permitted, provided that full acknowledgement is made. The thesis may not be reproduced in full or partially without the prior written consent of the author.

Sections 1.3, 1.4 and 1.6 of Chapter One draw loosely on material from ‘Securitisation: A Critical Analysis’ my dissertation submitted as part of my MA in International Politics (Research track) at the University of Manchester. This material, however, is exclusively my own work.

I confirm that this thesis has not been submitted for a degree at another university.
Abstract

This thesis examines counter-terrorism efforts in relation to the United Kingdom’s ports and harbours (its ‘maritime infrastructure’) in the context of the ‘war on terror’. To do this the thesis utilises the Copenhagen School’s securitisation theory as the analytical framework through which a case study, focusing on developments in a five year period between 1 July 2004 and 30 June 2009 and utilising the cases of Felixstowe, Holyhead and Tilbury, is undertaken. The thesis argues that UK maritime infrastructure was securitised in the context of the macrosecuritisation of the ‘civilised way of life’, which were in a mutually reinforcing relationship. By reorienting emphasis towards the ‘post-securitised environment’ and on to examining what securitisations ‘do’ in practice, the thesis subsequently demonstrates the substantial impact of securitisation on the management of UK maritime infrastructure. More specifically it argues that a counter-terrorism security response was evident which constantly evolved, was layered and increasingly expansive in scope and that had a series of prominent, recurring features. The thread which ran through this response was the pursuit of increased power in relation to UK maritime infrastructure, undertaken by the British state and port owners in particular. The thesis concludes by noting how the key findings of the case study progressively demonstrate a greater level of complexity to the securitisation of UK maritime infrastructure than can at first be apparent.
Abbreviations

ACPO – Association of Chief Police Officers
ACPO(TAM) – Association of Chief Police Officers (Terrorism and Allied Matters)
AEO - Authorised Economic Operator
AMSA – Aviation and Maritime Security Act, 1990
API - Advanced Passenger Information
ARGUS – Area Reinforcement Gained Using Scenarios
ATCSA – Anti-Terrorism, Crime and Security Act, 2001
BBC – British Broadcasting Corporation
BIA - Border and Immigration Agency
CAMPACC - Campaign Against Criminalising Communities
CBRN – Chemical, Biological, Radiological and Nuclear
CCTV – Closed-circuit Television
CNN – Cable News Network
CONTEST – The United Kingdom’s Strategy for Countering Terrorism
CPNI - Centre for the Protection of Critical National Infrastructure
CSI – Container Security Initiative
CSO – Company Security Officer
CTA – Common Travel Area
CTiU – Counter-Terrorism intelligence Unit
CTU – Counter-Terrorism Unit
DfT – Department for Transport
DSP - Designated Security Post
EMSA – European Maritime Safety Agency
EU – European Union
HMRC – Her Majesty’s Revenue and Customs

HPH – Hutchison Port Holdings

IDACS – Identification and Access Control System

ILO – International Labour Organization

IMO – International Maritime Organization

ISF – International Shipping Federation

ISPS code – International Ship and Port Facility Security code.

JBOC - Joint Borders Operational Centre

JIC – Joint Intelligence Committee

JTAC – Joint Intelligence Analysis Centre

KPI - Key Performance Indicator

KUP’s - Knowledge, Understanding and Proficiencies

MATRA – Multi-Agency Threat and Risk Analysis

MCA – Maritime Coastguard Agency

MET – Metropolitan Police

MI5 – Security Service

MoU – Memorandum of Understanding

NaCTSO - National Counter-Terrorism Security Office

NATO – North Atlantic Treaty Organization

NCPP - National Coordinator Ports Policing

NHS – National Health Service

OECD – Organisation for Economic Co-operation and Development

OSCT – Office for Security and Counter-Terrorism

PFSO – Port Facility Security Officer

PNMSS – Police National Maritime Security Strategy

PNR - Passenger Name Record

PSI – Proliferation Security Initiative
PSNI - Police Service of Northern Ireland

PSP – Port Security Plan

ReMIIT - Regional Maritime Information and Intelligence Teams

ReMRT - Regional Maritime Response Teams

RHIDES – Road Haulier IDENTification System


RO-RO – Roll-on/Roll-off

RYA – Royal Yachting Association

SAFE Port Act - Security and Accountability for Every (SAFE) Port Act, 2006

SB – Special Branch

SFI - Secure Freight Initiative

SIA – Single Intelligence Account

SO12 – Special Branch (MET)

SO13 – Anti-Terrorist Branch

SO15 – Counter Terrorist Command

SOLAS – International Convention for the Safety of Life at Sea, 1974

SSO – Ship Security Officer

SSP – Ship Security Plan


TA – Terrorism Act, 2000

TRANSEC – Transport Security and Contingencies Directorate

UK – United Kingdom

UKBA - United Kingdom Border Agency

US – United States of America

VBS- Vehicle Booking System

WCO - World Customs Organization
WECTU - Welsh Extremism and Counter-Terrorism Unit
Introduction

Counter-terrorism and the United Kingdom’s maritime infrastructure

(I.1) The study:

During December 2009 a television series entitled ‘Coastline Cops’ was aired in the United Kingdom (UK). It followed the working lives of a number of different British police officers operating in the maritime environment. On a number of occasions concern about international terrorism was evident as the series showed the work of a police maritime unit checking the hull of a cruise liner for explosive devices and intercepting an unknown pleasure craft off the coast from Southampton.¹ These were just small, public glimpses of the way in which counter-terrorism considerations had shaped day-to-day activities within the maritime environment. Six years before the broadcasting of the television series, on 1 July 2004, a new international regulatory code governing security in relation to the largest ports globally came into force. The International Ship and Port Facility Security (ISPS) code represented the international maritime community’s response to the terrorist attacks in the United

States (US) on 11 September 2001. Amongst other things the code demanded the introduction of restricted zones around the ship/port interface, introduced a new three-tiered security level system for major ports and led to the creation of a new Port Facility Security Officer (PFSO) role. Counter-terrorism had moved towards the very top of the policy agenda.

This thesis seeks to examine counter-terrorism efforts in relation to the UK’s ports and harbours (its ‘maritime infrastructure’\(^3\)) in the context of responses to international terrorism. Its objectives are to set out what policies were implemented, how, and with what impact on the management of UK maritime infrastructure in the period between 1 July 2004 and 30 June 2009. In doing this the study provides further, specific insights into the impact of the ‘war on terror’ on practice. Within the UK the ‘war on terror’ has been the justification for a wide range of policy decisions. In terms of foreign policy it led to the UK embarking upon military conflict in Afghanistan and Iraq. Domestically it led to the introduction of a raft of domestic counter-terrorism legislation which has, amongst other things, seen the expansion of pre-charge detention for terrorist suspects. The British government’s counter-terrorism strategy ‘CONTEST’, arranged around the 4 p’s of ‘Protect’,


\(^3\) In this thesis a ‘port’ is understood to be a location at which facilities are in place for a vessel to be loaded and unloaded. A port then is understood to be generally larger than a ‘harbour’, a place at which generally smaller vessels may dock and/or be stored. There are both artificial and natural harbours.
‘Prepare’, ‘Prevent’ and ‘Pursue’ framed and continues to frame the business of state in a multitude of different ways.\(^4\)

Research conducted into the ‘war on terror’ is of course by no means novel. Yet this should do nothing to diminish efforts at learning more about its widespread effects. Although 10 years have passed since the terrorist attacks which led to the pursuit of the ‘war’, this distance has served only to provide additional speeches and policies to examine, offering new opportunities to locate trends. The study is also of interest because of the specific case which is placed under scrutiny – UK maritime infrastructure. The UK’s ports and harbours represent one part of the wider supply chain. An estimated 95% of British international trade by volume and 75% by value is transported through its maritime infrastructure by sea.\(^5\) Ports and harbours are also part of the transport network and the UK border representing points of entry and exit in to the country. The result is that counter-terrorism efforts in relation to UK maritime infrastructure have a wider impact upon the lives, not only of the very many people who live and work near in and around that infrastructure, but arguably of the country as a whole who rely on the goods imported through those sites or travel through them on a more periodic basis.


By bringing together a particular context, the ‘war on terror’, and a specific case, UK maritime infrastructure, the thesis does then place two interesting strands of research in to one study. In examining efforts to counter international terrorism, the study is at its heart a study about security. While acknowledging that security is an essentially contested concept, the thesis utilises the securitisation theory, as developed by the Copenhagen School, as the analytical framework through which the case study is examined. Securitisation theory argues that security is socially constructed through discourse. More specifically an issue becomes a security issue when a referent object is successfully presented through language as being existentially threatened and thus in need of securing through emergency measures. The logic of security is then survival.

The choice of securitisation theory rests on the view that in focusing on language, the theory effectively captures the way in which the terrorist attacks in the US on 11 September 2001 were utilised to justify the pursuit of a ‘war on terror’. By presenting international terrorism as posing an existential threat to the ‘civilised way of life’ and thus in need of securing, the space was created through which counter-terrorism considerations increasingly shaped policy. Securitisation theory’s well elaborated components including ‘securitising actors’, ‘referent objects’, ‘audience’ and ‘facilitating conditions’, also makes the process of deconstructing security far

---


more straightforward. The belief that securitisation facilitates emergency action also effectively captures the way in which security policy can bring about substantial change, fundamentally altering accepted practice in the name of security. This thesis’ interest in examining the impact of counter-terrorism efforts on the management of UK maritime infrastructure means that research emphasis will be reoriented towards what can be called the ‘post-securitised environment’ and on to the implementation of emergency measures.

(I.2) Contribution:

In undertaking this study the thesis intends to make a contribution in three main ways. First, in utilising securitisation theory as an analytical framework, the thesis provides an additional case study with which to illustrate the strengths of using an approach that conceptualises security as being socially constructed, specifically through discourse, to understand the impact of the ‘war on terror’ on policy. More specifically by highlighting securitisation theory’s emphasis on the performative power of language, the acknowledgement of the role meta-narratives can play which is captured in the concept of macrosecuritisation, and the belief that the politics of security is the politics of emergency specifically, the thesis captures the way in which policy relating to UK maritime infrastructure was increasingly shaped by concerns about international terrorism after 11 September 2001.

Following on from this, by reorienting the securitisation theory towards the ‘post-securitised environment’ and on to the implementation of emergency measures, the
thesis places greater emphasis on understanding what securitisations ‘do’ in practice. Securitisation theory has been widely utilised to undertake a range of studies, yet predominantly they have focused on how an issue has specifically been securitised or on debates about whether securitisation is positive or negative. By shifting emphasis on to examining the content of emergency measures, their delivery along the policy chain and impact on day-to-day activities over a sustained period of time, the intention is to more effectively balance securitisation theory’s vast insights over how security policy is facilitated with a stronger understanding of these policies effects. This represents a deepening of securitisation theory and in doing so promises to open up a range of future research avenues by offering a wider pool of empirical material from which a fuller study in to say, the wider implications of securitisation on civil liberties can be initiated.

Finally the thesis will provide a diverse user community consisting of both academics and practitioners with an analysis of those policies which have been introduced in relation to UK maritime infrastructure security in the context of responses to international terrorism, and of their impact on that infrastructure’s management. Existing literature in the broad area of maritime infrastructure security often focuses on developments outside of the UK and specifically on the US and/or can be mechanistic outlining security policy without fully elaborating either the

---

environment in which it emerges or its impact on practice over a sustained period of time. In setting out the securitising narratives that underpin security policy, charting developments in practice chronologically over a five year period, and underpinning all this with reference to day-to-day activities within three UK cases, the thesis seeks to offer a fuller examination of developments. Specifically here, the thesis hopes to make a valuable contribution for anyone with responsibilities relating to the security of UK maritime infrastructure interested in building additional institutional memory.

(I.3) Central argument:

The thesis argues that the United Kingdom’s maritime infrastructure was securitised in the context of the macrosecuritisation of the ‘civilised way of life’, which were in a mutually reinforcing relationship. This macrosecuritisation was captured in the ‘war on terror’ discourse of counter-terrorism. Here western political leaders internationally, most prominently in the US and UK, acted as securitising actors presenting a macro-level referent object, the ‘civilised way of life’ as being existentially threatened by a macro-level threat, ‘international terrorism’. Successfully appealing to a broad audience made up of the national policy networks specifically constructed with the responsibility for the counter-terrorism security

---

response, and the general public to whom governments must appeal for support for their decisions, the macrosecuritisation facilitated the implementation of a wide range of emergency measures. This resulted in the focus on enhancing security permeating and framing ever greater areas of life, including UK maritime infrastructure.

Acknowledging that ports and harbours are ultimately geographic spaces, UK maritime infrastructure is described as a ‘site of securitisation’ as everyone, everything, and all activities associated with this space are increasingly presented as requiring ‘securing’ against a presented terrorist threat. It is argued that the presented threat was captured within two main narratives described as the ‘target’ and ‘vulnerable node’ narratives respectively. In the former narrative UK maritime infrastructure is presented as being a possible target of terrorist attack. Here international terrorism threatens the operability of the infrastructure which in turn may have wider negative consequences for the ‘civilised way of life’. In the latter narrative UK maritime infrastructure is presented as being a space which may be exploited by terrorists to facilitate attacks elsewhere with equally negative consequences.

The description of the relationship between the macrosecuritisation of the ‘civilised way of life’ and the securitisation of UK maritime infrastructure as mutually reinforcing is an acknowledgement that these narratives draw upon understandings of a wider international terrorist threat, and in their reproduction ensure that threat remains in wider consciousness. This situation is extenuated with the implementation
of emergency measures as counter-terrorism considerations remain centre-stage. The thesis argues that the securitisation of UK maritime infrastructure, like the macrosecuritisation itself, remained markedly stable over the course of the case study period in so far as it was resilient to resistance and largely unchanged in form.

The impact of this securitisation on the management of UK maritime infrastructure is described as substantial. The counter-terrorism security response evident had three main characteristics - it constantly evolved, was layered and increasingly expansive in scope. More specifically then there was an element of restlessness about counter-terrorism efforts with new practice emerging continually. There were a number of different dimensions to the practice examined, with a belief amongst those responsible for counter-terrorism of the importance of ensuring that if one measure failed another would take its place. While the increasingly expansive scope was captured in the way in which both a growing range of day-to-day activities were shaped by counter-terrorism considerations and by the way in which the space that was deemed to require securing in relation to UK maritime infrastructure continued to expand. There was then a spatial dimension to the securitisation.

Alongside these main characteristics the argument is advanced that the counter-terrorism security response had a number of prominent, recurring features. Legislation and regulations with some counter-terrorism implications played a central role in the response. A focus on enhancing co-ordination between different members of the policy network responsible for UK maritime infrastructure security was evident. There was a growth in spending on security and on the use of
technology to enhance security. The counter-terrorism security response was underpinned with a sense of urgency, while security undoubtedly gained a higher profile in day-to-day activities within UK maritime infrastructure. The thread which ran through this counter-terrorism security response was the pursuit of increased power in relation to UK maritime infrastructure undertaken by the British state and port owners in particular. Security and power in this case then were very much intertwined.

(I.4) Thesis structure:

The thesis’ primary objective is to examine the impact of securitisation on the management of UK maritime infrastructure between 1 July 2004 and 30 June 2009. This starting point represents the date on which the ISPS code, the clearest manifestation in practice of the securitisation after 11 September 2001, formally came in to force. To meet this objective and advance the argument set out previously the thesis is structured in the following way.

The first chapter sets out how the Copenhagen School’s securitisation theory is utilised as the analytical framework for this case study. Before doing this the assumptions on which the choice of the theory rests are set out and defended. As part of this process the theory is placed in its wider intellectual context within security studies literature, the case for a reorientation of research emphasis towards the ‘post-securitised environment’ is made, and prominent criticisms of securitisation theory
are discussed. With this complete the parameters of the case study are elaborated, with both the methods and sources to be utilised laid out and justified.

The second chapter places the case study within its immediate historical context. It charts the way in which the ‘war on terror’ discourse of counter-terrorism was constructed in the aftermath of the 11 September 2001 terrorist attacks in the United States (US). It argues this discourse captured the macrosecuritisation of the ‘civilised way of life’. Here then a way of life, characterised as encapsulating democracy, economic prosperity and individual liberty, was successfully presented as being existentially threatened by international terrorism and thus in need of securing. The chapter illustrates how this macrosecuritisation placed counter-terrorism at the very top of the policy agenda framing large swathes of both foreign and domestic policy.

With the focus on UK maritime infrastructure firmly in mind it then progresses first to elaborate the impact the ‘war on terror’ had domestically in the UK and then to provide an early insight in to how UK maritime infrastructure specifically was securitised in this context. By focusing on the initial implementation of the ISPS code the chapter highlights the two main narratives in which the terrorist threat relating to UK maritime infrastructure was presented. It also begins the process of demonstrating how the relationship between the macrosecuritisation of the ‘civilised way of life’ and the securitisation of UK maritime infrastructure could be described as mutually reinforcing. Finally a number of prominent features of the counter-terrorism security response relating to UK maritime infrastructure are noted. In contextualising the case study the second chapter provides evidence to support the
thesis’ starting premise that UK maritime infrastructure had been securitised, whilst providing a base point in terms of both discourse and practice from which future developments can be compared.

The case study itself is undertaken across three chapters. Chapter three covers developments between 1 July 2004 and 6 July 2005, the year after the ISPS code came into force. Chapter four examines the period between 7 July 2005 and 26 June 2007, the two years after the terrorist attacks on the London transport network. Chapter five focuses on the first two years of the premiership of Gordon Brown between 27 June 2007 and 30 June 2009. Recognising the desire to ensure the environment in which security policy emerges is fully elaborated, as noted in the sub-section ‘contribution’, attention falls first on examining discourse. This process is captured in the first core research question, ‘How has UK maritime infrastructure been securitised in the context of responses to international terrorism?’ Here most prominently the thesis seeks to shed further light on the specific narratives produced and reproduced with regards to the presented terrorist threat, whilst analysing any instances of resistance.

The reorientation of emphasis towards the post-securitised environment and on to the implementation of emergency measures then takes place. This represents the primary focus of each chapter as attention falls on examining practice. To better facilitate this process each chapter has an identical structure. This acknowledges the process in policy process facilitating an assessment of change over time whilst enabling the prominent features and main characteristics of the counter-terrorism security
response to be located and discussed. The totality of counter-terrorism practice is sub-divided into three constituent parts. These are ‘legislation and regulations’, ‘institutional changes and infrastructure developments’ and ‘working practices’. The case study also draws upon specific experience from three cases of UK maritime infrastructure to help illustrate trends. These are the ports of Felixstowe, Holyhead and Tilbury. All this is framed by the second core research question, ‘What has been the impact of securitisation on the management of UK maritime infrastructure?’ which puts the thesis’ objective in question form. With the case study complete the thesis draws to a close. In the overall conclusion the development of the thesis’ line of argument is sketched out, the two core research questions listed here are addressed directly with reference to the case study’s key findings, and possible future research avenues are highlighted.
Chapter One

Reorienting towards the ‘post-securitised environment’: utilising the Copenhagen School’s securitisation theory as an analytical framework

(1.1) Introduction:

The purpose of this first chapter is to set out how securitisation theory will specifically be utilised as an analytical framework through which this examination of counter-terrorism efforts in relation to the United Kingdom’s (UK) maritime infrastructure in the context of responses to international terrorism is undertaken. In particular there is a need to explain two assumptions on which the selection of the theory is based. The first assumption is that the conceptualisation of security as socially constructed, which lies at the heart of the theory, captures the way in which particular and dominant understandings of the threat posed by international terrorism, and the subsequent response to it, emerged out of intersubjective processes of contestation and negotiation. There was nothing inevitable then in a policy environment being framed by an emphasis on the pursuit of a ‘war on terror’. The second assumption is that securitisation theory in particular, with its emphasis on discursive construction and its highlighting of the politics of emergency, offers a
particular set of insights that more fully captures developments relating to UK maritime infrastructure whilst offering a useful accompanying framework with which the case study can be undertaken.

To make this case the chapter begins by placing securitisation theory, as developed by the Copenhagen School, in its wider intellectual context within security studies. After acknowledging that there is no single, agreed definition of security, the chapter moves on to elaborate what it means to conceptualise security as being socially constructed, before elaborating a variety of approaches that accept such a conceptualisation in order to substantiate the first assumption. At this point, securitisation theory is outlined, and it is here that the more specific insights securitisation theory offers for the case study are noted and the second assumption defended. In particular the chapter highlights the theory’s ability to capture the performative power of security on the policy environment, effectively grasping how policy was increasingly justified on the basis of being a necessity, part of the wider response to the existential threat presented as being posed by international terrorism. Here the introduction of the Copenhagen School’s concept of ‘macrosecuritisation’ is presented as being particularly relevant in capturing the way in which responses to international terrorism came to dominate the policy agenda. Beyond this, the necessity for audience acceptance before an issue is securitised represents an important acknowledgement of the need to legitimise emergency action, specifically in liberal-democracies. Finally and more practically, the ability to utilise the theory to analyse policy developments without explicitly signing up to a particular normative agenda appeals in a case study that is interested primarily in policy implementation.
With these insights elaborated the chapter moves on to elaborate how specifically securitisation theory serves as the analytical framework for the case study. Here the argument is advanced that there remains a need to reorient research towards what is termed the ‘post-securitised environment’ and on to implementation, examining in more depth what securitisations ‘do’ in practice. The ability to engage in such a reorientation without undermining the conceptualisation of security as being discursively constructed is raised as an additional strength of the theory. This reorientation is positioned as a deepening of securitisation theory, emphasising the need to shed light on the implementation of emergency measures (the counter-terrorism security response) and allowing more attention to fall on charting how securitisations are reinforced and challenged over time. This reorientation then places focus on examining the content of emergency measures, how they are delivered on the ground and their impact on day-to-day activities. At this point an assessment of the main criticisms lodged against securitisation theory are made and their implications for the case study discussed. With this complete, the parameters of the case study are set out in relation to the theory. The chapter concludes by elaborating the methods which are used and sources that will be utilised to undertake the case study.
(1.2) **Contextualising the Copenhagen School’s securitisation theory:**

‘Security’ has been and continues to be heavily debated as a concept.¹ Defining what security is, what it means to be secure or how this security can ultimately be realised has provoked a considerable amount of disagreement. Such debates have been further energised by key events internationally, such as the end of the Cold War, or the terrorist attacks in the United States (US) on 11 September 2001.² Security is ultimately an example of what W.B. Gallie termed an ‘essentially contested concept’, one where there is “no one clearly definable use […] which can be set up as the correct or standard use”.³ Despite this situation, efforts to emphasise commonalities between research agendas through conducting surveys of the use of the concept have continued.⁴ These organisational exercises and the labels utilised have not been beyond critique themselves, occasionally regarded as counter-productive, becoming “weapons in disciplinary mud-slinging matches, which can close down discussion and inquiry before a close reading of specific arguments”, or for representing an inaccurate reading of the literature and the arguments contained

---


there within. Yet with no consensus being possible over the concept, the onus increasingly falls on the analyst to elaborate their specific understanding of it, in doing so drawing out commonalities across the literature in order to provide additional clarity to research.

In this case study the conceptualisation of security as being socially constructed, as encapsulated in the Copenhagen School’s securitisation theory, is embraced. Here the central assumption made is that our understanding of what it means to be secure, what issues are regarded as security issues, indeed what is regarded as the reality of security as a whole is constructed inter-subjectively through processes of negotiation and contestation. While the meaning of security could well become sedimented, there is an explicit rejection of the idea that it is objectively fixed. As an approach it ultimately results in greater emphasis being placed on contextual understanding. To elaborate, utilising an example provided by Jutta Weldes, while those supporting this conceptualisation would not challenge the existence of nuclear weapons, they would

---


seek to understand why it is “that the United States is threatened by Russian, but not British, nuclear weapons”.7

Emerging from this emphasis on contextual understanding is a broader ontological position embraced by analysts as ideational factors such as identity, norms and values are regarded as being as important as material factors (weapons, troop numbers) when studying security, particularly in relation to the designation of threat. This emphasis on social construction was most famously espoused by Alexander Wendt in his article ‘Anarchy Is What States Make of It: The Social Construction of Power Politics’. Here Wendt argued that agents and structures are mutually constituted writing that, “it is collective meanings that constitute the structures which organize our actions”, noting for example that “if society ‘forgets’ what a university is, the powers and practices of professor and student cease to exist”.8

The conceptualisation of security as being socially constructed stands most explicitly in contrast with the realist, specifically structural realist position, where security is regarded as an objective condition - something that exists independently to be studied - with that study being fixed narrowly on “the threat and use of force”.9


Capabilities, particularly military capabilities, are highlighted as being of central importance, ensuring that it is those material factors that are placed at the centre of study. There is a wider drive amongst structural realists to remove “notions such as environment, situation, context and milieu”, ideational factors, from a theory of security because they are deemed to be too vague and variable to be useful when seeking explanation.¹⁰

First elaborated by Kenneth Waltz in his 1979 text, ‘Theory of World Politics’, structural realism rests on a belief that there are certain timeless realities – results that always take place if particular conditions are in play - which ultimately means contextual understanding is deemed to be of little importance.¹¹ Studying security, then, is to seek “cumulative knowledge about the role of military force”¹² and this is obtained by following what Stephen Walt describes as “the standard canons of scientific research: careful and consistent use of terms, unbiased measurement of critical concepts, and public documentation of theoretical and empirical claims”.¹³ The analyst then can completely separate themselves from an observable world, locating and testing laws of international politics, like those in the natural sciences may locate and test, say, the laws of physics.¹⁴


The conceptualisation of security as being socially constructed, and by association the rejection of the structural realist conceptualisation of security as a fixed and objective condition, has been embraced by a range of security scholars who would otherwise diverge in their views on security.\footnote{Although highlighting how they diverge is not relevant to this case study, two common forms of divergence are over how an issue specifically comes to be regarded as a security issue and over the politics of security; what security does.} Periodically attempts have been made to bring these scholars together, an endeavour most effectively initiated by Keith Krause and Michael Williams in their book ‘Critical Security Studies: Concepts and Cases’ during the mid-1990’s. Here they noted and sought to question the idea that when studying security “one already \textit{knows} what it is to be studied”,\footnote{Keith Krause and Michael C. Williams (eds.), \textit{Critical Security Studies: Concepts and Cases} (London: UCL Press/Routledge, 1997), p. ix.} arguing “the concept of security is not empty; it implicitly invokes and relies on a series of accepted prior visions of what it is to be secured.”\footnote{Ibid., p. x.} More recently scholars came together under the name ‘c.a.s.e collective’ to assess the evolution of those approaches underpinned by “the identification and denunciation of \textit{depoliticization}, both in the social realm and in the realm of academia”.\footnote{c.a.s.e. collective, ‘Critical Approaches to Security in Europe: A Networked Manifesto’, \textit{Security Dialogue}, 37:4 (2006), p. 445. A brief debate followed on the manifesto see Andreas Behnke, ‘Presence and Creation: A Few (Meta-) Critical Comments on the c.a.s.e Manifesto’, \textit{Security Dialogue}, 38:1 (2007), pp. 105-111; Mark B. Salter, ‘On Exactitude in Disciplinary Science: A Response to the Network Manifesto’, \textit{Security Dialogue}, 38:1 (2007), pp. 113-122 and c.a.s.e collective, ‘Europe, Knowledge, Politics – Engaging with the Limits: The c.a.s.e collective Responds’, \textit{Security Dialogue}, 38:4 (2007), pp. 559-576. Also see Columba Peoples and Nick Vaughan-Williams, \textit{Critical Security Studies: An introduction} (Abingdon, Oxford: New York: Routledge, 2010) for another survey of these kind of approaches.}
The emphasis on the role ideational factors play in the construction of security has been particularly highlighted by critical constructivist security scholars who seek to shed light upon the way in which, say, particular understandings of identity come to be seen as dominant, despite identity ultimately being “inherently unstable, contingent and a site of constant competition.” Ultimately they have a more explicitly normative dimension to their research as they aim to explode “the myths associated with identity formation” and understand how identities come to be regarded as a “single version of a naturalized truth”. Empirically this has resulted in an interest in examining how particular understandings of identity determine what responses are deemed legitimate and possible. Notable examples of this approach include Roxanne Doty’s work on the relationship between national identity, representations of immigration and understandings of border security, and Michael Barnett’s study of Yitzhak Rabin’s representation of identity and history in the context of building support for the Oslo Peace Accords.

Poststructural security scholars also seek to highlight the role understandings of identity play on conceptualising security, arguing that ultimately “identity is

---


constituted in relation to difference.”

Here they seek to focus on the way in which the construction of a series of binary opposites such as inside/outside, self/other, domestic/foreign, act in a self-perpetuating fashion, to give identity, indeed world politics as a whole, a (false) sense of stability. Locating how knowledge of the social world plays a role in (re)producing it is therefore of utmost interest. In terms of security research, the work of David Campbell on US foreign policy represents a particularly notable example of this approach. By deconstructing political discourse Campbell examines the way in which US national identity has been forged through the production of what it means to be ‘dangerous’, noting “the constant articulation of danger through foreign policy is thus not a threat to a state’s identity or existence: it is its condition of possibility.”

Feminist security scholars meanwhile seek to challenge the idea that security is a gender-neutral concept, instead highlighting gender-hierarchies. Research efforts have focused on addressing what is regarded as the marginalised role of women in security studies literature, with for example, emphasis placed on examining both the


25 Peoples & Williams, Critical Security Studies, p. 67. On a wider level W.B.J Walker notes in: W.B.J Walker, Inside/outside: international relations as political theory (Cambridge: Cambridge University Press, 1993), p. 5, how IR theories themselves can be read “as a crucial site in which attempts to think otherwise about political possibilities are constrained by categories and assumptions that contemporary political analysis is encouraged to take for granted”.

26 Peoples & Williams, Critical Security Studies, p. 67. Also see James Der Derian and Michael J. Shapiro, International/intertextual relations: postmodern readings of world politics (Lexington, Mass.: Lexington Books, 1989) for an introduction to this approach.


role of women in conflict and the impact conflict has had on them. Beyond this, the role security plays in actually constructing understandings of gender and vice-versa has also been the subject of investigation. More recently here research led by scholars such as Sandra Whitworth and J. Ann Tickner have concentrated on studying the way in which particular understandings of masculinity have been wrapped up in the response to the terrorist attacks in the US on 11 September 2001, and with what implications. Beyond this rich body of literature the view that security is socially constructed is also shared by three ‘schools’ of research – the Welsh, Paris and Copenhagen School itself - that have played a major role in influencing European security studies. Outlining their work then can serve the function of both further demonstrating the diversity of research that rejects the view that security is a fixed, objective condition, and illustrating in greater depth the intellectual environment in which securitisation theory emerged.

The label Welsh School stems from the location of its most prominent scholars, Ken Booth and Richard Wyn Jones. Most comprehensively set out in Booth’s book

---


‘Theory of World Security’, for the Welsh School the construction of something as a security issue is not necessarily a sign of failure or something to be avoided, but only if the logic of security is re-defined as being about more than survival. Booth argues that security and survival do not necessarily go hand in hand and as such a ‘survival plus’ approach to conceptualising security (adding dignity, for example) should be embraced. Here the pursuit of emancipation is central, defined as:

the theory and practice of inventing humanity, with a view to freeing people, as individuals and collectivities, from contingent and structural oppressions. It is a discourse of human self-creation and the politics of trying to bring it about.

Emancipation is achieved by reorienting security towards the individual and through immanent critique. This emphasis on the centrality of individuals rests in part on the school’s belief that institutions can “divide humanity”, while undertaking an immanent critique is to “undertake a critique of an existing order from within, rather than relying on an ahistorical point of reference”. For the Welsh School, the potential for change exists within society now, but the key is to recognise and develop it. This emphasis on revealing and then challenging hegemonic ideas illustrates the theoretical underpinnings of the school’s work which can be connected to the work of the Frankfurt School, the writings of Antonio Gramsci, and their

34 Booth illustrates the argument with an example of the position of prisoners held in Nazi death camps. Booth, Theory of World Security, p. 104.
35 Booth (ed.), Critical Security Studies and World Politics, p. 181. Humanity encapsulates ideas such as love, hospitality and tolerance. (Ibid., p. 182)
36 Ibid., p. 267.
37 Fierke, Critical Approaches to International Security, p. 167. Fierke notes that immanent critique enables a scholar to stand “within time, yet creates a critical distance from his or her historical context, in order to explore its origins, development, institutions and potential for change”. (Ibid., p. 182).
Aberystwyth colleague Andrew Linklater’s pursuit of a Critical Theory of International Relations.\textsuperscript{38}

Representing a post-structural inspired approach to security, the Paris School includes scholars such as Didier Bigo and Jef Huysmans and takes its name from the Institut d’Etudes Politiques in Paris where the former is based. The school places greatest emphasis on developing the concept of ‘(in)security’, seeking to challenge the idea that International Relations has what Bigo calls “a monopoly on the meanings of security”.\textsuperscript{39} The school argues that security can at various points be economic and social, and it may even mean comfort or general unease.\textsuperscript{40} It is not the defining logic of security which is necessarily the most important issue under consideration, rather it is the need to acknowledge that “security cannot be global and for all. Security has winners and losers”, and that “the practices of securing some are simultaneously practices rendering others insecure”.\textsuperscript{41} Their focus on (in)security therefore results out of this acceptance that security and insecurity are not mutually exclusive. In short, “security is not the opposite of insecurity. How security is defined conditions what is considered as insecurity.”\textsuperscript{42}

\textsuperscript{38} The Frankfurt School included scholars such as Max Horkheimer, Theodor Adorno and Jurgen Habermas. They provided the Welsh School with what Booth has described as the “inspiration to critique” (Booth, \textit{Critical Security Studies and World Politics}, p. 44) and are the source of their use of immanent critique. Richard Wyn Jones provides a good overview of the links between the Frankfurt and Welsh School’s in Wyn Jones, \textit{Security, Strategy and Critical Theory}. Also see Antonio Gramsci, \textit{Prison Letters}, translated by Hamish Henderson (London: Pluto Press, 1996) and Andrew Linklater, \textit{Beyond Realism and Marxism: Critical Theory and International Relations} (Houndmills, Basingstoke, Hampshire: Macmillan, 1990).


\textsuperscript{40} Ibid., p. 123.

\textsuperscript{41} Idem. This links with those scholars who seek to examine the creation and reinforcement of ‘Us versus Them’ dichotomies as a mechanism of maintaining power relations and control. See Campbell, \textit{Writing Security} and Weldes et al (eds.), \textit{ Cultures of Insecurity} for more.

\textsuperscript{42} c.a.s.e collective, ‘Critical Approaches to Security in Europe: A Networked Manifesto’, p. 457.
The School’s work emerges out of an engagement with the writings of Michel Foucault and Pierre Bourdieu in particular. (In)security then is understood as a technique of government and as a mechanism through which privileged positions are maintained. Bourdieu’s concept of ‘field’ defined as a “network or a configuration of objective relations between positions” is utilised as the methodology through which the processes of (in)security are examined. Empirically the school examines the routines, practices and “mundane bureaucratic decisions of everyday politics” that facilitate (in)security becoming a domain of practice, are interested in the role technologies such as surveillance cameras and large-scale databases play in disciplining society and maintaining existing power relations, and in the role of security professionals, both state and private.


46 For more on this see Didier Bigo and Elspeth Guild (eds.), *Controlling frontiers: free movement into and within Europe* (Aldershot, Hants.: Burlington, VT.: Ashgate, 2005) and Nick Vaughan-Williams, *Border Politics: The Limits of Sovereign Power* (Edinburgh: Edinburgh University Press, 2009). The focus on technology and its controlling effects can be traced to Jeremy Bentham’s idea of a ‘Panopticon’ first published in 1791. The panopticon was Bentham’s design idea for a prison whereby all prisoners would be controlled through the fear of constant inspection.

47 They are also interested in the relationships between these actors. For example, Bigo & Guild, *Controlling frontiers*, p. 4, argue there is a growing distinction, indeed tension between policy professionals who remain “sovereignty-bound and –minded, and the professionals of security who are more and more globally orientated”.
(1.3) **The Copenhagen School:**

It is the third of these schools of thought that embrace the idea that security is socially constructed – the Copenhagen School – who developed the securitisation theory that will be utilised as an analytical framework in this case study. Originally based at the now defunct Copenhagen Peace Research Institute (COPRI), the school, including Barry Buzan and Ole Waever, has been the source of a wide range of literature on security.\(^{48}\) Most evidently starting in the seminal work ‘People, States and Fear’, Buzan argued that a tendency amongst realists to regard “security as a derivative of power”\(^{49}\) and for liberals to regard security as a consequence of peace, had meant that there was a failure to analyse security on its own terms and to see it as being unique in its own right. It was this belief that has led the school to continually challenge scholars to think and rethink what it means to talk about and study security.

Securitisation theory emerged out of this process as the central component of the school’s work. Alongside this the school has also been responsible for the development of the concepts of ‘security sectors’ and ‘regional security complexes’.\(^{50}\) Briefly elaborating these two concepts shows how the school have sought to unpack the concept of security. It also completes the process of setting out


\(^{50}\) These are most comprehensively weaved together in *Security: A New Framework for Analysis*. 
the intellectual context in which securitisation theory sits because as Matt McDonald argues, “‘sectors’ and ‘regional security complexes’ are significant for the broader framework primarily as either sites for securitization practices or as dynamics conditioning the success or failure of such practices in particular geographic areas”. 51

The Copenhagen school’s focus on security sectors emerged out of a belief that the study of security could most effectively be undertaken by being broken down in to more manageable parts in order “to reduce complexity to facilitate analysis”. 52 Defining security in terms of existential threat (survival), the school focuses on five broad areas in which threats may transpire each of which is referred to as a ‘sector’. The school acknowledges the separation between these sectors is imperfect; reassembly must always follow because each sector “is looking at the whole but is seeing only one dimension of its reality”. 54 The ‘military sector’ focuses primarily on military capabilities and state perceptions of these, the ‘political sector’ on the organisational stability of states, the ‘economic sector’ on access to the resources necessary to sustain power and particular standards of welfare, the ‘societal sector’ on the sustainability of a particular language, culture and identity, and the ‘environmental sector’ on the maintenance of local and the planetary biosphere. 55

51 Matt McDonald, ‘Constructivism’ in Williams, Security Studies: An Introduction, p. 69.
53 Idem.
54 Idem.
55 Ibid., p. 19.
Although the Copenhagen School undoubtedly regard the state as the primary referent object of security in practice (something which is presented as being threatened) acknowledging it holds a sedimented and dominant position in security studies today\textsuperscript{56}, they also argue that “a multisectoral approach to security” demands that other referent objects have “to be allowed into the picture”.\textsuperscript{57} Barry Buzan had argued that security is “primarily about the fate of human collectivities and only secondarily about the personal security of individual human beings”.\textsuperscript{58} In this vein the School later expended considerable energy on studying societal security, understood as “situations when societies perceive a threat in identity terms”.\textsuperscript{59} Here as well as being one sector of state security, society is regarded as a referent object of security in its own right because in certain circumstances society could be regarded as a viable unit within the international system itself. The focus on identity is particularly interesting in this case study because the wider context is one where international terrorism has been presented as threatening the ‘civilised way of life’ best understood as encapsulating democracy, economic prosperity and individual liberty. Here identity is wrapped up with being part of (or not) the ‘civilised world’ and it is, as the next chapter argues, what the subsequent pursuit of a ‘war on terror’ has been based upon.

\textsuperscript{56} Ibid., p. 37 and pp. 205-207.

\textsuperscript{57} Ibid., p. 8.

\textsuperscript{58} Buzan, \textit{People, States and Fear}, p. 19. A succinct expansion of this position can be found in Waever et al., \textit{Identity, Migration and the New Security Agenda in Europe}, p. 20, when it is argued that “the resultant focus on individual and global security simply misses out the essential dynamics of collective units (states, societies) constituting themselves as social and political realities by interacting in an international system”.

\textsuperscript{59} Waever et al., \textit{Identity, Migration and the New Security Agenda in Europe}, p. 20. This text most comprehensively sketches out the school’s ideas in relation to societal security.
The Copenhagen School’s development of the concept of regional security complexes stems from their interest in how these human collectivities interact. Security is regarded very much as a relational matter, it is about “how human collectivities relate to each other in terms of threats and vulnerabilities”. The school argues that the widest, systemic level of analysis fails to adequately conceptualise how different states have different security situations yet do not directly impact upon each other, leading them to focus instead on the regional level of analysis. A ‘security complex’ is defined as “a set of states whose major security perceptions and concerns are so interlinked that their national security problems cannot reasonably by analyzed or resolved apart from one another.”

They are defined by examining the patterns of both power relations and amity and enmity between states and they can be charted on a continuum from ‘conflict formation’ (where interdependence is driven by fear, rivalry and shared threat perceptions) through to ‘security regimes’ (where states view each other as potential threats, but make arrangements to reduce the security dilemma) through to a ‘pluralistic security community’ (where there is no expectation or preparation to use force in relations with each other). Europe is understood as a pluralistic security

---


61 Ibid., p. 11. In People States and Fear, 186, Buzan expands further by arguing that two additional reasons for focusing on regional security dynamics is to “provide area specialists with the language and concepts to facilitate comparative studies across regions” and “to offset the tendency of power theorists to underplay the importance of the regional level in international security affairs”.

62 Ibid., p. 12.

63 Buzan, People, States and Fear, p. 189.

64 More details can be found in: Buzan et al, Security: A New Framework for Analysis, p. 12.
community, a position that can help us to understand how a common foreign and security policy has emerged between the member states of the European Union (EU). Again this is of some use in this case study as this element of regional cohesion serves as the backdrop in which a number of measures designed to tackle the presented threat posed by international terrorism to UK maritime infrastructure have emerged at the European level of governance.

(1.4) **The Copenhagen School’s securitisation theory:**

The chapter to this point has sought to elaborate the intellectual context in which securitisation theory can be located, arguing it is the central component of the work of the Copenhagen School, one body of research among many that share the view that security is socially constructed. Here the meaning of security is constructed intersubjectively through processes of contestation and negotiation, and although it may become sedimented, it cannot be fixed. Securitisation theory itself was originally developed in a series of unpublished working papers by Ole Waever in the mid-1980s, one of which ‘Security, the Speech Act: Analysing the Politics of a Word’ was kindly provided by Waever to help facilitate further an understanding of its genealogy here. Securitisation theory fleshes out the notion of social construction encapsulating the idea that security is constructed discursively through the articulation of a speech act. Since its conception, the theory has evolved quite considerably, most notably through the addition of the requirement for ‘audience


66 Ole Waever, ‘Security, the Speech Act: Analysing the Politics of a Word’, (paper presented at the Research Training Seminar, Sostrup Manor, June 1989.) I would like to thank Professor Waever for providing me with a copy of this paper.
acceptance’ of any speech act in the Copenhagen School’s 1998 book ‘Security: A new framework for analysis’. It is this later version which is utilised in this case study. Securitisation theory has framed examinations in to a diverse range of subjects from state foreign policy behaviour to migration studies to the management of HIV/AIDS.67

Through securitisation theory the Copenhagen School seek to explain and understand what security is, how it is constructed, and provide answers to the following questions:

who can ‘do security’, on what issues, under what conditions – and with what effects?68

As already noted, at its heart security is defined as a speech act - the “(symbolic) interactionist act of achieving security with words”.69 For the Copenhagen School, a securitising actor identifies an existential threat to a particular referent object and in doing so frames the issue “either as a special kind of politics or as above politics”70 so that emergency measures can be pursued. This securitising move is only successful if an audience ‘accepts’ the need for emergency measures, creating an environment in which ordinary liberal-democratic rules can be and are revoked,


suspended and/or circumnavigated; in doing so changing the relationship between securitising actor, referent object and audience in some way. Security then is “a self-referential practice, because it is in this practice that the issue becomes a security issue – not necessarily because a real existential threat exists but because the issue is presented as such a threat.”71

(1.4.1) The speech act:

The speech act represents an acknowledgement that under certain conditions simply by uttering words, something is done – like betting, making a promise or naming a ship.72 Here speech does more than simply describe and report and is more than simply true or false: it can perform. The defining logic of the speech act for the Copenhagen School, and thus of security itself, is the claim of an ‘existential threat’, the framing of an issue in the language of survival. For the Copenhagen school “the basic definition of a security problem is something that can undercut the political order within a state and thereby ‘alter the premises of all other questions’”.73 Thus securitisation is about framing an issue in such a way that it becomes generally accepted that it is of the utmost priority, that implementing a response is a necessity, because a failure to act risks the demise of a particular referent object.

71 Idem.


Securitisation then occurs when the rhetoric of existential threat is used to take an issue out of what “under those conditions is ‘normal politics’”.\textsuperscript{74} The politics of security is the politics of emergency and is characterised by a sense of urgency and secrecy.\textsuperscript{75} Overall the school argues that there are a range of possible governing mechanisms, from securitisation at one end of a spectrum, towards politicisation at the other.\textsuperscript{76} To elaborate the theory further, focus will now fall on outlining how an issue is presented as being existentially threatened and by whom (a securitising move), on explaining under what conditions an audience are likely to accept a securitising move so that we can say we are witnessing securitisation, and in charting the Copenhagen School’s development of the idea of a macrosecuritisation which has particular relevance for this case study.

\textit{(1.4.2) A securitising move:}

The Copenhagen School make it clear that there are three units involved in a securitising move – referent objects, securitising actors and in a more peripheral role, functional actors. Referent objects are those “things that are seen to be existentially threatened and that have a legitimate claim to survival”.\textsuperscript{77} In principle anything can be a referent object, but the Copenhagen School suggest that in practice there are


\textsuperscript{76} Ibid., p. 29.

\textsuperscript{77} Ibid., p. 36.
fewer referents. In order to successfully put forward the case that something has to survive depends to a large extent on the size of the referent object. They argue that both individuals and small groups or the whole of humanity “seldom establish wider security legitimacy” and suggest it is the middle scale – states, nations and civilizations - that are more durable referent objects. For the school this position is simply a reflection of history, security has generally been about the survival of states and so forth and is not a negative judgement on the importance of individual rights or the well being of humanity as a whole.79

It is a securitising actor who declares a referent object existentially threatened. The Copenhagen School argue that the individual or group who performs the speech act are commonly “political leaders, bureaucracies, governments, lobbyists, and pressure groups.”80 Who can be a securitising actor is framed by capabilities, who is accepted as having the authority to ‘speak’ security. The school acknowledges that locating the securitising actor is “more complicated than identifying referent objects”.81 On some occasions the line between referent object and securitising actor can be blurred, such as with the state where “the referent object will in a sense speak for itself through its authorized representatives”.82

78 Idem.

79 This line of thinking can be seen in the school’s work on ‘societal security’ in particular, outlined in the previous section.


81 Idem.

82 Ibid., p. 42.
Further complications arise because it is often hard to judge and then categorise from which position security is being spoken; when for example does a particular Minister speak for him or herself and when do they speak for the government as a whole? The Copenhagen School argue that the key to overcoming such a situation is to ask what logic shapes the action in the first place and locate the securitising actor from there. Specifically one should focus on “the organizational logic of the speech act” rather than individual logic. While individuals are always the actor who is technically ‘speaking’, it is “usually more relevant to see as the ‘speaker’ the collectivities for which individuals are designated authoritative representatives”.

For example, Prime Minister Tony Blair could be said to have materialised as the United Kingdom. Through his legal position as Prime Minister, his views were more than just his own but became those of the state as a whole.

Finally functional actors can “significantly influence(s) decisions in the field of security”, “without being the referent object or the actor calling for security on behalf of the referent object”. The school provides the example of a polluting company who “can be a central actor in the environmental sector – (but) it is not a referent object and is not trying to securitize environmental issues (quite the contrary)”.

---

83 Ibid., p. 41. Once again this position is grounded in the school’s view that security is ultimately about the fate of collectivities.

84 All quotes taken from Ibid., p. 36.
(1.4.3) Securitisation - a successful securitising move:

The school acknowledges that there are no guarantees that when a securitising move is made that it will be successful. Rather “a successful securitisation [...] has three components (or steps)” to it. First a referent object has to be positioned as being faced by an existential threat. This is the only way that a securitising actor can gain the authority to call for some form of emergency action (the second step), and in doing change the dynamics of the relationship between various units by at least legitimising the possibility of the revocation, suspension and/or circumnavigation of the normal rules of engagement (the third step). Central to this is the requirement that a particular threshold is met whereby an audience accept the securitising move. They have to accept that a referent object is existentially threatened, that emergency measures may be required and that this action could change what they regard as normality. It is only at this point that we witness securitisation.

To achieve this audience acceptance a number of facilitating conditions must be in place. First, the rules of the speech act must be followed, these conditions are described as “the internal, linguistic-grammatical”. Here then securitising actors must present a referent object that has “a legitimate claim to survival” as being existentially threatened and in need of securing. The second series of facilitating conditions are described as “the external, contextual and social”. The Copenhagen

87 Ibid., p. 36.
88 Ibid., p. 32.
School sub-divide these into two. First, the securitising actor must be seen by a particular audience to have the necessary authority to make securitising claims and second, the alleged threats must be salient and understood. The absence of any of these conditions may result in securitising moves failing and thus securitisation does not occur.

As it was noted earlier, the inclusion of the audience represents the most significant development of the theory from its early form, when securitisation occurred simply through the utterance of the speech act. Locating the rationale for such a development is far from straightforward, however the school gives us a glimpse in to their thinking when they acknowledge that “one danger of the phrases securitization and speech act is that too much focus can be placed on the acting side, thus privileging the powerful while marginalizing those who are the audience and the judge of the act.” Understanding the exact role of the audience and its wider implications for securitisation theory as a whole has been the subject of some debate and even critique, all of which will be discussed in more depth later in this first chapter. Nevertheless the inclusion of the audience and a requirement for their acceptance serves as a further reminder, alongside the speech act itself, of the Copenhagen School’s acceptance of the view that security is socially constructed. As they summarise:

---

89 Ibid., p. 33.
90 Ibid., p. 41.

It is not easy to judge the securitization of an issue against some measure of whether the issue is ‘really’ a threat; [because] doing so would demand an objective measure of security that no security theory has yet provided. [...] [But] the label subjective, however, is not fully adequate. Whether an issue is a security issue is not something individuals decide alone. Securitization is intersubjective and socially constructed. [...] Thus, security (as with all politics) ultimately rests neither with the objects nor with the subjects but among the subjects.92

(1.4.4) Macrosecuritisation and security constellations:

More recently Buzan and Waever have introduced the concept of ‘macrosecuritisation’ to their work.93 They examine the possibility that securitisations can be maintained between the middle level of analysis where “collective political units, often but not always states, construct relationships of amity and enmity with each other” and the system level of analysis.94 Here they acknowledge how “one over-arching conflict” can result in a “higher order of securitisation” becoming embedded with other “more parochial securitisations beneath it.”95 In examining the relationship between securitisations, Buzan and Waever also highlight the concept of ‘security constellations’ which they acknowledge had been originally under-developed.96 A security constellation is a wider concept than security complexes outlined earlier and encapsulates “the totality of possible security interrelationships at all levels”.97 The focus on constellations is

94 Ibid., p. 253.
95 Idem.
96 Ibid., p. 254.
designed to serve as an acknowledgement that securitisations are not isolated. 98

There is an acknowledgement that macrosecuritisations can generate constellations “because they structure and organise relations and identities around the most powerful call of a given time.” 99

Macrosecuritisations still require the same components as any other securitisation in terms of speech acts, securitising actors and responsive audiences. 100 They are however more complex and thus more prone to breakdown. This may take place if the macro-level threat or referent object is desecuritised or if mid-level securitisations contradict it and/or break away. 101 Four types of universalist beliefs are raised up as one central source for macrosecuritisations. The first is ‘inclusive universalisms’ where it is claimed particular ideological beliefs “about the best way to optimise the human conditions” are applicable to all. 102 This may include “Liberalism, Marxism, Christianity, Islam”. 103 The second is ‘exclusive universalisms’ that claims superiority for one group and the right to rule over all others such as Nazism and Japanese imperial doctrine. 104 The third is ‘existing order universalisms’ which take “the global level international social structure as their


99 Ibid., p. 259. As the authors note on (Ibid., p. 268) actors may not recognise these larger structures (constellations) or they may not generate wider consciousness. This is something highlighted by the analyst.

100 Ibid., p. 265

101 Ibid., pp. 257-8. For example, they note that other states may believe that the ‘Global War on Terror’ is actually more about efforts to protect US national interest (national security securitisation) than securing civilisation.

102 Ibid., p. 260

103 Idem.

104 Ibid., p. 261.
referent object” and claim threats to institutions within that society. The final universalism is ‘physical threat universalisms’ that claim humankind is threatened on a “planetary scale”, for example from global warming. The Cold War is noted as encapsulating a conflict between two inclusive universalisms, the US and Soviet visions of the world. Buzan and Waever stress however that “universalist claims does not necessarily mean that the macrosecuritisation is in fact universal in terms of participation.”

The concept of macrosecuritisation and the associated emphasis on security constellations further developed securitisation theory by serving as a formal acknowledgement of the way in which different secuitisations can influence each other. By focusing on the evolution of securitisations, an element of process is introduced to the theory giving it added dynamism. Moreover through the study of macrosecuritisations a mechanism is provided through which analysts can examine how particular meta-narratives can frame and dominate the policy environment.

105 Idem.
106 Idem.
107 Idem.
108 Ibid., p. 264.
(1.5) Reorienting securitisation theory towards the ‘post-securitised environment’:

It is clear that both the specific conceptualisation of security and the accompanying analytical framework securitisation theory encapsulates, offers a range of insights useful for this case study. Conceptually, the theory effectively recognises the performative power of security on the wider policy environment. The way in which through an articulation of a speech act there is a possibility that the wider environment in which policy emerges and is implemented can change, thus enabling emergency measures to be pursued, effectively captures how in the aftermath of terrorist attacks in the US on 11 September 2001, both foreign and domestic policy was increasingly framed by responses to international terrorism. Securitisation theory then both demands, and provides a defining logic - existential threat - to locate the work done by verbal communication. For example, when President George W. Bush in his address to the nation on 11 September 2001 referred to the terrorist attacks as an attack “on our way of life, our very freedom”, his choice of words were not simply descriptive. Rather they were performative, representing an early attempt at highlighting a referent object whose survival was at stake: the ‘civilised way of life’. His decision to describe the response as a “war against terrorism”, rather say than to talk in terms of a crime, raised the prospect of military means being necessary, suggested a larger scale response was likely and emphasised the emergence of an ‘us versus them’ dichotomy.

---

109 This is a point advanced in (Ibid., p. 266) when they note “the exploitation by China, Russia and Israel of the alibi of fighting terror for agendas quite unrelated to the American one”.

110 This kind of analysis on responses to international terrorism can be seen in Sandra Silberstein, War of Words: language, politics and 9/11 (London: Routledge, 2004) and Richard Jackson, Writing the war on terrorism.
The Copenhagen School’s acknowledge that securitisations can become institutionalised, “finding expression in watch words that can be invoked to move specific issues into the realm of securitisation without elaborate arguments about the securityness of the specific case”,\textsuperscript{111} also emphasises the way a range of issues that have been linked to terrorism have immediately become security issues themselves. Moreover the recent work on macrosecuritisations and security constellations also adds something here effectively capturing the way in which both foreign and domestic policy and in a number of different states have been organised around the pursuit of a ‘war on terror’. Buzan and Waever note that while Russia and China might be “sceptical of the larger US world order strategy” [...] “the GWoT [Global War on Terror] is too attractive for them for local reasons not to be exploited”.\textsuperscript{112}

In a case study interested primarily in examining policy developments relating to UK maritime infrastructure, securitisation theory also provides analysts with a clear and well-developed framework through which to analyse those developments. A presented existential threat, securitising actors, referent objects and audience acceptance, all underpinned with a range of facilitating conditions, serve as useful signs with which security research can be structured. Related to this it is possible to utilise this analytical framework without explicitly sharing/rejecting the conclusion drawn in the school’s main text ‘Security: A New Framework for Analysis’, that

\footnotesize{


\textsuperscript{112} Buzan and Waever, ‘Macrosecuritisation and security constellations’, p. 274.
}
Securitisation is a “failure of ordinary politics”. Here the school argues that issues should be moved away from the all or nothing logic of existential threat and survival towards the less divisive, discussion driven political realm where threats can be turned into challenges. In short then there is no demand placed on the analyst to state whether they believe securitisation is positive or negative at the outset of research in order to be able to use the theory to study security. In this case study the relatively clear separation between undertaking analysis and engaging explicitly with normative questions about whether securitisation is positive or negative is maintained.

Securitisation theory effectively captures the policy environment in which the ‘war on terror’ has come to shape an increasing range of foreign and domestic policy. As it has already been noted securitisation is witnessed when an existential threat is argued and gains “enough resonance for a platform to made from which it is possible to legitimize emergency measures or other steps that would not have been possible had the discourse not taken the form of existential threats, point of no return, and necessity”. Yet beyond rather general pronouncements that the emergency measures may result in the revocation, suspension and/or circumnavigation of normal rules of engagement, the Copenhagen School tell us very little about what can be described as the ‘post-securitised environment’.

---


115 Ibid., p. 25.

More widely in comparison to the amount of literature focusing on how an issue has specifically been securitised or on debates about whether securitisation is a good or bad thing, there has been relatively little emphasis on examining the post-securitised environment. In short, securitisation theory can tell us how UK maritime infrastructure came to be securitised as part of the ‘war on terror’ but places relatively little attention on elaborating what securitisations ‘do’ in practice, engaging in the substantive policy analysis inherent in such a move.

There is a requirement to reorient research emphasis towards the post-securitised environment and on to implementation, addressing these shortcomings and therefore deepening securitisation theory. The reorientation does not involve any departure from the school’s conceptualisation of security as being constructed discursively, nor from the theory’s defining logic of existential threat/survival. The other central components for securitisation – securitising actors, referent object, facilitating conditions – also remain unchanged. The flexibility of being able to reorient research emphasis without fundamentally undermining the core components of securitisation theory is arguably another one of its strengths.

The reorientation involves the analyst utilising securitisation theory as it currently stands before moving on to elaborate the specific content of resultant emergency

---


118 One notable exception is Paul Roe’s article, ‘Actor, Audience(s) and Emergency Measures: Securitization and the UK’s Decision to Invade Iraq’, Security Dialogue, 39:6 (2008), pp. 615-635.

119 It is envisaged that failed securitisations also have an impact on practice. However this will not be discussed in this case study primarily because securitisation is witnessed here and also due to the limits of space in one study.
measures, explaining how they are delivered along the policy chain and discussing what impact they have on day-to-day activities. The phrase ‘emergency measures’ is the Copenhagen School’s and encapsulates those policies pursued to tackle a presented existential threat. The sense of ‘emergency’ then stems as much from the context in which those policies emerge with the sense of necessity, alongside the grounds on which they may subsequently be justified and defended, than it does from the content of the policies themselves. This focus on the content of emergency measures, their delivery and subsequent impact can collectively be understood as an examination of the totality of the counter-terrorism security response. To illustrate with an example, while the deployment of tanks by the British government at Heathrow Airport in February 2003 was justified as a necessary response to a possible terrorist threat; the preparations made prior to deployment, what impact those tanks had on day-to-day activities when at the airport, and the implications of the deployment on, say, the public’s view of the military, are just three things that would be of interest to analysts keen to focus on what securitisations do.¹²⁰

The reorientation of emphasis towards the post-securitised environment also provides a means through which it becomes possible to examine the relationship between discourse and practice in greater detail. Resting on an acknowledgement that securitisation is more process than moment, it is possible for example to chart how securitisations evolve as emergency measures are implemented. This can help to better understand whether the pursuit of particular policies ultimately reinforce or undermine the facilitating idea that a referent object is existentially threatened and

elaborate how a securitisation becomes institutionalised.121 Alongside this, by placing greater emphasis on implementation a wider pool of information becomes available with which to draw conclusions on the wider implications of securitisations on issues such as civil liberties, thus facilitating a more informed judgement about the extent to which a securitisation is positive or negative. A brief example here can illustrate. Securitisation theory without reorientation can help analysts to understand how it became possible that the British government decided to utilise Belmarsh Prison in London to hold a number of foreign nationals suspected of terrorism in December 2001 without charge or trial, but it is only through examining how this decision was delivered along the policy chain, charting what reaction it received from various agents and noting what impact that reaction had on the practice itself, that we can more fully grasp the significance of securitisation.

The reorientation of emphasis towards the post-securitised environment can be summarised with the help of the following figure:

---
Here then, through discourse, securitising actors present to an audience the argument that a referent object is existentially threatened by a particular threat and is thus in need of securing – the securitising moves. If both internal and external facilitating conditions are met, then audience acceptance follows resulting in securitisation as the implementation of emergency measures are understood to be a necessity in order to deliver security for the referent object. At this point then a shift in policy trajectory can take place as those policies pursued prior to the presentation of existential threat are deemed to be inappropriate to deal with the situation as it currently stands. In short, the environment in which policy emerges has changed as expectations and requirements have changed.
A shift in emphasis on to the post-securitised environment places greatest focus on examining those emergency measures implemented as a result of this shift in policy trajectory. Here focus falls on highlighting the specific narratives which draw upon the securitisation, further distilling the presented threat in order to justify specific emergency measures. The content, delivery and impact on a day-to-day basis of the emergency measures is charted, this can subsequently enable the wider implications for say, civil liberties to be more fully highlighted. The reference to ‘policy reflection’ in the figure recognises the element of process to securitisation. It is an acknowledgement of how, during the implementation of emergency measures, like policy generally, those doing the implementation reflect on progress, which can subsequently shape which elements of the presented threat are specifically emphasised, which in turn shapes the content and delivery of emergency measures thereafter in a continual cycle. It is envisaged that by focusing on this reflection that any resistance can be highlighted.

The need for reorientation is also captured in the core research questions that were first set out in the introduction to this thesis. The first question, ‘How has UK maritime infrastructure been securitised in the context of responses to international terrorism?’, encapsulates the case study’s starting assumption that the UK’s ports and harbours have been successfully presented in public discourse as needing ‘securing’ in relation to the threat posed by international terrorism. The question demands that attention falls on elaborating just how this has taken place over a

sustained period of time (highlighting the policy environment), shedding light on the specific speech acts articulated, by whom, to whom and if any resistance was noticeable. Addressing the second question, ‘What has been the impact of securitisation on the management of UK maritime infrastructure?’ is the primary research objective. It explicitly shifts the research emphasis on to the counter-terrorism security response relating to that infrastructure, telling us more about what securitising moves ‘do’ in practice.

(1.6) The Copenhagen School’s securitisation theory and its critics:

Despite the proposed reorientation of emphasis there remain criticisms that have been lodged against securitisation theory which have implications for this case study and as such need to be examined.\textsuperscript{123} The first is that securitisation theory is, in various ways, underdeveloped and as such is not fit for purpose as an analytical framework with which to gain a complete picture as to how security is socially constructed. In particular critics argue securitisation theory rests on an understanding of discourse that is too ‘thin’, while also suggesting that the exact role played by the audience remains unclear. The former criticism stems from the view that the theory’s emphasis on the role the spoken word (the speech act) plays in the construction of

\textsuperscript{123} It is worth noting that securitisation theory has been critiqued on other grounds to those listed here, but which more clearly have no bearing on the theory’s use in this case study. For example the theory has been criticised for being restrained by a Westphalian Straitjacket, an “assumption that ‘European’ or, more accurately, the Euro-American mode of the state and the accompanying political culture is valid globally”, Wilkinson, ‘The Copenhagen School on Tour in Kyrgyzstan’, p. 7. Here of course the case study is interested in developments in a European country, while securitisation theory has actually been utilised in a non-Euro-American context. See Nicole Jackson, ‘International Organizations, Security Dichotomies and the Trafficking of Persons and Narcotics in Post-Soviet Central Asia: A critique of the Securitization framework’, \textit{Security Dialogue}, 37:3 (2006), pp. 299-317 and Juha A. Vuori, ‘Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders’, \textit{European Journal of International Relations}, 14:1 (2008), pp. 65-99.
security is inadequate “for understanding processes of contemporary political communication in an age when that communication is increasingly conveyed through electronic media, and in which televisual images play an increasingly significant role”. For scholars such as Lene Hansen then, securitisation theory needs to be taken from the word to the image if it is to maintain its relevance. Utilising the example of the Danish cartoon controversy in 2005 she argues for an increased awareness of the securitising potential of images.

Although the Copenhagen School do argue that it is the grammatical structure of “existential threat, point of no return, and a possible way out” which characteristics the speech act, and that it “is not defined by uttering the word security” alone, they fail to elaborate how this relates to different forms of visual communication. That said it remains accurate to argue that it is often largely through the spoken word that the visual is, at least initially, distilled and given wider meaning. For example, while there is little doubt that the images of the Twin Towers burning and collapsing on 11 September 2001 fulfilled the old adage ‘a picture paints a thousand words’, it was arguably through verbal communication those images were linked to the idea of a ‘war on terror’. As a result, although Hansen is right to highlight the need to consider the role of the image in securitisation, the School’s relative lack of focus here does not render the theory irrelevant. Ultimately


127 Ibid., p. 27.
the Copenhagen school embrace the conceptualisation of ‘language as discourse’, while a relatively thin conceptualisation, it has to some extent been utilised by a range of different security scholars.128 Here discourses are understood as “related sets of ideas expressed [in language] in a variety of places by those with social power and are reproduced by others with power and those without”.129 Securitising actors then are regarded as having social power and audiences less so. Language as discourse is as Stuart Croft notes “not simply about representing the world; it is concerned with treating it as a form of social action”.130 This then captures the performance in securitisation and the idea that security is socially constructed more generally.

In this case study, to chart how UK maritime infrastructure has been securitised, attention will first be placed on examining the language deployed by securitising actors in their public statements. This remains of central importance in setting the wider policy environment in which emergency measures are legitimised. However the reorientation of emphasis towards the post-securitised environment and onto the implementation of those measures opens up the space in which both the written word and images may also be examined. For example it is envisaged that charting the delivery of emergency measures will involve attention falling on outlining how those measures are elaborated and justified along the policy chain. Such delivery is likely to involve the development of publications (including images) that seek to elaborate

128 Campbell, Writing security; and Jackson, Writing the war on terrorism.


130 Ibid., p. 43.
an emergency measure and justify its introduction, which in turn reiterate the securitisation itself. In short then different mediums will be considered but only as part of the focus on implementation. It will be a process then which is led by the specific practices under scrutiny. In doing this, Hansen’s criticism is acknowledged, and the role of images in securitisation is deemed to be worthy of consideration.

The criticism that the role of the audience remains under-developed, has been most powerfully expressed by Thierry Balzacq. In his article ‘The Three Faces of Securitization’ Balzacq goes as far to argue that security cannot be “at one and the same time a self-referential activity as it is an inter-subjective process”, challenging the very coherence of the theory. Balzacq’s argument is grounded on the view that if security is a self-referential activity then there would be no requirement for a securitising move to be accepted at all. He concludes that either the “acquiescence of the audience” is forsaken or “we abandon self-referentiality”, suggesting that the Copenhagen School would favour the former option because “its framework ignores that audience”.

While it is true the specific role of the audience is underdeveloped in comparison to other components of securitisation theory, the Copenhagen School do list the internal and external facilitating conditions (outlined earlier) which are required if a securitising move is to gain audience acceptance. There is a difference between a component of a framework being underdeveloped and it being ignored and as such


132 All taken from Ibid., p. 177.
Balzacq’s criticism is somewhat misplaced. Moreover, Balzacq’s argument that security as a self-referential activity and an inter-subjective process are mutually exclusive is wrong. It is through negotiation and contestation securitising actors and their audience reach a common understanding that a specific referent object is existentially threatened by a particular threat, which then legitimises emergency measures. Yet this process still does not mean that a real existential threat exists, rather it is through the reiteration of this agreed discourse something becomes a security issue. It is possible then that security can at one and the same time be a “self-referential activity as it is an inter-subjective process”.

Nevertheless, in this case study the reorientation of emphasis does offer the opportunity to deepen understanding of audience acceptance. By focusing on implementation, a loosening of what Matt McDonald argues is the theory’s over-emphasis on the moment of intervention takes place. Assessing the extent of audience acceptance, and thus securitisation, is notoriously difficult to do, but the Copenhagen School place the greatest onus on the analyst. The result is that a framework, clearly expressed and consistently utilised, is required to be set out through which acceptance can be located. Here then audience acceptance is understood to be evident in three main ways. First, if securitising discourses are consistently deployed by securitising actors over time it is assumed that this is because the audience accept that the presented threat remains salient and is

---

133 Ibid., p. 179.


understood. This clearly represents a more implicit form of audience acceptance. A second more explicit form of acceptance is witnessed in the expression of support for securitisation, particularly through the reproduction of securitising discourses by the audience. The third and clearest sign of audience acceptance is the implementation of emergency measures themselves, suggesting a point has been reached whereby the measures are deemed legitimate. All three signs don’t have to be evident at one time, but the more that are, the more certain an analyst can be of audience acceptance. The envisaged audience in this case study is elaborated in the following section of this chapter.

With regards to resistance, ultimately an audience’s position vis-à-vis securitisation can become sedimented but is never fixed. Resistance is always possible and reinforcement may be necessary. Securitisation may squeeze the space for discussion, but it does not eradicate it. Resistance is understood to be an overt challenge in this case study, and can be directed at different targets. As securitisation is socially constructed it is of little surprise that resistance may emerge against securitising discourses themselves. Yet it may also be directed at particular elements of the counter-terrorism security response itself, over the content of particular emergency measures, how they have been delivered and the perceived negative impact of both. This resistance emerges out of a process of continual reflection over policy, included in Figure 1, as emphasis falls on assessing whether the counter-terrorism security response is working and what, if anything, should come next. This reflection can subsequently shape both discourse and practice. How these different

136 This is one of the two external facilitating conditions the Copenhagen School acknowledge. Ibid., p. 33.
forms of resistance interact, and what impact they have, is something that will become evident during the case study.

Alongside the accusations of underdevelopment, the second line of critique with implications for this case study is that securitisation theory is too conservative. One argument advanced here is that the logic of security encapsulated in the theory, described as being “associated with secrecy, urgency and ‘panic politics’ [...] is actually quite ‘unconstructivist’ in the sense that it is positioned as relatively fixed and inevitable”.\textsuperscript{137} This is a position particularly held by those, like the Welsh School, who seek emancipation through security.\textsuperscript{138} Alongside this the charge of conservatism also emerges from those who argue that securitisation theory’s emphasis on the mid-level of referent objects and their requirement that a securitising actor must “be in a position of authority”,\textsuperscript{139} reifies the role of the state and risks “further silencing those already marginalised from security debates”.\textsuperscript{140} The implications of this perceived conservatism is that securitisation theory once again fails to fully capture how security is socially constructed, while those who use the theory are content with a particular view of security and are not interested in bringing about wider structural change.

\textsuperscript{137} McDonald in Williams: \textit{Security Studies: An Introduction}, p. 71.

\textsuperscript{138} This argument follows similar lines to that advanced by Bill McSweeney in \textit{Security, Identity and Interests: a sociology of international relations} (Cambridge: New York: Cambridge University Press, 1999) where he argues that the Copenhagen School’s notion of societal security is undermined because it overestimates the cohesion and stability of identity.

\textsuperscript{139} Ibid., p. 40.

The Copenhagen school describe themselves as “radically constructivist regarding security” and while self-labelling does not represent a satisfactory defence, the theory’s rejection of the idea that security can be boiled down to a list of objective threats and rather is constructed discursively represents a clear departure from the conceptualisation of security as a fixed, objective condition as elaborated by structural realists. It is important then to recognise where securitisation theory is very much constructivist in its leanings. Although it is the case that the logic of security encapsulated in securitisation theory is consistently understood in terms of emergency, the School does not stipulate in great detail what this actually means in practice, in part the justification for the reorientation of research emphasis in the first place.

A distinction then can be raised between saying overall that a general result emerges (the politics of emergency) out of securitisation and that the specific nature of that emergency (its impact and implications) is fixed. Indeed there is no reason to think it is fixed. This case study provides an opportunity to examine how the counter-terrorism security response evolves over time. Finally, a starting assumption of this thesis is that the politics of emergency have been increasingly evident in relation to the management of UK maritime infrastructure. There has been more urgency, the level and scope of policy discussion has been somewhat restricted and practices have been implemented that could not have realistically been envisaged prior to securitisation taking place. As such the Copenhagen school’s understanding of the

---

logic of security is appropriate to the case under scrutiny. The requirement in subsequent chapters is to illustrate this.

The second implication – that those who utilise securitisation theory are not interested in bringing about structural change - is ultimately not a concern for this case study. As it was noted earlier, the reorientation of emphasis towards the post-securitising environment and on to implementation is designed to facilitate a more complete understanding of what securitisations ‘do’. Reorientation will facilitate an examination of the way in which securitising discourses are reproduced more widely, but the central focus is on practice. Passing judgement then on the merits of securitisation, the role of the state and the possible marginalisation of other voices is something that may be facilitated with the findings that emerge out of this case study, but is not a primary objective due in large part to research practicalities. Ultimately, as it was noted earlier, while the Copenhagen school do discuss the state and political leaders a lot in their work, the school sees no reason why other referent objects and securitising actors cannot emerge. Despite all this, in the conclusion to the case study wider implications of those developments examined will be noted and future research avenues highlighted.
(1.7) *The case study – the securitisation of the UK’s maritime infrastructure:*

This elaboration of some of the criticisms levelled at securitisation theory serves as a reminder that no theory can ever satisfy all the demands placed upon it. The Copenhagen school are pragmatic enough to acknowledge the theory must evolve.\(^{142}\) As Claire Wilkinson has commented, “even opponents [...] have conceded that the ‘spirit’ of the School is to invite and open up the discussion of security rather than to entrench into fortified positions”.\(^{143}\) With the relevant criticisms considered then and their limited impact on the case study outlined, it is now possible to set out the parameters of the case study in relation to the theory, before proceeding finally to discuss the research methods that will be used and sources utilised.

The case study focuses on the five year period between 1 July 2004 and 30 June 2009. Recognising the primary interest in reorienting emphasis towards the post-securitised environment and on to implementation, the starting date enables an examination to take place of developments in the immediate aftermath of the date the International Ship and Port Facility Security (ISPS) code came in to force in the UK.\(^{144}\) Driven forward by the International Maritime Organization (IMO) in the aftermath of the terrorist attacks in the US on 11 September 2001, the ISPS code represented the clearest manifestation in practice of the acceptance of the need to

\(^{142}\) This can be seen in the way the school introduced ‘audience acceptance’ to the theory in Buzan, Waever & de Wilde, *Security: A New Framework for Analysis* and the introduction of the concept of macrosecuritisation in Buzan & Weaver, ‘Macrosecuritisation and security constellations’.


secure maritime infrastructure internationally in the context of responses to international terrorism before the case study period. In short it was the central emergency measure with relevance to maritime infrastructure internationally and within the UK that emerged out of the securitised environment constructed in the aftermath of the terrorist attacks in the US. The subsequent five years were also a period of intense incident, with amongst other things, the terrorist attacks in London on 7 July 2005 and the change of Prime Minister in the UK in the summer of 2007, all of which shaped the response to international terrorism.

When considering the first core research question the assumption is made that the calls to secure UK maritime infrastructure were bound up in a ‘mutually reinforcing relationship’ with the macrosecuritisation of the ‘civilised way of life’. Here a macro-level referent object, the ‘civilised way of life’, described as encapsulating democracy, economic prosperity and individual liberty, was successfully presented as being existentially threatened by a macro-level threat, international terrorism, thus facilitating a counter-terrorism security response. The securitising actors in this macrosecuritisation were political leaders internationally, most prominently including high-profile members of the administration of George W. Bush and in relation to the UK, the governments of both Tony Blair and Gordon Brown. It is these representatives of the state whom have historically been endowed with the authority to develop and speak policy on behalf of the general population. It is envisaged that there were two audiences who were appealed to and who legitimised the macrosecuritisation. On the one hand, the national policy networks specifically constructed with the responsibility for the counter-terrorism security response, and
on the other hand the general public to whom governments must appeal for support for their decisions.\textsuperscript{145}

This macrosecuritisation was captured in the ‘war on terror’ discourse of counter-terrorism, a discourse that incorporated the presentation of international terrorism as being existentially threatening to the ‘civilised way of life’, and then framed counter-terrorism efforts as necessary and inevitable, as a Manichean battle between good and evil, fought in an effort to secure that ‘civilised way of life’ – the good. In the UK this resulted in both foreign and domestic policy in a range of areas increasingly being framed by counter-terrorism considerations, such as military operations in Afghanistan and the expansion of pre-charge detention powers. These moves in turn served to reinforce the macrosecuritisation itself. UK maritime infrastructure has been securitised in this context, in the pursuit of a ‘war on terror’.

More specifically UK maritime infrastructure can be understood as a ‘site of securitisation’.\textsuperscript{146} This comes from an acknowledgement that ports and harbours are ultimately geographic spaces in which buildings and equipment (assets) can be

\textsuperscript{145} Here the Copenhagen School’s view (Buzan, Waever & de Wilde, \textit{Security: A New Framework for Analysis}, p. 34) that “attempted securitizers are ‘judged’ first by other social actors and citizens” is taken in to account to help determine the audiences.


62
located and a series of activities take place.\textsuperscript{147} The idea that a geographic space where everyone, everything, and all activities associated with it, can be increasingly positioned as requiring ‘securing’ against presented threats with the associated policy implications, is effectively captured by Natalie Bormann and Michael Sheehan in their work on outer space. Here for example they note how “the deployment of technologies with the aim to secure, safeguard, defend, and control certain assets, innovations and activities in space is presented to us as an inevitable and necessary development”.\textsuperscript{148}

It is envisaged that two main narratives have been produced and reproduced which draw upon the macrosecuritisation and capture the presented international terrorist threat in relation to UK maritime infrastructure. On occasion it can even be difficult to fully differentiate between the narratives. In the first maritime infrastructure is presented as a possible ‘target’ of international terrorism. Here the spectre is raised that the failure to adequately secure maritime infrastructure risks its survival operationally should terrorists attack, and as such an attack on maritime infrastructure serves as a means through which the ‘civilised way of life’ is threatened. Maritime infrastructure’s importance, say to the wider economic prosperity then is noted. In the second narrative maritime infrastructure is described as a ‘vulnerable node’ that terrorists could exploit, thus extenuating the existential threat to the ‘civilised way of life’. Here then maritime infrastructure requires

\textsuperscript{147} To reiterate, in this thesis a ‘port’ is understood to be a location at which facilities are in place for a vessel to be loaded and unloaded. A port then is understood to be generally larger than a ‘harbour’, a place at which generally smaller vessels may dock and/or be stored. There are both artificial and natural harbours.

securing to prevent exploitation and the possibility of attacks elsewhere. Both narratives rest on maritime infrastructure being regarded as an example of critical national infrastructure understood as one part of the wider supply chain, transport network and UK border.

Acknowledging the multi-levelled governance of UK maritime infrastructure emerging out of UK membership of organisations such as the IMO and EU, it is anticipated that these narratives have been produced by all those political leaders with some responsibility for policy relating to UK maritime infrastructure who have constructed a community of concern through emphasising the dangers inherent in lax coastal vigilance. The case study will also examine the extent to which these narratives have also been reproduced and even resisted by the rest of the specific policy network responsible for the counter-terrorism security response relating to UK maritime infrastructure, and more widely still by the maritime media such as the newspaper Lloyd’s List.

This thesis understands ‘policy network’ as referring “to the set of political actors inside and outside government who are involved in, or take an interest in, the making of public policy, and/or relations between these actors”.  


network relating to UK maritime infrastructure includes those political leaders noted earlier, alongside parliamentarians, civil servants, security professionals both state and privately funded such as the police (particularly Special Branch ports officers) and port private security guards, and the maritime industry as a whole, especially port owners and their senior management teams; all with an interest in and some responsibility for the counter-terrorism security response relating to UK maritime infrastructure.\(^{151}\)

Intelligence Services, specifically the UK Security Service (MI5), are additional examples of state security professionals and as such are also part of the policy network. However, as their work by its very nature remains highly secretive it was not open to direct examination in this thesis.\(^ {152}\) The members of this specific policy network form part of those wider policy networks that can be said to be responsible for counter-terrorism efforts as a whole, beyond UK maritime infrastructure, and

\(^{151}\) The reference to ‘security professionals’ here is simply a generic term utilised to capture all those, both state and privately funded, who’s primary responsibility is the maintenance of security.

which have been highlighted as one of the audiences for the macrosecuritisation of the ‘civilised way of life’. To avoid confusion however, the use of the phrase policy network in the three chapters which make up the case study refers specifically to those with responsibilities relating to UK maritime infrastructure security.

When considering the second core research question which most clearly represents the desired reorientation of research emphasis towards the post-securitised environment and on to implementation, the five year focus of the case study is subdivided further into three periods of time: 1 July 2004 to 6 July 2005, 7 July 2005 to 26 June 2007 and 27 June 2007 to 30 June 2009. The first represents the 12 months after the ISPS code formally came in to force in the UK. The second encapsulates the immediate aftermath of the terrorist attacks on London up to the transfer of power from Tony Blair to Gordon Brown. The third charts the first two years of the Brown premiership and includes notable incidents such as the terrorist attacks on Glasgow airport.

With an interest in the post-securitised environment and thus the counter-terrorism security response (the content of emergency measures, their delivery and impact on day-to-day activities), it is practice which serves as the focal point of the case study. Here the totality of counter-terrorism practice is sub-divided in to three broad constituent parts in order to more effectively highlight trends. The first part - ‘legislation and regulations’ – includes those documents laid down in law which introduced or framed particular emergency measures relating to UK maritime infrastructure. The second part - ‘institutional developments and infrastructure
changes’ – often, though not always, emerge as a result of the requirements laid down in new legislation and regulations. Institutional developments are understood as those changes in the institutional structures that are put in place to implement emergency measures.

Representing then the way in which members of the policy network are organised, attention is placed on charting the creation and operation of new agencies, working groups and committees, to name three examples. Infrastructure changes on the other hand encapsulate those material changes deemed to be necessary to secure UK maritime infrastructure. This includes physical changes within the maritime infrastructure itself, through say, the construction of new fencing, and the development and use of new technologies to maintain security procedures. The third part - ‘working practices’ – includes those day-to-day practices undertaken by members of the policy network, many of which have emerged as a result of the other components. One such set of working practices are those security training programmes undertaken by those working within UK maritime infrastructure.

Here, as with the three periods of time, some cross-over between each part is expected, whilst implementation is assumed to take place at multi-levels of governance, particularly in relation to the initiation of legislation and regulations. Developments relating to three cases of UK maritime infrastructure are specifically utilised to add even further depth to the examination. The UK has approximately 650 ports and harbours that have statutory powers, of which around 120 are deemed to be
commercially active.153 In 2004 the UK ports industry handled 573 million tonnes of foreign and domestic traffic, the largest in Europe in terms of freight tonnage.154 There are three main types of port in the UK. Private ports account for 70% of UK port capacity and are those ports where the private sector own the land, facilities and control nearly all port services and regulatory functions.155 Trust ports account for a large number of UK ports and are established by acts of Parliament and are “controlled and administered by […] self-governing independent statutory” bodies.156 Finally there are a number of municipal ports whereby the local authority may act as landlord with some private tenants.157

Inevitably due to scale of the industry, research practicalities prevent operations at every port and harbour being examined. As a result the Port of Felixstowe, the Port of Holyhead and the Port of Tilbury are selected for their position as leading examples of a UK container port, passenger terminal (including roll on-roll off Ferries) and mixed use port (dealing with containers, bulk carrier vessels and cruise liners) respectively.158 Undertaking the primary functions of UK ports, the use of


154 Idem.


156 Idem.


158 The Port of Tilbury is one of a number of facilities deemed to form part of the larger Port of London. The Port of London encapsulates all facilities along the Thames River, and each have different types of ownership. The
these three cases, which are all privately owned and operated, enable trends to be located across the industry. The inclusion of Holyhead also ensures that the case study is not focused geographically on the east coast of England in isolation. Adding to the variation then, the case of Holyhead also enables the case study to consider what impact, if any, the Common Travel Area (CTA) between the UK and Republic of Ireland where some passport controls are waivered, and devolution in Wales, have had on the counter-terrorism security response. Holyhead then is not the largest by passenger volume of UK passenger terminals (with Dover holding that position), but its position in the top three, coupled with its location provide additional research opportunities by way of compensation.159

Beyond these reasons, the decision to focus on the three cases was also determined by available access to undertake the regular site visits and conduct those interviews with members of the policy network necessary to gain a fuller understanding of the impact of securitisation. After liaison with individuals at a senior level responsible for co-ordinating UK maritime infrastructure security, relationships were fostered facilitating access at particular sites. Acknowledging then both the restrictions of access that accompanies an examination of security practice, and the busy schedules of members of the policy network, it was decided to concentrate on getting to the point at which trust could be built to a sufficient level that multiple visits and interviews could take place, over time, to further deepen the examination.

Port of London Authority is responsible for the navigational of the Thames near Tilbury and the promotion of the river generally.

159 Information on the port’s prominence in terms of passenger numbers was ascertained during an interview conducted by the author.
Recognising the way however in which developments in one case at any one time can be more evident and take place at a greater pace than those in another case, alongside the need to maintain interviewee anonymity and certain levels of confidentiality with particular information collected, the case study does not examine each case in turn. Rather developments relating to each case are utilised both to highlight trends and provide concrete examples to illustrate them across the maritime industry in any one time period.

(1.8) Research methods and sources:

Each part of the case study will have a consistent structure to it. Initial attention falls on addressing the first core research question through an examination of how the mutually reinforcing relationship envisaged between the macrosecuritisation of the ‘civilised way of life’ and UK maritime infrastructure’s position as a site of securitisation is maintained over the specific time period. Emphasis is placed on determining the stability – understood in terms of a continuity of audience acceptance of securitising discourses with resilience to any resistance - of the ‘war on terror’ counter-terrorism discourse in which the macrosecuritisation is captured. Here the three signs of audience acceptance outlined earlier – the consistent deployment of securitising discourses by securitising actors, evidence of the reproduction of such discourses by the audience for the macrosecuritisation, and the implementation of emergency measures themselves will be highlighted. Becoming more specific, attention then falls on examining the production and reproduction of the two narratives that present the terrorist threat relating to UK maritime
infrastructure in this context. It is envisaged that due to the institutionalisation of the macrosecuritisation that the reiteration of watchwords such as ‘terrorism’ and ‘counter-terrorism’ capture the threat as presented to UK maritime infrastructure that underpins the narratives.

In terms of methods this requires an analysis of discourse to be undertaken. Recognising the language as discourse definition embraced earlier, both the spoken and written word will be analysed. The discourse analysis is conducted on three broad types of sources. The first is the official discourse of government and intergovernmental organisations, the second is the wider policy debate which takes place in Parliament and in the media and the third is what Lene Hansen describes as the marginal political discourses from non-governmental organisations and academia.

The selection of these sources is very much driven by working back from the practices themselves and analysing just how they emerged. The official sources encapsulate all legislation, regulations, reports and statements which relate to counter-terrorism and where maritime infrastructure is also referenced directly or indirectly. Predominantly found at the level of the UK national government, some sources can also be traced to non-UK organisations such as the IMO and the EU. Examples include the statement by Tony Blair on the policy implications of the July 2005 London terrorist attacks, the speech by the Secretary-General of the IMO reminding contracting states of their duties to implement the ISPS code fully, the EU

---


161 Lene Hansen, Security as Practice: discourse analysis and the Bosnian War, pp. 59-64.
regulation introducing ISPS code measures across the union and the Cabinet Office report on better securing the UK border.\footnote{Each of these examples will be discussed later in the thesis. For Blair’s statement see p. 201; for the Secretary-General’s speech see p. 122; for the EU regulation see p. 119 and for the Cabinet Office paper see p. 290.}

The second set of sources includes all relevant debates conducted in the context of the development of the previously outlined sources, alongside prominent media reports. Here particular attention is placed on Parliamentary Select Committee reports such as the one published by the Transport Committee on transport security in the aftermath of the July 2005 London terrorist attacks, and on publications closely associated with the maritime industry such as the newspaper ‘Lloyd’s List’.\footnote{A wide range of Lloyd’s List stories and additional media sources are utilised. The Transport Committee report noted here is raised on p. 209.} The media serves as a platform through which the two narratives may be reproduced both by reiterating the language of others and reiterating the presented terrorist threat themselves in, say editorials. These editorials then are also analysed. The third set of sources includes any relevant publications such as newsletters and reports from a number of non-government organisations and academia where maritime infrastructure security is discussed. This includes any publications by the owners of the three UK cases under scrutiny. The archives of the IMO proved to be a particularly useful site at which to locate many of these sources with six individual trips being taken for source collection.

Thinking about the second core research question and the reorientation of emphasis on to the post-securitised environment, any information relating to the implementation of emergency measures in relation to UK maritime infrastructure...
will also be located in these three sets of sources. Interest then is less on the presentation of threat and setting out the case for counter-terrorism and more on the details of the counter-terrorism security response. Focusing on institutional flow charts, organisational objectives and action plans, one example includes the EU regulation which sets out the objectives and powers of a pan-European port inspection programme designed to ensure ISPS code compliance.\footnote{This regulation is discussed on p. 161.} To further facilitate the reorientation a final set of sources more explicitly relating to policy implementation will also be turned to. These include internal memos, financial reports, company audits, official presentations and training programmes, once again including those developed by the owners of the three cases, alongside those developed by the local constabulary’s where they are situated. The first three sets of sources can be described as generally operating on the macro or big picture level, this fourth set of sources operate on a micro level.

This is complimented by material gained from a series of site visits undertaken, meetings attended and interviews conducted. The object here is to shed further light on the counter-terrorism security response and thus the impact of securitisation on the management of UK maritime infrastructure. Detailed site visits to each case took place in order to tour the infrastructure and to witness some security activities. Each of these visits lasted between two and three days. On at least one additional occasion return visits to the area around each case also took place, to conduct additional interviews, attend meetings, and in order to gain a greater feel for the maritime environment. It was during these visits that those photographs utilised in the case study were taken or provided by an interviewee. The use of photographs, such of
port search procedures in chapter three, is primarily to illustrate the impact of securitisation on day-to-day activities recognising the desired reorientation of research emphasis.

The interviews themselves were conducted with members of the policy network right along the policy chain including those responsible for the development of the broad contours of the counter-terrorism security response, such as senior civil servants and senior police officers, and those whose task it is to implement particular components of the response on the ground. Amongst the interviewees here were both public and private sector personnel such as police officers, port managers and trade union representatives. All in all 17 interviews were conducted, including a number of repeat interviews with individuals to gain further information. Where access was gained to confidential sources during the course of research, the insights provided are only used for deep background and not directly quoted or referenced in the main body of text. Equal care is also taken when dealing with interview material, specifically ‘off-record’ and ‘background only’ material (see Appendix A).

(1.9) Conclusion:

By placing the securitisation theory in its intellectual context, elaborating its core components and setting out how it will be utilised to address the core research questions, this first chapter provides the analytical framework through which counter-terrorism efforts in relation to UK maritime infrastructure in the context of responses to international terrorism can be more effectively examined. Specifically, it has been argued, the Copenhagen School’s conceptualisation of security as being
discursively constructed, primarily through the articulation and acceptance of speech acts, effectively captures the way in which concerns over international terrorism have increasingly influenced policy since September 2001. Their work on macrosecuritisations here is particularly insightful, while securitisation theory offers a set of useful signs with which security research can be structured. Moreover it is possible to utilise securitisation theory without actively embracing the Copenhagen School’s preference for desecuritisation.

By reorienting emphasis towards the post-securitising environment and on to implementation the chapter has also demonstrated how securitisation theory can be deepened without undermining the conceptualisation of security on which it is founded. The reorientation enables this case study to make a practical turn providing an opportunity to study what securitisations ‘do’ in practice, facilitating greater attention being placed on the content of emergency measures, how they are delivered, what impact they have on day-to-day activities, all of which offers the opportunity that the wider implications of securitisation, such as those relating to civil liberties, can be more fully examined.

The case study itself examines developments in the five year period between 1 July 2004 and 30 June 2009, the starting date representing the point at which the ISPS code, an emergency measure with significant impact on UK maritime infrastructure, came into force. The five year period is sub-divided in to three shorter periods of time to better enable trends to be located. Attention first falls on demonstrating how UK maritime infrastructure was a site of securitisation in a mutually reinforcing
relationship with the macrosecuritisation encapsulating the ‘civilised way of life’. Through a discourse analysis the case study will elaborate how securitising discourses were produced and subsequently reproduced, highlighting the process of reflection and any resistance where it is evident.

Recognising the desired reorientation the case study then undergoes a transition from examining discourse to examining practice, as emphasis is placed on the counter-terrorism security response. To provide additional focus the totality of counter-terrorism practice is sub-divided into three constituent parts: ‘legislation and regulations’, ‘institutional developments and infrastructure changes’, and ‘working practices’, while developments within the ports of Felixstowe, Holyhead and Tilbury are particularly highlighted. A combination of analysing policy delivery documents, undertaking site visits, attending meetings and conducting interviews with members of the policy network all enable the impact of securitisation on the management of UK maritime infrastructure to be fully assessed.

In the next chapter an effort is made to place the case study in its immediate historical context. First, the dominant discursive trends which framed policy both internationally and in the UK in the aftermath of the terrorist attacks on 11 September 2001 are elaborated. Here attention falls on explaining how the ‘civilised way of life’ was successfully presented as being existentially threatened by international terrorism, captured in the ‘war on terror’ discourse of counter-terrorism. The initial impact of this macrosecuritisation in the UK more generally is highlighted, with emphasis being placed on explaining how counter-terrorism efforts
increasingly took centre-stage, shaping more foreign and particularly domestic policy. With this complete, the chapter turns to maritime infrastructure and illustrates how in this context it was securitised as a site of securitisation. Here the introduction of the ISPS code is raised up as being the clearest manifestation in practice (an emergency measure) of this securitisation. By elaborating the introduction of the ISPS code and who was responsible for its initial implementation, it is possible to highlight the two main narratives produced and reproduced in relation to the presented threat and set out what initial impact it had on UK maritime infrastructure. Collectively then in terms of both discourse and practice, the chapter provides a point from which future developments can be compared.

Beyond chapter two, the following three chapters represent the main body of the case study as both core research questions are progressively tackled, first through an examination of discourse and then, primarily, through an examination of practice in a particular period of time. In chapter three attention falls on the way in which those practices associated with the ISPS code were further institutionalised within UK maritime infrastructure. The following chapter turns its attention to examining the way in which a proliferation of different emergency measures emerged in the aftermath of the terrorist attacks in London in July 2005, measures that demonstrated the continued pursuit of a ‘war on terror’ and associated securitisation of UK maritime infrastructure. In the final chapter the arrival of Gordon Brown as the new Prime Minister is shown to have no discernible impact on the securitisation of UK maritime infrastructure. Each chapter builds upon the last in order to provide additional detail over how, in this case, the post-securitised environment can be characterised.
Chapter Two

*Contextualising the case study: the ‘war on terror’ and the emergence of the ISPS code*

America and our friends and allies join with all those who want peace and security in the world, and we stand together to win the war against terrorism.\(^1\)

(President George W. Bush – Address to the Nation, 11 September 2001)

**(2.1) Introduction:**

The previous chapter made the case that the Copenhagen School’s securitisation theory offers an insightful and clear analytical framework with which the case study can be undertaken. In embracing the conceptualisation of security as being socially constructed, specifically through discourse, it was argued that securitisation theory captures the performative power of security on the policy environment effectively grasping how policy was increasingly justified on the basis of being a necessity, part of the wider response to an existential threat presented as being posed by international terrorism. Alongside this, the school’s concept of ‘macrosecuritisation’,

---

their acknowledgement that an audience legitimises emergency action and the well-established framework of ‘securitising actors’, ‘facilitating conditions’ and beyond that serve as signs to study security, were all highlighted to further justify the theory’s use. The chapter then made the case that by reorienting emphasis towards the post-securitised environment and on to implementation, focusing in greater depth on what securitisations do in practice, an even more complete examination of securitisation could be facilitated. The chapter drew to a close by discussing some of the criticisms levelled at securitisation theory, by providing further detail on how specifically the theory would be utilised, before setting out the methods that would be embraced and sources used in the study itself.

The central objective of this second chapter is to place the case study in its immediate historical context. In doing this the strengths of securitisation theory and its value for policy examination will be illustrated further, while a base point will be provided from which those trends both in terms of discourse and practice, highlighted in the case study, can be examined. The chapter first elaborates how, in the aftermath of the terrorist attacks on 11 September 2001, the ‘war on terror’ discourse of counter-terrorism came to increasingly frame both foreign and domestic policy, placing counter-terrorism considerations centre-stage. The ‘war on terror’ discourse rests on a particular understanding of the nature of the terrorist threat being faced and provides answers to questions as diverse as why the terrorist attacks took place, what the response should be, and why it is important.
More specifically the September 2001 terrorist attacks were framed as emerging ‘out of the blue’, as being representative of the start of a ‘new’ era in International Relations, characterised by a fundamentally different and new terrorist threat in its complexity, scale and resulting violence. As such, the ‘war on terror’ was presented as a necessity, a matter of survival and the honourable choice, increasingly becoming the raison d’état. Ultimately then, the chapter argues, the discourse captures the macrosecuritisation of the ‘civilised way of life’ as political leaders internationally presented that way of life - encapsulating democracy, individual liberty and economic prosperity - as being existentially threatened by international terrorism, and thus in need of securing.

With this complete and with both the reorientation of emphasis towards the post-securitised environment and an acknowledgement of the UK focus of the case study firmly in mind, the chapter elaborates in greater depth how the pursuit of the ‘war on terror’ impacted upon UK domestic counter-terrorism efforts in the immediate period after the September 2001 terrorist attacks. Here the case is advanced that counter-terrorism moved to the very top of the domestic policy agenda. There was a proliferation of counter-terrorism legislation introduced in the UK that resulted in an increase in state power. There was an emphasis on enhanced co-ordination in counter-terrorist efforts across the UK which led to a variety of institutional changes. Counter-terrorism budgets grew, whilst the work of security professionals gained a higher public profile. All of this was underpinned with a notable sense of urgency.
Focus then turns to UK maritime infrastructure, as the chapter argues that it is within this context that UK maritime infrastructure can be understood as being securitised, specifically as a ‘site of securitisation’. Attention primarily falls on the International Ship and Port Facility Security (ISPS) code, a prominent emergency measure that highlighted that very securitisation. Its initial implementation in the UK, from conception in the immediate aftermath of the September 2001 terrorist attacks up until the date it formally came in to force in the UK on 1 July 2004, is the subject of a more detailed examination. The chapter explains how, through the production and reproduction of two main narratives primarily by members of the policy network with a responsibility for the counter-terrorism security response in relation to UK maritime infrastructure, the threat to maritime infrastructure posed by international terrorism was presented creating the policy space in which the development of the ISPS code became possible.

The first narrative presented maritime infrastructure as a possible ‘target’ of international terrorism, whilst the second described the infrastructure as a ‘vulnerable node’ that could be exploited by international terrorists. In doing this the first steps towards demonstrating the mutually reinforcing relationship between macrosecuritisation and the securitisation of maritime infrastructure are made, while a greater understanding of the policy network, its members and multi-levelled structure is provided. The chapter concludes by shifting emphasis further from discourse to practice, focusing on the impact the initial implementation of the ISPS code had on day-to-day activities in UK maritime infrastructure through a brief assessment of the experiences of the three cases that form the basis of the case study – the ports of Felixstowe, Holyhead and Tilbury. Whilst further enhancing
knowledge of the policy network, this final section also enables those other counter-terrorism practices relating to UK maritime infrastructure which sat alongside the ISPS code to be noted, deepening contextual understanding further.

(2.2) The construction of the ‘war on terror’ discourse of counter-terrorism:

It was the pursuit of a ‘war on terror’ which represented the wider context in which UK maritime infrastructure was itself increasingly presented as requiring ‘securing’. The ‘war on terror’ emerged out of and became dominant as a discourse of counter-terrorism in large part because of the way in which the terrorist attacks in the United States (US) on 11 September 2001 were themselves presented.2 Most prominently by particular political leaders internationally, the attacks were presented as the manifestation of a terrorist threat which was more complex, larger in scale and inherently more violent than that which had been witnessed previously.3 As UK

---

2 There is of course no agreed definition of ‘terrorism’, although many make some reference to the threat and use of violence for political ends. This complexity around definition is acknowledged and discussed in texts such as Walter Laqueur, Terrorism (London: Weidenfeld and Nicolson, 1977), pp. 3-20; Bruce Hoffman, Inside Terrorism (New York: Columbia University Press, 2006), 2nd Edition, pp. 1-42 and Alex P. Schmid, ‘The Definition of Terrorism’, in Alex P. Schmid (ed.), The Routledge Handbook of Terrorism Research (Abingdon, Oxford: New York: Routledge, 2011), pp. 39-157. Despite this complexity this thesis seeks to demonstrate, starting in this sub-section, how a particular presentation of terrorist threat was made by political leaders and subsequently became widely accepted, captured in the ‘war on terror’ discourse. Here the presented threat was understood by virtue of its supposed nature (extremely violent and international in scope), its presented target (the ‘civilised way of life’) and whom the ‘enemy’ was deemed to be (Al Qaeda, Al Qaeda inspired individuals/groups and ‘rogue states’).

3 Discussions over supposedly ‘new’ terrorism were not particularly novel of course. John Gearson, ‘The Nature of Modern Terrorism’, in Lawrence Freedman (ed.), Superterrorism: policy responses (Oxford: Malden, MA.: Blackwell, 2002), pp. 7-24 outlines how, after the sarin attack on the Tokyo subway in 1995 in particular, discussion amongst practitioners and scholars increasingly turned to considering whether terrorists would utilise chemical and biological weapons representing a form of ‘superterrorism’. In Frank Furedi, The Expanding Empire of the Unknown (London: New York: Continuum, 2007), pp. 23-24, Furedi notes that discussions about a ‘new’ form of terrorism and the idea that a particular era of terrorism is upon us have their own genealogy and indeed represent something of a self-fulfilling prophecy. This sense that a new era had been brought about by the terrorist attacks in the US on September 11th 2001 was captured in the idea of an ‘Age of Terror’. For example the historian John Lewis Gaddis wrote that the attacks represented the end of the ‘post-cold war era’, commenting “from the moment they did happen, everyone acknowledged that everything had changed.” See John
Prime Minister Tony Blair summarised in the House of Commons on 14 September 2001:

Let us make this reflection too. A week ago, anyone suggesting that terrorists would kill thousands of innocent people in downtown New York would have been dismissed as alarmist, yet it happened. We know that these groups are fanatics, capable of killing without discrimination. The limits on the numbers that they kill and their methods of killing are not governed by any sense of morality. The limits are only practical and technical. We know, that they would, if they could, go further and use chemical, biological, or even nuclear weapons of mass destruction. We know, also, that there are groups of people, occasionally states, who will trade the technology and capability of such weapons.

Beyond the large-scale and inherent violence of the threat claimed by Blair here, its target was presented in particularly broad terms. Here as it was noted in the previous chapter, on 11 September 2001 itself, President George W. Bush presented the attacks as an attack “on our fellow citizens” and “on our way of life, our very freedom”, immediately projecting outwards their significance. This broad conceptualisation of what was being threatened – the referent object - was expanded further when the attacks were presented as not simply being an attack on an American way of life, but as an attack on a set of values more universal in reach. Again it was a presentation advanced by Tony Blair when he argued:

These attacks were not just attacks upon people and buildings; nor even merely upon the United States of America; these were attacks on the basic democratic values in which we all believe so passionately and on the civilised world. […]


But one thing should be very clear. By their acts, these terrorists and those behind them have made themselves the enemies of the entire civilised world.\textsuperscript{6}

The ‘civilised world’, characterised here by Blair as encapsulating democratic values, but arguably also associated with economic prosperity and individual liberty, was under attack by an enemy.

The move to frame the response to the terrorist attacks in the language of ‘war’ happened quickly. The phrase the ‘war against terrorism’ was first used by President Bush on 11 September 2001 itself, and the main characteristics of the ‘war on terror’ discourse were constructed over the following months, culminating in the reference to the ‘axis of evil’ in Bush’s State of the Union address in January 2002.\textsuperscript{7} At its core the ‘war on terror’ was presented as a Manichean battle between good and evil, fought in an effort to secure the ‘civilised way of life’. The discourse then was characterised by a dualism, the separation of the international community into two diametrically opposing sides, which in turn helped to facilitate and sustain the notion of ‘war’. Bush, for example, suggested that states were “either with us or against us in the fight against terror”, while Blair warned that “those who harbour or help them [here Al Qaeda] have a choice: either to cease their protection of our enemies or be

\textsuperscript{6} Tony Blair, ‘International Terrorism and Attacks in the USA’, House of Commons, 14 September 2001, Hansard columns 604 and 605.

treated as an enemy themselves”. This dualism also alluded to the way in which the presented threat posed to the ‘civilised way of life’ by international terrorism was understood in existential terms, there was to be no room for compromise.

Somewhat paradoxically however, in the immediate aftermath of 11 September 2001, the ‘war’ was also presented as being something of a pre-emptive move; as the mechanism which would ensure that the existential threat did not fully materialise in reality in the first place. As President Bush told Congress on 20 September 2001:

> After all that has just passed – all the lives taken, and all the possibilities and hopes that died with them – it is natural to wonder if America’s future is one of fear. Some speak of an age of terror. I know there are struggles ahead, and dangers to face. But this country will define our times, not be defined by them. As long as the United States of America is determined and strong, this will not be an age of terror; this will be an age of liberty, here and across the world.⁹

This paradox can, to a large extent be explained by the inevitable changes of argument and contradictions which emerge as understandings of events such as the terrorist attacks on 11 September 2001 are inter-subjectively constructed. By embracing the conceptualisation of security as socially constructed it is acknowledged that public policy is neither developed nor delivered in a vacuum, but rather is framed by specific considerations, ideas and norms, often competing with

---


each other at any one time. These are all encapsulated and communicated in
discourse and these discursive moves subsequently structure social relations, policy
and our understandings of identity.

Despite its relatively rapid construction there was nothing inevitable about the
emergence and subsequent dominance of this discourse of counter-terrorism. As
Stuart Croft summarises, the attacks could have been understood, amongst other
ways, as a failure of the American state to protect its citizens, provoking even greater
self-reflection than already took place.\(^\text{10}\) They could have been framed as the
moment that the American Arab and Muslim communities betrayed their own
country or they could have been framed predominantly as a criminal act, thus leading
to greater emphasis on undertaking evidence gathering and so forth. Each would
have differed quite markedly both in tone and resulting impact from the arguably
more emotive, less nuanced emphasis on ‘war’ with its heightened sense of
emergency.\(^\text{11}\)

Examining why this specific discourse emerged and how it gained dominance is
largely beyond the scope of this chapter. The influence of neo-conservative ideology
within the US administration and the strong religious views of prominent world
leaders have been offered as two possible answers to the first question.\(^\text{12}\) Addressing

\(^\text{10}\) This self-reflection in the US was most clearly evident in the work and subsequent publication of the ‘9/11
Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton &
Co., 2004).

\(^\text{11}\) Stuart Croft, *Culture, Crisis and America’s War on Terror*, pp. 113-115.

\(^\text{12}\) Bush and Blair set out their arguments with considerable ‘certainty’. Such ‘certainty’ in International Relations
has been elaborated and critiqued by Jenny Edkins and Maja Zehfuss in their paper, ‘Generalising the
the latter question arguably rests, in part at least, on the fact that the ‘war on terror’
built upon previous, already utilised and understood discursive efforts, such a
dominant discourse did not simply emerge from nowhere. There is a long genealogy
to the argument that good and evil are in conflict with each other, that the threat of
terrorism is particularly vicious and that the ‘civilised world’ is existentially
threatened as a result, even if the speed of the deployment of these ideas was faster
and the scale of their impact considerably greater on this occasion.\(^{13}\)

Ultimately the ‘war on terror’ counter-terrorism discourse captured a
macrosecuritisation. Here a macro-level referent object, the ‘civilised way of life’
was presented as being existentially threatened by a macro-level threat, ‘international
terrorism’. The events of 11 September 2001 were understood as a point of no return
and subsequently emergency action was presented and accepted as a necessity, an
inevitable response to the threat posed, it was a matter of survival. With this came a
sense that constant vigilance and no complacency with regards to the presented
threat were essential if that threat was to be tackled and the referent object secured. If
western political leaders internationally, most prominently in the US and UK, were
the securitising actors making the presentation of an existential threat, then their
audience was made up of the national policy networks specifically constructed with

\(^{13}\) For a discussion of such a genealogy see Joseba Zulaika and William A Douglass, *Terror and taboo: the
the war on terrorism*, pp. 154-159; and Frank Furedi, *Invitation to Terror*, pp. 23-24.
the responsibility for the counter-terrorism security response, and the general public to whom governments must appeal for support for their decisions.\footnote{The US/UK relationship is particularly close and has long been the subject of debate. For a good background text on the relationship see John Dumbrell, *A Special Relationship: Anglo-American relations from the Cold War to Iraq* (Houndmills, Basingstoke, Hampshire: New York: Palgrave MacMillan, 2006), 2nd edition. For a more overtly political text in support of the partnership see Robin Harris, *Beyond Friendship – The Future of Anglo-American Relations*, (The Heritage Foundation, 2006). Beyond President Bush, other political leaders within the US reproduced the ‘war on terror’ discourse. Richard Jackson includes a copy of a number of speeches from the Bush administration in *Writing the war on terrorism*, appendix. There was also reproduction by other members of the UK cabinet which will be discussed later in the chapter. Beyond the US and UK, political leaders in a number of states also latched on to the discourse. For more information see Barry Buzan and Ole Waever, ‘Macrosecuritisation and security constellations: reconsidering scale in securitisation theory’, *Review of International Studies*, 35:2 (2009), pp. 253-276 and for a detailed assessment of the impact of the ‘war on terror’ in four different states see Clive Jones, ‘Israel and the al-Aqsa intifada: the Conceptzia of terror’; Cerwyn Moore and David Barnard-Wills, ‘Russian and counter-terrorism: a critical appraisal’; Ted Svensson, ‘Fixing the elusive: India and the foreignness of terror’ and Jack Holland and Matt McDonald, ‘Australian identity, interventionism and the War on Terror’, all in Asaf Siniver (ed.), *International Terrorism Post-9/11*.}

The macrosecuritisation became institutionalised in the immediate aftermath of the 11 September 2001 terrorist attacks, as the reiteration of the need to undertake a ‘war’ and references to terrorism were themselves increasingly understood as references to the presented existential threat to the ‘civilised way of life’.\footnote{An examination of how the discourse has been reproduced by the media and other institutions in society, further institutionalising it, can be found in Danny Schechter, *Media Wars: News at a Time of Terror* (Oxford: Rowland & Littlefield, 2003); Jeff Lewis, *Language Wars: The role of Media and Culture in Global Terror and Political Violence* (London: Pluto Press, 2005) and Stuart Croft, *Culture, Crisis and America’s War on Terror*.} A further demonstration of the influence the terrorist attacks had was evident in the common reference to ‘9/11’. It was symbolic of the way in which the attacks were memorialised and inextricably linked with the ‘war on terror’.\footnote{The common reference to ‘9/11’ rather than ‘11/9’ even in countries where this represents a reversal of the normal structure of dates, is testament to the power of this specific act of memorialisation. Such memorialisation is not new of course, President Reagan proclaimed the creation of a memorial day in the US for the victims of terrorism in 1986. Jan-Werner Muller’s provides a historical perspective in his text, *Memory and Power in Post-War Europe: studies in the presence of the past* (Cambridge: Cambridge University Press, 2002). For more information on ‘memory’ in International Relations see Avishai Margalit, *The Ethics of Memory* (Cambridge, Mass.: London: Harvard University Press, 2004, c2002) and for a more specific paper relating to September 11th 2001 see Maja Zehfuss, ‘Forget September 11’, *Third World Quarterly*, 24:3 (2003), pp. 513-528.} Ultimately both foreign policy, and most pertinently for this case study domestic policy, came to be viewed through this new lens; the ‘war’ would be fought on all fronts. These policies
were the emergency measures positioned as necessary to secure the referent object from the presented existential threat.

In terms of foreign policy, immediately after the September 2001 terrorist attacks the North Atlantic Treaty Organization (NATO) invoked for the first time Article Five of its charter which states that an attack on one member is considered an attack on all. Military operations in Afghanistan under the codename ‘Operation Enduring Freedom’ were launched, justified on the grounds of destroying Al Qaeda training camps and removing the Taliban regime that was harbouring them. Domestically, new institutions and laws in a number of states were justified by the requirement to ensure the security of the home front. On occasion the ‘war on terror’ became more prominent as a justification for action as time progressed such as with the war in Iraq where claims about weapons of mass destruction became increasingly discredited.

Overall while each of these policy developments were justified in their own terms in

---


specific narratives by different actors, and could for example more explicitly involve calls to secure smaller referent objects such as the state; each ultimately could be traced in some way to the ‘war on terror’, facilitated and defended by the need to secure the ‘civilised way of life’. Each then could be described as elements of the wider ‘war’, the implementation of which did in turn serve as a reminder of the macrosecuritisation. There were a series of mutually reinforcing relationships in play.

(2.3) The ‘war on terror’ in the UK:

The chapter has so far argued that in the aftermath of the terrorist attacks in the US on 11 September 2001, western political leaders internationally presented the ‘civilised way of life’ as being existentially threatened by international terrorism. This in turn facilitated the implementation of a range of foreign and domestic policies that were justified on the grounds of securing that way of life, placing counter-terrorism considerations centre-stage. This macrosecuritisation was captured in the ‘war on terror’ discourse of counter-terrorism. Recognising the case study’s focus on developments relating to UK maritime infrastructure, attention now turns to examining in a little more detail the impact of the ‘war on terror’ domestically in the UK in the immediate aftermath of the September 2001 terrorist attacks. By examining the post-securitised environment in the UK generally, one can understand how UK maritime infrastructure specifically was securitised.
The assessment of the ‘war on terror’ discourse thus far, and the associated reference to speeches made by Tony Blair illustrates how, at the very top of the UK government, the idea that international terrorism posed an existential threat to the ‘civilised way of life’ was firmly acknowledged and reiterated. Beyond Blair, the notion that the 11 September 2001 terrorist attacks represented the beginning of a new era was for example emphasised by Chancellor Gordon Brown who told the Labour Party Conference in October 2001 that “September 11 transformed our times and our task. Let us be in no doubt: it has fallen to our generation to bear the burden of defeating international terrorism.”\textsuperscript{21} At the same event Foreign Secretary Jack Straw linked the attacks to a long line of previous conflicts noting that “there are some who wish completely to destroy our values and our way of life.”\textsuperscript{22} Cabinet ministers would also emphasise how the threat posed was in some way different to that which had gone before it,\textsuperscript{23} and how the response must utilise all means available, “military, diplomatic, economic, political”.\textsuperscript{24}

Although generally the word ‘war’ itself was less widely utilised by political leaders outside of the US than it was within,\textsuperscript{25} the core characteristics of the discourse were


\textsuperscript{24} ‘Full Text: Straw’s Speech’, \textit{The Guardian Online}.

\textsuperscript{25} Tony Blair did not actually utilise the word ‘war’ in his first few opening statements to the House of Commons after 11 September 2001, although the leader of HM Official Opposition Iain Duncan Smith did express his agreement that President Bush had been right to describe the September 11\textsuperscript{th} 2001 terrorist attacks as an act of war. See Iain Duncan Smith, ‘International Terrorism and Attacks in the USA’, House of Commons, 14 September 2001, Hansard column 608, accessed 10 September 2009, \url{http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo010914/debtext/10914-02.htm}. 

91
quickly supported and reiterated. This serves as a reminder that it is the grammatical structure of “existential threat, point of no return, and a possible way out” that is significant over the reiteration of particular terminology, such as ‘war’. On one notable occasion in November 2002, the government’s choice of language came under particular scrutiny. The Home Office withdrew a published statement on terrorism written in the Home Secretary David Blunkett’s name, which had noted, amongst other things, that “we [the Home Office] cannot be sure of when or where or how terrorist will strike. But we can be sure they will try,” and that “maybe they [the terrorists] will try to develop a so-called dirty bomb, or some kind of poison gas, maybe they will try to use boats or trains rather than planes. The bottom line is that we simply cannot be sure.” Blaming the publication on a “clerical error”, the Home Office quickly published a second statement where any reference to a dirty bomb was removed, with the Home Secretary acknowledging the language had been toned down to avoid “creating unjustified panic and disruption”.

Despite the withdrawal the new statement continued to warn of the serious threat posed to the country.

Returning to the three signs of audience acceptance of securitisation highlighted in the previous chapter, the widespread reiteration by political leaders in the UK was clear evidence that the first sign - consistent deployment of securitising discourses by securitising actors which demonstrates that the presented threat was both salient and


understood – was in place. Illustrating the second sign of acceptance, wider expressions of support for the ‘war on terror’ were also evident amongst parliamentarians in this period, one group with some responsibility for the development of counter-terrorism legislation as a whole in the UK. For example, the leader of the official opposition Iain Duncan Smith noted that parliamentarians were “the guardians of a set of values that are underpinned by that democracy and the rule of law”, that it was “those values that were attacked with such callous and brutal ferocity”, and that the UK was united with the US in defending “civilised values against those who seek to bring them down by violence.”

A Defence Select Committee report on the threat from terrorism concluded that:

The threat from terrorism is now more pressing and more dangerous. A threshold has been crossed in terms of scale and level of casualties. In response, the global campaign against terrorism must be pursued relentlessly. We must not lose our sense of the urgency and importance of this task in the months ahead.

Finally a range of foreign and domestic policies were pursued in this period which demonstrated that the third sign of acceptance – the implementation of emergency measures themselves – was very much present. The UK was an active supporter of the military action in both Afghanistan and Iraq committing considerable military forces to both campaigns. Domestically Blair had noted soon after the 11

---

30 All taken from Iain Duncan Smith, ‘International Terrorism and Attacks in the USA’, Hansard columns 607-608.


32 UK military operations in Afghanistan went through a number of phases. The codename ‘Operation Veritas’ was given to the first months of operations. Here the UK provided, amongst other things, a number of RAF assets including VC-10 tanker aircraft, the aircraft carrier HMS Illustrious and 200 members of 40 Commando Royal Marines to support the US. Further details can be found in House of Commons Library, Operation Enduring
September 2001 terrorist attacks that counter-terrorism legislation would need to be revisited and that the country had to become more prepared to defend itself from any future terrorist threats. By December 2001 the Anti-terrorism, Crime and Security Act (ATCSA) had been passed giving the authorities additional powers, including the ability to detain without charge certain foreign nationals suspected of terrorism. Although on face value it was the foreign policy dimension of the ‘war on terror’ that was more militaristic in character and domestically the emphasis generally remained on investigation, evidence gathering and prosecution. The sense of emergency and military logic that accompanied the ‘war on terror’ blurred the distinction between the military and criminal justice models of countering terrorism, most evident with the extended pre-charge detention powers. Overall in the immediate period after the 11 September 2001 terrorist attacks, it was clear that counter-terrorism had moved to the very top of the domestic policy agenda.

---


35 For more see Mathieu Deflem, The policing of terrorism: organizational and global perspectives. Ronald Crelinsten makes a distinction between “September 10 thinking” and “September 12 thinking” in relation to counter-terrorism acknowledging that in the latter the military option played a far more significant role. See Ronald Crelinsten, Counterterrorism (Cambridge: Malden, MA.: Polity Press, 2009), pp. 1-16.
Before the United Kingdom’s domestic counter-terrorism efforts in this period are elaborated in greater depth two further points are worth acknowledging. The first is that while a number of emergency measures were successfully implemented there was some resistance. There were a minority who totally rejected the idea of a ‘war on terror’ discourse and the macrosecuritisation it captured and were vocal about it. For example, within the House of Commons, Jeremy Corbyn, criticised the way in which the label ‘terrorist’ was utilised, argued that in referring to a war between civilisation and the rest of the world President Bush had “denigrated” Islam, highlighted the US role in “the production and financing” of organisations that they subsequently raised up as the enemy, and challenged the value of military solutions asking:

```
if we [the UK] are such a close friend of the United States, cannot we use our relationship as a basis to persuade it that, in the interests of justice and of causing no more needless deaths, we must have an international rule of law and a proper international court at which criminals can be brought to justice?36
```

Yet most often the resistance was directed at particular counter-terrorism practices, rather than against the ultimate rationale for them – the need to secure the ‘civilised

---

way of life’ against an existential terrorist threat. Specific elements of the ‘war’ then, such as the conflict in Iraq and the expansion of pre-charge detention were resisted both by those with some responsibility for counter-terrorism efforts as a whole and the public.\footnote{In terms of the war in Iraq, there were a series of mass public demonstrations in the UK against the military action. On 15 February 2003 approximately 1 million marched in London. Rajeev Syal, Andrew Alderson and Catherine Milner, ‘One million march against war’, The Telegraph Online, 16 February 2003, http://www.telegraph.co.uk/news/uknews/1422228/One-million-march-against-war.html. The Leader of the House of Commons Robin Cook would also resign over the war on 17 March 2003 outlining his decision to the House of Commons later that day. Robin Cook, ‘Personal Statement’, House of Commons, 17 March 2003, Hansard columns 726-728, http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030317/debtext/30317-33.htm#30317-33_spnew0. Concerns about extending pre-charge detention for terrorist suspects were expressed, amongst others, by a number of parliamentarians. See ‘Anti-terrorism, Crime and Security Bill’, House of Commons, 19 November 2001, Hansard columns 31-32, http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo011119/debtext/11119-08.htm; and ‘Criminal Justice Bill’, House of Commons, 20 May 2003, Hansard columns 941-954, http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030520/debtext/30520-31.htm. All accessed 14 September 2009.} This suggests that resistance can take numerous forms. Overall however the ‘war on terror’ remained the dominant discourse in this period despite of this resistance, and a range of measures that would not have been possible prior to 11 September 2001 were implemented.\footnote{One example of a parliamentary challenging government critics was evident in the second reading of the ‘Anti-terrorism, Crime and Security Act’. In an intervention Labour MP Kevin Hughes told David Blunkett that he welcomed the legislation before asking the Home Secretary whether he found it “bizarre—as I do—that the yoghurt and muesli-eating, Guardian-reading fraternity are only too happy to protect the human rights of people engaged in terrorist acts, but never once do they talk about the human rights of those who are affected by them?” Kevin Hughes, ‘Anti-terrorism, Crime and Security Bill’, House of Commons, 19 November 2001, Hansard column 30, accessed 14 September 2009, http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo011119/debtext/11119-08.htm#11119-08_spnew3.} Second, just like the discourse itself, counter-terrorism practices have their own genealogy. Elements of the ‘war on terror’ built upon and were influenced by UK experiences of counter-terrorism particularly in relation to Northern Ireland.\footnote{A wide range of literature examines British counter-terrorism efforts in Northern Ireland. See Paul Dixon, Northern Ireland: the politics of war and peace (Houndmills, Basingstoke, Hampshire: New York, N.Y.: Palgrave, c2001); Terence Taylor, ‘United Kingdom’, in Yonah Alexander (ed.) with a foreword by R. James Woolsey, Combating terrorism: strategies of ten countries (Ann Arbor, Mich.: University of Michigan Press, 2002), pp. 201-203; Clive Walker, ‘Policy Options and Priorities: British Perspectives’ in Marianne van Leeuwen (ed.), Confronting Terrorism: European Experiences, Threat Perceptions and Policies (The Hague, Netherlands: Kluwer Law International, 2003), pp. 11-36; and Steve Hewitt, The British War on Terror (London: New York: Continuum, 2008), pp. 9-28.} Although the impact of the ‘war’ was arguably more extensive then than that which had been evident beforehand, the call to maintain the security of some referent object is a longstanding and recurring one.
The pursuit of the ‘war on terror’ and the resultant positioning of counter-terrorism at the very top of the domestic policy agenda resulted in a flurry of activity. There was a proliferation of legislation with some counter-terrorism implications. The previously highlighted Anti-terrorism, Crime and Security Act (ATCSA) was the government’s central response in this period and was introduced just months after the 11 September 2001 terrorist attacks. Illustrating the genealogy of counter-terrorism efforts, it built upon the wide-ranging provisions encapsulated in what were themselves still relatively new pieces of legislation - the Terrorism Act (TA) and Regulation of Investigatory Powers Act (RIPA) – both of which had been introduced the previous year.\(^{40}\) The Terrorism Act had established “a more unified”\(^{41}\) counter-terrorism legal regime placing on a permanent footing a number of counter-terrorism powers which had up until this point been encapsulated in emergency legislation that required regular Parliamentary renewal. It also placed greater emphasis on international terrorism, extending focus beyond Northern Ireland to cover all forms of terrorism in the UK.\(^{42}\) RIPA on the other hand set out to regulate how public bodies could conduct surveillance and investigations whilst elaborating under what conditions and how communications may be intercepted.\(^{43}\)

The ATCSA provides an interesting insight into the impact of ‘war on terror’ in practice as it demonstrates both how the British state increased its power and how a


\(^{42}\) Ibid., pp. 14-16.

\(^{43}\) ‘Regulation of Investigatory Powers Act’, particularly Parts I-IV.
notable sense of urgency underpinned counter-terrorism efforts in this period. ‘Power’ here and in the thesis as a whole is defined broadly as the possession of influence over increasing areas of life, while state power is understood to be exercised by a government and associated bureaucracy, alongside those institutions tasked with state security, the intelligence services and police primarily. Provisions in the ATCSA enabled the Home Secretary to order the indefinite detention without charge of non-UK citizens suspected of terrorism-related offences, who, for a variety of reasons could not otherwise be deported. This increase in the state’s power to deny an individual their liberty in the name of national security became all the more palpable because it rested on the United Kingdom suspending its adherence to Article Five of the European Convention on Human Rights.

Article Five states, amongst other things, that an individual must be brought to trial “within a reasonable time” and must only be detained “after conviction by a competent court”. The government derogated its responsibilities by arguing that a ‘state of emergency’ existed – itself an explicit sign of the wider securitising impact

---

44 ‘Power’ has also been described, accurately, as an essentially contested concept (see Michael Barnett and Raymond Duvall, ‘Power in International Relations’, *International Organization*, 59:1 (2005), p. 41). There have been a range of studies in to the concept, specifically in relation to International Politics, all of which highlight the way in which the study of ‘power’ is, at its heart, the study of the way in which actors affect each other. For example see K.J. Holsti, ‘The Concept of Power in the Study of International Relations’, *Background*, 7:4 (1964), pp. 179-194; Joseph S. Nye Jr., *Soft Power: The means to success in world politics* (New York: Public Affairs, 2004), specifically pp. 1-32; Steven Lukes, *Power: a radical view* (Houndmills, Basingstoke, Hampshire: New York: Palgrave Macmillan, 2005), 2nd edition and Barnett and Duvall, ‘Power in International Relations’, pp. 39-75. Undertaking a detailed examination in to the different forms of power, how it is gained and lost is beyond the scope of this thesis. It is envisaged however that the thesis will provide insights in to how, in this particular case study, both the state and port owners increased their power in relation to UK maritime infrastructure.


of the ‘war on terror’ – and utilised Article Fifteen, clause 1 of the same convention
to support its action. This clause states:

In time of war or other public emergency threatening the life of the nation any
High Contracting Party may take measures derogating from its obligations
under this Convention to the extent strictly required by the exigencies of the
situation, provided that such measures are not inconsistent with its other
obligations under international law.\textsuperscript{47}

Although there was resistance to the pre-charge detention provisions as a whole, the
suspension of Article Five lasted for an initial fifteen months and was also renewed
by the UK Parliament in both March 2003 and 2004 before finally being repealed in
April 2005.\textsuperscript{48}

The sense of urgency was evident in the fact that the ATCSA was initially brought
before Parliament on 19 November 2001 and was subsequently debated, scrutinised,
voted upon and gained Royal Assent bringing it in to law in less than a month.\textsuperscript{49} This
situation led to a rebuke for the government from the House of Commons Home
Affairs Select Committee. In their first report of the 2001-2002 parliamentary session
they questioned whether it was:

---

\textsuperscript{47} ‘European Convention on Human Rights’, Article Fifteen, Clause one.


Appropriate for this Bill to be passed through the House of Commons in exactly two weeks with only three days of debate on the floor of the House. [Arguing that] a Bill of this length - 125 clauses and eight schedules covering 114 pages - with major implications for civil liberties should not be passed by the House in such a short period and with so little time for detailed examination in committee.\(^50\)

The extent to which this urgency was in any way unique is certainly open to debate. In both 1974 and 1998 the government of the time also introduced counter-terrorism legislation at a similar pace,\(^51\) whilst there is an argument to be made that by its very nature counter-terrorism rests on a requirement for speed of action. Yet undoubtedly the presentation of terrorism as posing an existential threat to the ‘civilised way of life’, encapsulated in the ‘war on terror’ discourse, ensured that speed of action could be presented as essential when survival was deemed to be at stake.

This increase in state power and sense of urgency was also evident beyond the ATCSA. The power to arrest and detain an individual without charge for example, was closely related to the power introduced in the TA allowing Police Officers to arrest any person, who was reasonably suspected of being a terrorist.\(^52\) Once detained the individual could initially be held for up to 48 hours and then up to five additional days with the permission of a judge, before a charge had to be brought or the individual released. This had broken with UK legal traditional which stated that an


\(^{52}\) ‘Terrorism Act’, Part Five, Section 41, Clause One.
individual had to be charged or released within 24 hours of arrest. The period of pre-charge detention was extended with considerable controversy to 14 days in the Criminal Justice Act, 2003 and to 28 days in the Terrorism Act, 2006.\[^{53}\] Attention also fell in this period on the need to introduce major new initiatives which would also increase the power of the state further, such as a proposed national identity database and its associated identity cards, and new legislation to aid emergency planning.\[^{54}\]

In terms of urgency, in a speech to the Financial Services Authority’s money laundering conference in July 2002, the Financial Secretary to the Treasury, Ruth Kelly, summarised what she referred to as the United Kingdom’s “rapid response” towards locating and freezing suspected terrorist assets. Since September 2001 she noted that, amongst other things, the UK had frozen £70 million of assets associated with Osama Bin Laden, the Taliban and Al Qaeda, that over 300 individuals and entities had been listed on asset freeze lists, and that the Bank of England had


notified over 600 banks and financial institutions to search their records against these lists.\textsuperscript{55}

Beyond the proliferation of new counter-terrorism legislation, focus also fell on ensuring that there was enhanced co-ordination between those responsible for counter-terrorism.\textsuperscript{56} Internationally this was largely driven by the view that the terrorist threat was truly global in scale and that no one state could deal with it in isolation.\textsuperscript{57} Domestically it was largely framed by a desire to develop a seamless approach to counter-terrorism where strategic leadership could be provided and perceived areas of weakness could be overcome.\textsuperscript{58} Although once again the United Kingdom had already begun this process before September 2001, particularly with the creation in July 2001 of a Civil Contingencies Secretariat within the Cabinet Office tasked with co-ordinating national emergency planning;\textsuperscript{59} a view was expressed by the House of Commons Defence Select Committee that more could still be done.


\textsuperscript{56} Here ‘enhanced co-ordination’ is understood in broad terms and as such an assumption is made that enhanced co-operation is intertwined with co-ordination.


\textsuperscript{58} As argued by Ruth Kelly in ‘Speech to the Financial Services Authority’, paragraph 13.

\textsuperscript{59} The Civil Contingencies Secretariat website, accessed 18 May 2009, \url{http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx}. 

102
In a report published in July 2002 entitled ‘Defence and Security in the UK’, the committee were scathing, arguing that “instead of being the solution to the habitual ‘departmentalism’ of Whitehall, it [the Civil Contingencies Secretariat] has become a causality of it”\(^{60}\), ultimately concluding that:

There has been inadequate central co-ordination and direction. The Government has not taken the opportunity to conduct a proper and comprehensive examination of how the U.K would manage the consequences of a disaster on the scale of 11 September. In many areas the Government has confused activity with achievement. A strong central authority is needed to lay down clear criteria for the work of individual government departments and to co-ordinate the efforts of other agencies.\(^{61}\)

The extent to which co-ordination and centralisation necessarily move hand in hand, as the committee seem to suggest, is of course questionable.\(^{62}\) The UK’s ‘lead department’ approach to counter-terrorism in this period rested, as Paul Cornish notes, on “the operating premise [...] that the responsibility for managing an emergency or crisis should lie with the agency and/or level of government most appropriate to deal with the incident.”\(^{63}\) Yet while there was no creation of a central UK Department of Homeland Security like that in the US in this period, further efforts to enhance co-ordination did take place.


\(^{61}\) Ibid., p. 7.

\(^{62}\) Arguably co-ordination of activity can take place well away from the perceived centre of governance, while centralisation can imply control is held more in the hands of one party than by a collection of parties working increasingly closely together.

Across government a new counter-terrorism strategy known as ‘CONTEST’, was written and introduced in 2003. It sought to organise counter-terrorism efforts along four strands – ‘Pursue’, ‘Protect’, ‘Prevent’ and ‘Prepare’ and encapsulated the argument that “counter-terrorism cannot be carried out in isolation”.\(^6^4\) Further institutional changes also followed. In June 2002 a new position of Security and Intelligence Co-ordinator was created as “the intelligence responsibilities of the Cabinet Secretary were delegated” to a new individual.\(^6^5\) Initially this individual advised the Prime Minister on intelligence and security through chairmanship of the Joint Intelligence Committee (JIC) and had overall responsibility for delivering CONTEST.\(^6^6\) The following year the Joint Intelligence Analysis Centre (JTAC) was also established to analyse and assess “all intelligence relating to international terrorism, at home and overseas”.\(^6^7\) Based within the headquarters of the Security Service (MI5) it brought together staff from all the intelligence agencies, the Metropolitan Police (MET) and relevant government departments to analyse terrorist threats.\(^6^8\)

Expanding this kind of joint working was also the focus of wider discussion. For example, a report provided by Her Majesty’s Inspectorate of Constabulary (HMIC) on Special Branch (SB) and Ports Policing entitled ‘A Need to Know’, called for


\(^{65}\) Sir Francis Richards, ‘The development of the UK intelligence community after 9/11’, in Asaf Siniver (ed.), International Terrorism Post-9/11, p. 120.

\(^{66}\) Idem.

\(^{67}\) Taken from the ‘Joint Terrorism Analysis Centre’ (JTAC) website, accessed 17 November 2010, https://www.mi5.gov.uk/output/joint-terrorism-analysis-centre.html.

\(^{68}\) Sir Francis Richards, ‘The development of the UK intelligence community after 9/11’, p. 120.
greater co-ordination between different constabulary Special Branches particularly at a regional level. The report also noted that while co-ordination between SB and the Security Service (who took over SB’s role as the main collector of intelligence relating to terrorism in 1992) was generally good, it could be improved between SB and other parts of the Police and those agencies who operated in UK ports at this time such as the Immigration Service and Her Majesty’s Revenue and Customs (HMRC). Described as the ‘golden thread’ between the intelligence services and local police, SB is charged with gathering “intelligence to meet national security requirements as well as to support other policing priorities such as the prevention of disorder”. The MET and every other Home Office police constabulary each has its own SB drawn from its officer pool.

Alongside enhanced co-ordination, the pursuit of the ‘war on terror’ also resulted in a growth in counter-terrorism budgets. In the immediate aftermath of the 11 September 2001 terrorist attacks, the UK government set aside a combined £50 million in additional funding to tackle terrorist financing, develop anti-terrorism measures, and finance additional policing. By April 2002 it was estimated that an additional £1

---

69 Her Majesty’s Inspectorate of Constabulary, A Need to Know: HMIC Thematic Inspection of Special Branch and Ports Policing (Home Office Communication Directorate, January 2003), paragraphs 2.79-2.94, 37-42. The report was kindly provided to the author by HMIC Press Office.

70 Ibid., paragraph 2.9, p. 17 and paragraphs 3.18-3.32, pp. 52-55.

71 Ibid., paragraph 2.3, p. 16. The ‘golden thread’ represents the two way linkage Special Branch plays between national intelligence and security agencies and local police and communities.

72 Ibid., paragraph 1.9, p. 10.

73 This figure represents the combination of an additional £20 million which was made available “to cut off the supply of finance to terrorists and to fund other anti-terrorism measures” and £30 million made available to “fund the need for additional policing since September 11th”. Gordon Brown, ‘Pre-Budget Report’, House of Commons, 27 November 2001, Hansard column 834, accessed 15 September 2009, http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo011127/debtext/11127-06.htm#11127-06_spmin0.
billion had been allocated since the previous September towards operations with some counter-terrorism purpose.\footnote{This figure represents a combination of the £50 million additional spending previously highlighted and an additional £950 million for the Ministry of Defence. Gordon Brown, ‘Budget Statement’, House of Commons, 17 April 2002, Hansard column 588, accessed 15 September 2009, \url{http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo020417/debtext/20417-04.htm#20417-04_spmin1}.} According to the Parliamentary Intelligence and Security Committee’s annual report 2003-04 the resource element of the Single Intelligence Account (SIA) – the budget allocated to fund the three intelligence services – increased from £908.9 million in 2001-02 to £1,111.7 million in 2004-05, an increase of over £200 million in three years.\footnote{The first figure represents the budget spent, while the latter figure represents a budget allocation at the time of the report’s publication. House of Commons Intelligence and Security Committee, \textit{Annual Report 2003-04} (London: The Stationery Office Ltd, June 2004), p. 11. All of the committee’s reports and the government responses can be found via the Cabinet Office website, accessed 28 June 2011, \url{http://www.cabinetoffice.gov.uk/resource-library/intelligence-and-security-committee-isc-annual-reports}.} In terms of the allocation of this budget, the Security Service moved from committing 57\% of its resources on counter-terrorism in 2001-02 to 72\% by 2004-05, of which the percentage spent on international counter-terrorism as opposed to Irish-related terrorism jumped from 25\% to 52\% in the same period.\footnote{Steve Hewitt, \textit{The British War on Terror}, p. 94.}

Finally alongside this growth in spending, the work of security professionals arguably also gained a higher public profile in this period.\footnote{As noted in the previous chapter the reference to ‘security professionals’ here is simply a generic term utilised to capture all those, both state and privately funded, who’s primary responsibility is the maintenance of security. State security professionals include the Police, specifically SB officers, but also officers from the intelligence services. Private security professionals include ports police units funded by port owners and private security guard companies.} Security operations have periodically been the subject of public attention, seen for example in the SAS operation during the Iranian Embassy siege in 1980.\footnote{A taste of this attention can be located in ‘1980: SAS rescue ends Iran embassy siege’, \textit{BBC News Online}, accessed 28 June 2011, \url{http://news.bbc.co.uk/onthisday/hi/dates/stories/may/5/newsid_2510000/2510873.stm}.} In the years immediately after the 11 September 2001 terrorist attacks however, such focus only increased and...
became more sustained. One illustration of this changing situation can be seen in the way in which the Director General of the Security Service made more regular, albeit still relatively rare, public contributions. Here Dame Eliza Manning-Buller made her first public speech in June 2002, another in October 2003 and then once a year for the rest of her time in office. Leading police officers such as the Commissioner of the Metropolitan Police also continued to have a significant public profile. Commissioner Sir John Stevens would go on to the flagship BBC political programme ‘Breakfast with Frost’ in February 2003 to explain and support the decision to deploy tanks at Heathrow Airport. The extent to which senior police officers in particular played a more public role in pushing for and supporting specific legislation and powers would be something that came under further scrutiny in later years.

(2.4) The securitisation of UK maritime infrastructure during the ‘war on terror’:

The pursuit of a ‘war on terror’ then resulted in counter-terrorism moving to the very top of the domestic policy agenda within the UK. The proliferation of legislation with counter-terrorism implications, legislation that resulted in an increase in state power, the focus on the need for more co-ordinated counter-terrorism efforts which helped to bring about considerable institutional changes, particularly within central

79 The first public speech by a Security Service Director General took place in June 1994. Between then and September 2001 there were just two additional public speeches. Between June 2003 and September 2010 there were eight public speeches. A transcript of each one can be found at ‘Speeches by the Director General’, Security Service (MI5), accessed 14 September 2009, https://www.mi5.gov.uk/output/speeches-by-the-director-general.html.

government, the growth in counter-terrorism budgets to meet the terrorist threat presented as being faced, the higher public profile for the work of security professionals, all underpinned with a notable sense of urgency, were the prominent features of counter-terrorism efforts as a whole domestically. This represented the backdrop in which UK maritime infrastructure itself was a ‘site of securitisation’ as concern about international terrorism and the focus on enhancing security permeated and framed ever greater areas of life, in a growing range of ways and on a more sustained basis. As outlined in the previous chapter, the description of UK maritime infrastructure as being a ‘site of securitisation’ stems from an acknowledgement that ports and harbours are ultimately geographic spaces. With securitisation, everyone, everything, and all activities associated with this space are increasingly presented as requiring ‘securing’ against presented threats.

The securitisation of UK maritime infrastructure in this period was most evident in the development and introduction of the International Ship and Port Facility Security (ISPS) code, an example of an emergency measure. The code emerged in the immediate aftermath of 11 September 2001 out of discussions initiated by the International Maritime Organization (IMO), a specialised agency of the United Nations responsible for developing and maintaining a comprehensive regulatory framework for shipping. Covering both vessels and the ship-port interface, defined as “the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services

---


82 Information on the work of the IMO can be found at their website, accessed 8 February 2008, [http://www.imo.org/Pages/home.aspx](http://www.imo.org/Pages/home.aspx).
to or from the ship”, the code provides a framework within which both vessels and port facilities at this interface can be secured. The code was implemented through the adoption of amendments to a re-identified Chapter XI-1, ‘Special measures to enhance maritime safety’ and the addition of a new Chapter XI-2 titled ‘Special measures to enhance maritime security’, to the central maritime treaty the International Convention for the Safety of Life at Sea (SOLAS, 1974). The code “applies to passenger ships and cargo ships of 500 gross tonnage and upwards, including high speed craft, mobile offshore drilling units and port facilities serving such ships engaged on international voyages”.

The code is split into two parts, the first is mandatory and the second is recommendatory. Within Part A there is a requirement to introduce a maritime security regime whereby the ship/port interface becomes a restricted area where access is increasingly controlled and activities more heavily monitored. There can be a number of port facilities within any one port. Alongside this, the code requires the introduction of Ship and Port Security Plans (SSP’s/PSP’s), a Ship Security Officer (SSO), Company Security Officer (CSO) and Port Facility Security Officer (PFSO) with responsibility for their management. The code introduces a process of certification for both ships and ports to ensure compliance which is managed by the state where the relevant port is located or ship registered. Three different security levels are also introduced which enable the level of threat to be constantly

---


monitored and the appropriate responses to be initiated. The code also demands that all security decisions made are recorded in some detail, and that the required training, drills and exercises are undertaken to ensure familiarity with the plans.  

Part B of the code provides a little more detail and contains advice on how to most effectively comply with those mandatory requirements in Part A. For example, regulation 4.2 states that a contracting government to the IMO (a member state) may identify “a Designated Authority within government to undertake their security duties relating to port facilities as set out in chapter XI-2 or part A of this Code.”

Within the United Kingdom, responsibilities are split between the Transport Security and Contingencies Directorate (TRANSEC) which sits within the Department of Transport (DfT) and the Maritime and Coastguard Agency (MCA).

Another example is regulation 4.9 which elaborates what is meant by security level three:

Setting security level 3 should be an exceptional measure applying only when there is credible information that a security incident is probable or imminent. Security level 3 should only be set for the duration of the identified security threat or actual security incident. While the security levels may change from security level 1, through security level 2 to security level 3, it is also possible that the security levels will change directly from security level 1 to security level 3.

86 IMO, ISPS Code, pp. 6-36.
87 Ibid., p. 43.
The leadership provided by the IMO here illustrates the multi-levelled governance of UK maritime infrastructure. Alongside the UK’s membership of the IMO, its membership of the European Union (EU) also placed it under a number of obligations in relation to the security of its maritime infrastructure as is elaborated throughout the case study. This situation also represents recognition of the global and inter-connected nature of the maritime industry where developments relating to the management of ships would have an impact on activities relating to the management of port facilities and vice versa, and where actions in one state or region were deemed to have knock-on effects elsewhere. The membership of regional and international organisations provided one mechanism to better manage this inter-connectedness.

Examining the securitisation of UK maritime infrastructure then demands an acknowledgement that maritime infrastructure internationally was securitised in this period, and that an assessment of the impact of securitisation on the management of UK maritime infrastructure requires policy developments outside of the UK to be considered too.\textsuperscript{90} This is the case throughout the case study period.

Ultimately the development and introduction of the code occurred quickly after 11 September 2001. It was less than a week after the attacks that the Secretary-General of the IMO William O’Neil noted how international terrorism represented a threat to the maritime industry. Speaking at a conference on safety in maritime transport, O’Neil commented that “in the longer term, it is clear that security measures surrounding all forms of transport will have to be re-examined and re-assessed in the

light of this tragedy. *We are all potential targets of terrorist activity.*”

The following month O’Neil again emphasised there was a threat, focusing on the way in which the 11 September 2001 terrorist attacks had challenged old assumptions and as such required the organisation’s priorities to change as a result:

The attack on the United States on September 11th has resulted in shock waves that have spread throughout the whole globe. The ramifications are already being felt in almost every facet of our lives. Old assumptions are being challenged and even the fundamental economic and social structures that have evolved over time are now being called into question. [...] Safety and security have assumed a higher profile than ever and have been placed at the top of the priority list. This is witnessed by the fact that the UN Security Council adopted a resolution, on September 28th, containing wide-ranging comprehensive measures and strategies to combat international terrorism. *Shipping and maritime structures are vulnerable and I therefore initiated steps to place a Resolution before this Assembly which focuses on terrorism.*

The links between those ideas encapsulated in this extract and those encapsulated in the ‘war on terror’ discourse are clear. The emphasis on 11 September 2001 being in some way a turning point, and the notion that “old assumptions are being challenged” related to the idea that a new era began on 11 September 2001 and that the threat posed by international terrorism was now on a different level. The discussion of “fundamental economic and social structures” interplayed with considerations over the extent to which international terrorism and the response to it may impact upon a particular way of life. The reiteration that safety and security were at the top of the

---


There is a genealogy to the IMO highlighting the threat to the maritime industry from terrorism as seen in the aftermath of the Achille Lauro hijacking in 1985. It resulted in the ‘Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation’ (SUA) being adopted in 1988. It set out the appropriate action which should be undertaken in the event of unlawful acts taking place against ships, including hijacking. More specifically it required, amongst other things, for contracting governments to prosecute or extradite alleged offenders.

priority list and the certainty with which O’Neil noted that “shipping and maritime structures are vulnerable” linked to the sense of inevitability often attached to the way the threat posed by international terrorism was presented and the urgency which underpinned calls for a response.93

Such links illustrate the mutually reinforcing relationship between the macrosecuritisation of the ‘civilised way of life’ captured in the ‘war on terror’ discourse and the securitisation of maritime infrastructure. The presentation of the threat posed by international terrorism as challenging the very survival of the ‘civilised way of life’ ensured the threat was regarded as so wide-ranging that danger could be presented as being around every corner. In turn by emphasising the threat posed to maritime infrastructure, which in turn facilitated the implementation of emergency measures, the existential threat relating to the ‘civilised way of life’ maintained its dominance in the wider public consciousness through reiteration. This also again emphasises the argument advanced in the previous chapter that securitisation is more process than moment.

This relationship between macrosecuritisation and the securitisation of maritime infrastructure is illustrated more clearly in O’Neil’s address to the IMO in December 2002 when he flagged up the possible wider ramifications of terrorist activity:

There is a deep and widespread concern about the worldwide escalation of acts of terrorism in all its forms, acts which endanger or take innocent human lives, jeopardize fundamental freedoms and seriously impair the dignity of human beings. The matter of maritime security has introduced a new, and very

93 Italics added by author for emphasis in quoted extract.
important, element in IMO’s series of responsibilities and I can understand the sensitivity that Governments and the industry have about it. At the same time, the need to ensure the uninterrupted flow of international seaborne trade cannot be ignored, which is why I have been taking every opportunity to raise the awareness of the importance and significance of shipping to world trade and the economic chaos that would be caused if the global supply chain were to be interrupted because of terrorist attacks against ships, ports, offshore terminals or other marine facilities.\textsuperscript{94}

This was to be a theme reiterated by the Organisation for Economic Co-operation and Development (OECD) who, in a report published in July 2003, discussed the potential economic cost of a port closure due to terrorist attack. They noted how the closure for 11 days in October 2002 of west coast ports in the US, as the result of a dispute between labour and management, was estimated to have resulted in a loss of at least $466.9 million for the US economy.\textsuperscript{95} In the same report the OECD produced this diagram.


It illustrates the way in which concerns about international terrorism had become increasingly dominant resulting in various possible dimensions to that presented threat being highlighted as worthy of further consideration.

Despite this, two main narratives, not always easily differentiated from each other, became increasingly evident. The first presented maritime infrastructure as a possible ‘target’ of international terrorism. International terrorism threatened the operability of the infrastructure which in turn had wider negative ramifications. One example of the reproduction of such a narrative could be glimpsed in a 2003 report by the European

---

Union Committee on Industry, External Trade, Research and Energy which wrote that “maritime transport is by definition vulnerable to attacks” and that “stronger measures of maritime security are also required for economic reasons, given the importance of maritime transport on the economy”. The second presented maritime infrastructure as a ‘vulnerable node’, a space that could be exploited by terrorists to do harm elsewhere. An example of this narrative could be seen in a warning delivered by the UK’s Parliamentary Under-Secretary of State for Transport David Jamieson MP, when he reminded IMO delegates of the threats posed if transportation was used as a weapon of mass destruction noting:

We saw, all too clearly in September, *that transport can itself become an instrument of international destruction*: piracy and terrorism are symptoms of disorder and I think this Organization will have its part to play in restoring order and peace.

Ultimately the production and reproduction of these two main narratives, directed here most prominently by political leaders with some responsibility for policy that related to UK maritime infrastructure, in a mutually reinforcing relationship with the macrosecuritisation of the ‘civilised way of life’, created the space in which, the rationale even, for the development and introduction of the ISPS code. During this initial stage of implementation as the code was conceived and preparations were made for it to come into force, the idea that maritime infrastructure was threatened and that there should be constant vigilance and no complacency with regards to that terrorist threat was reiterated.

---


Initial wider discussions over what response was necessary to the 11 September 2001 terrorist attacks had taken place in the IMO in November 2001. The idea of an internationally recognisable code had been proposed by the US delegation to the IMO and was developed in a series of committee meetings thereafter, in particular through the Intersessional Working Group on Security. It was formally adopted at the fifth SOLAS Conference which was held at the IMO’s headquarters in London between 9 and 13 December 2002, when 1 July 2004, just 18 months later, was set as the date when the code would come into force in all relevant member states. The International Convention for the Safety of Life at Sea (SOLAS) conference was attended by representatives of 108 contracting governments to the 1974 SOLAS Convention, and there had been a considerable level of expectation at its start. In his opening statement Admiral Thomas H. Collins, Commandant of the US Coast Guard, had declared its significance arguing:

Shipping is an international business. Terrorism is an international threat. Maritime Security requires long-term international solutions. IMO is the place to develop and adopt those solutions. The eyes of the world are now on this conference, watching and waiting to see what we will do. We must show them that IMO can act, and act decisively, to adopt meaningful maritime security requirements.

99 At the 22nd Regular Session of the IMO Assembly, 19 November 2001.

100 The terms of reference for the intersession working group were set out at the 22nd Regular Session of the IMO Assembly, specifically in document (A 22/5/(B)/2). The working group met between 11-15 February 2002 to discuss options with the intention of reporting back at the 75th Session of the Maritime Safety Committee in May 2002.


It was left to IMO members individually to undertake any specific legislative processes required to introduce the ISPS code into domestic law. In the case of the UK this process was initially driven forward by the EU to ensure that the code was implemented with consistency across member states ensuring a seamless approach to security, formalising a system of community-wide monitoring of its compliance, and maintaining competitiveness. This latter concern can be understood to stem from a fear that the uneven introduction of the required security measures under the code, at considerable financial cost and with possible effects on the pace of port operations, could give unfair commercial advantage.

Initial discussions took place in the Council of Ministers, while the development of the necessary regulation bringing the code into force was undertaken by the relevant committees, specifically the Committee on Regional Policy, Transport and Tourism. In November 2003, the committee’s report (A5-0385/2003) on enhancing ship and port facility security was first debated at a meeting of the European Parliament in Strasbourg, a little over 11 months after the code had first been adopted internationally.103 Four months later on 31 March 2004, the resultant Regulation (EC) No 725/2004 was adopted bringing the ISPS code into European law.104 This legislative process concluded on 10 June 2004, when the regulation was laid before the UK Parliament in the form of The Ship and Port Facility (Security) Regulations


The regulation took the form of a statutory instrument, a piece of secondary legislation, and was transposed unchanged from the EU regulation into UK law.

The most noticeable feature of the EU regulation was that the coverage of the ISPS code for European ships and port facilities had been extended beyond that set out by the IMO. First, a number of elements of the recommendatory Part B of the code were made mandatory by the regulations, including paragraphs 16.3-16.8 which set out the minimum standards for the port facility security plan and 18.5-18.6 which provided guidance on the frequency of drills and exercises. Alongside this the regulations also required that by 1 July 2005, the code cover all passenger ships which were engaged on domestic voyages that venture over 20 nautical miles from the coast (Class A Ships) and the port facilities which served them, not solely those engaged on international voyages. On similar grounds by 1 July 2007 European member states had to conduct a risk assessment regarding the extent to which the code should be expanded further, specifically to smaller ships engaged on domestic voyages. Finally the European Commission through the European Maritime Safety Agency (EMSA) was empowered to undertake a range of inspections to ensure compliance.


106 IMO members had envisaged this scenario in ‘Conference Resolution 7’ adopted at the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974, 12 December 2002, accessed IMO Knowledge Centre 13-14 October 2008. Also see IMO, ISPS Code, p. 133.


108 Ibid., Article 3, Paragraph 2.

Collectively these developments demonstrated a restlessness in relation to maritime infrastructure security as the scope of the counter-terrorism security response was expanded. There was an acknowledgement both at the IMO and within the EU that the ISPS code only covered the ship-port interface and that focus would have to turn to ensuring the security of the port at large. During 2003 the IMO in partnership with the International Labour Organization (ILO) conducted preparatory work on a code of practice titled ‘Security in Ports’.\textsuperscript{110} Amongst other things it would recommend that security plans be written for the entire port and that regular security assessments be conducted by an appropriate authority in each port.\textsuperscript{111} Many of these ideas would be encapsulated in Directive 2005/65/EC by the European Commission in October 2005, which introduced EU-wide security measures for the port as a whole.\textsuperscript{112}

As the 1 July 2004 deadline approached for the ISPS code to come into force, the IMO continued to keep a tight overview of the progress made towards implementation. Specifically, in the aftermath of the terrorist attacks in Madrid in March 2004, IMO member states were encouraged to seek speedy and early implementation. In his speech to the 12\textsuperscript{th} session of the sub-committee on Flag State Implementation, the new IMO Secretary-General Efthimios Mitropoulos, who took office in November 2003, reiterated the threat deemed to be posed by international terrorism captured in both main narratives, emphasising that:


\textsuperscript{111} Ibid., p. 11.

While the 1st July deadline constitutes a pact among Governments doing business in a civilized manner under the mutually binding provisions of a treaty instrument, this deadline means nothing to terrorists who may decide to strike wherever and whenever such an act might suit their evil purposes – and, have no doubt, they will do so if they assess that are defences are low or, to put it in a different manner, when they think that our defences are not high enough to prevent and deter them from committing any atrocities they may have in mind to commit against our industry, the international trade and world economy.  

As a final reminder the organisation also published statistics every five days during June 2004 showing the percentage of ships and port facilities which had had their security certificates/plans approved.

Moving along the policy chain, the responsibility for preparing for 1 July 2004 within the UK largely rested with those individual companies who owned and operated the relevant maritime infrastructure. This is because, as it was noted in the previous chapter, 70% of port capacity in the UK was privately owned and operated, just as the three cases utilised in this case study – Felixstowe, Holyhead and Tilbury are. Guidance and advice was provided by TRANSEC, the MCA and police officials, specifically SB ports officers, who collaborated with the intelligence services and the Security Service (MI5) specifically. It was TRANSEC in particular who had the responsibility for undertaking the initial port facility assessments. The policy network relating to UK maritime infrastructure security then was diverse, and besides ultimately encapsulating multiple levels of governance, also traversed both the public and private sectors. By briefly utilising the three cases which make up the

---


subsequent case study, further detail can be provided about the network, while a
greater sense of the impact of the code in this period can be seen.

Within the Port of Felixstowe, security activities on 1 July 2004 were primarily
undertaken by the Port of Felixstowe police. Empowered as Special Constables with
the full powers of an ordinary officer through section 79 of the Harbours, Docks and
Piers Clauses Act, 1847,115 this force of up to 27 officers are funded by the port
owner and operator Hutchison Port Holdings (HPH) Group, and conduct most
ordinary police functions on or within a mile of the port.116 The commanding officer
of the port unit, a Chief Inspector, acts as the PFSO and works in partnership with a
senior company official who is CSO to develop and maintain the Port Facility
Security Plan. The port police are supported in their duties by private security
personnel, employed as a direct result of the changes introduced by the ISPS code,
who monitor gates and conduct basic searches of selected vehicles leaving the port.
They are also funded by the HPH Group.117

At the Port of Tilbury in Essex, the situation is complicated slightly by the diversity
of both operations and tenants working out of the port. Alongside container
transportation, the port also serves as one of the largest grain terminals in the United

115 See ‘Harbours, Docks and Piers Clauses Act’, Royal Assent 11 May 1847, accessed 17 July 2009,

116 Information ascertained from an interview. Note that throughout this thesis the description ‘port police’ will
refer to private police forces, while ‘SB ports officers’ will refer to those officer’s attached to Home Office
forces.

117 Information ascertained from an interview.
Kingdom and welcomes cruise liners during certain months of the year. It is owned by Port of Tilbury London Ltd a subsidiary of Forth Ports PLC. As with Felixstowe, security operations are co-ordinated by a privately funded police team, the Port of Tilbury police, who are sworn in as constables under the Port of London Act, 1968.\textsuperscript{118} There are approximately 19 officers in this force, and while their jurisdiction is limited to the port itself, the act does provide the power to continue the pursuit of an individual from the port throughout the UK if that is required. At Tilbury, the PFSO is not a serving port police officer but a separate individual working out of the port police station. Once again a private security company are responsible for security patrols, most vehicle searches and the control of access points. Unlike Felixstowe however they serve only at Tilbury and are not part of a larger company. The number of private security personnel at the port more than doubled due to the requirements placed on the port through the ISPS code from approximately 30 to 70 staff.\textsuperscript{119}

Security operations at the Port of Holyhead in Anglesey are markedly different compared to the other two cases. Operated by Stena Line Ports Ltd, Holyhead is predominantly focused on passenger services provided through roll on-roll off (RO-RO) ferry routes between Wales and the Republic of Ireland. The routes fall within the Common Travel Area (CTA) which means that there is no consistent requirement for passport checks of Irish citizens travelling in to the UK, adding a further


\textsuperscript{119} Information ascertained from an interview. The author is grateful to one interviewee for providing a book that outlined the history of the Port of London Authority Police. Glyn Hardwicke, \textit{Keepers of the Door} (London: Peel Press on behalf of the Port of London Authority Policy, 1980).
Due to its relatively small geographic size in comparison to the other two cases, the entire port is regarded as a restricted area. There is no designated, privately funded port police force and as a result security is provided by a combination of private security personnel and North Wales Police Constabulary SB ports officers. The PFSO is the Port Manager, a senior Stena Line official. Although North Wales Constabulary plays a more active, day to day role in security operations at Holyhead, the management and investigation of major incidents and serious crimes, and intelligence gathering operations at each port, are ultimately the responsibility of the specific Home Office force and their SB ports officers specifically. At Felixstowe this responsibility falls upon Suffolk Constabulary, while at Tilbury it falls on Essex Constabulary. Finally Customs and Excise and Immigration officials, some of whom would later merge in to the UK Border Agency, also operated out of each site on 1 July 2004.

For an outsider the most visible impact of the changes brought about by the ISPS code was the introduction of new infrastructure – additional fencing, access gates and an expansion of Closed-circuit Television (CCTV) coverage - to enhance the protection of the port-ship interface. None were wholly new developments, but the pressures imposed by the ISPS code to place security considerations at the centre of day-to-day activities ultimately led to higher quality infrastructure being installed

---


121 Information ascertained from an interview.
across the board in the form of stronger fencing and more powerful cameras.\textsuperscript{122} This imposed a significant additional cost to port operators. At the Port of Felixstowe for example, approximately £1 million of new fencing alone was purchased and erected in the run up to 1 July 2004.\textsuperscript{123} The costs imposed by the ISPS code were further increased by the combined requirement to employ, train and maintain a larger number of security personnel to monitor the restricted zones and conduct security operations throughout the port as a whole, and through the installation and management of improved ID card systems, including more use of technology, for all port staff.\textsuperscript{124} The running costs would ultimately be met, partially at least, by the introduction of security charges to shipping companies. The UK’s long-standing ‘user-pays’ principle in maritime infrastructure security meant there was little to no financial support provided from central government.

While the ISPS code represented the main emergency measure implemented by the policy network as a result of the securitisation of UK maritime infrastructure, it was by no means the only element of the counter-terrorism security response. Recognising once again both that counter-terrorism efforts in the UK have their own genealogy, particularly in relation to counter-terrorism efforts in Northern Ireland, and the ‘vulnerable node’ narrative that highlights maritime infrastructure’s position as say, part of the wider UK border, the code built upon and sat alongside other

\textsuperscript{122} Author’s interview with number 7, 18 March 2009. The fact that TRANSEC set specific conditions to port operators in terms of height of fences and use of CCTV is noted in a Memorandum submitted by the United Kingdom Major Ports Group to a House of Commons report on transport security. House of Commons Transport Committee, \emph{Transport Security: Travelling without Fear (Oral and Written Evidence)} (London: The Stationery Office Ltd, 9 January 2008), TS 22, accessed 22 September 2009, \url{http://www.publications.parliament.uk/pa/cm200708/cmselect/cmtran/191/191we01.htm}.

\textsuperscript{123} Information ascertained from an interview.

\textsuperscript{124} Information ascertained from interviews.
measures. Most evident in terms of legislation, the Aviation and Maritime Security Act, 1990 specifically continued to serve as the source of a range of powers relating to maritime security in 2004.\textsuperscript{125} For example, covering RO-RO ferries, passenger vessels and the ports which served them, it enabled the Secretary of State for Transport to designate a particular area or an entire harbour a restricted zone, providing powers to conduct searches of vessels and buildings within those areas and made it an offence to make a false statement relating to any baggage, cargo or stores under investigation.\textsuperscript{126} Alongside this, general counter-terrorism and civil contingency legislation introduced after September 2001 and outlined earlier in the chapter also covered the infrastructure. For example suspects located within a Port could be detained under the Terrorism Act, 2000.

\textbf{(2.5) Conclusion:}

In charting the way in which UK maritime infrastructure was securitised in the context of the macrosecuritisation of the ‘civilised way of life’, captured in the ‘war on terror’ discourse of counterterrorism, it has been possible to place the case study in its immediate historical context. This provides a base point from which both discourse and practice can be examined in even greater detail over the course of the following three chapters. In terms of the post-securitised environment specifically, in relation to UK maritime infrastructure, the scene evident here was one which closely mirrored that seen in relation to the UK’s domestic counter-terrorism efforts as a whole. Its prominent features then were similar and represent a series of early trends to look for when examining practice in the case study itself.


\textsuperscript{126} Ibid., specifically Part III, in particular Sections 20, 22, 23, 37 and 38.
Although it was intended to tackle presented threats beyond international terrorism, the ISPS code undoubtedly emerged in a policy environment that was dominated by the idea of a ‘war on terror’. As a result, counter-terrorism considerations increasingly took centre-stage framing the actions of the policy network relating to UK maritime infrastructure. As the clearest manifestation in practice of the securitisation of maritime infrastructure, the ISPS code illustrated the way in which the use of formal, legally enforceable solutions with counter-terrorism implications, here new regulations, were turned to. The code resulted in an increase in state power as through TRANSEC in particular, as the designated authority for security, the British state gained additional responsibilities and influence relating to UK maritime infrastructure, having oversight over Port Facility Security Plans for example. Port owners also saw their power relating to maritime infrastructure increase as the introduction of access zones meant they could monitor and control the movement of people and goods within their port more effectively, all in the name of enhanced security.

The requirement for different actors to work more closely together to, both within and outside of the UK to prepare for the code coming in to force, illustrated the way in which further enhancing co-ordination between members of the policy network was deemed to be crucial to effective counter-terrorism. The additional expense incurred by port owners in putting in place the necessary infrastructure and security procedures demanded by the ISPS code required a growth in those budgets put aside for maritime infrastructure security. The increased use of private security personnel to deliver the code also contributed towards ensuring the activities of those charged
with maintained security gained an even higher profile in the day-to-day life of a port.

The way in which these developments were underpinned with a notable sense of urgency, associated with securitisation and seen in the UK’s domestic counter-terrorism efforts as a whole, was also clear. The initiation of policy discussions just a month after the 11 September 2001 terrorist attacks, the development and agreement of the content of the ISPS code 14 months later, and the requirement that member states undertake the necessary preparations and comply with the code just 18 months after this, represented a somewhat truncated timescale relative to previous efforts at implementing internationally binding regulations. The continued pressure imposed by the IMO on its member states to deliver on their ISPS commitments, specifically after the Madrid bombings, through the publishing of regular compliancy statistics was further evidence of this.

This high level of cross-over between the features of the UK’s domestic counter-terrorism efforts as a whole and those efforts relating to UK maritime infrastructure in this period, serves only to emphasise the close relationship between the macro-securitisation of the ‘civilised way of life’ and the securitisation of UK maritime infrastructure. On one level this was not particularly surprising as on a number of occasions those actors doing the implementing – the policy network responsible for the counter-terrorism security response relating to UK maritime infrastructure security – were those also responsible for counter-terrorism generally such as the
Police through their Special Branch’s. The chapter did however illustrate the multi-levelled structure of the UK maritime infrastructure policy network, with both the IMO and EU involved. This serves as a valuable reminder of the way in which UK ports and harbours represent part of an international, inter-connected maritime industry.

Ultimately this chapter has started the process of demonstrating just how and why the relationship between the macrosecuritisation of the ‘civilised way of life’ and securitisation of UK maritime infrastructure can be understood as mutually reinforcing. The ‘war on terror’ discourse, which captured the macrosecuritisation, led counter-terrorism considerations to take centre-stage in terms of both foreign and domestic policy. This in turn constructed a policy environment in which UK maritime infrastructure was itself deemed to be in need of ‘securing’, as the threat presented to be posed by international terrorism had to be tackled at every opportunity. The subsequent production and reproduction of the ‘target’ and ‘vulnerable node’ narratives, which were drawn from the macrosecuritisation and presented the threat posed by international terrorism to maritime infrastructure specifically, created the space and the rationale for the development and introduction of emergency measures such as the ISPS code. These narratives, the emergency measures which emerged, their delivery and impact, all then served to reiterate the idea that international terrorism was an existential threat, thus reinforcing the macrosecuritisation.
In the next chapter the detailed case study begins. Acknowledging the natural time lag between the initial implementation of emergency measures and the point at which an assessment of their impact becomes clearer, it examines developments relating to UK maritime infrastructure from the point at which the ISPS code came into force on 1 July 2004 and over the subsequent 12 months. As with each part of the case study, the central objective of the chapter is to shed further light on the post-securitised environment and chart just what impact securitisation had on the management of UK maritime infrastructure. To do this the chapter first demonstrates how the wider policy environment in which UK maritime infrastructure was securitised and discussed here, did not fundamentally change in this 12 month period. The ‘war on terror’ discourse and the macrosecuritisation it captured remained stable despite evidence of moments of resistance. As a result members of the policy network increasingly emphasised the need to maintain constant vigilance and no complacency with regards to the presented terrorist threat. This emphasis energised the continual process of reflection undertaken right along the policy chain in relation to the existing counter-terrorism security response and ensured perceived gaps and weaknesses related to it were highlighted to be addressed. The result was that attention fell first on ensuring there was full and proper compliance with the ISPS code and that it became further institutionalised in practice, and second that where necessary the counter-terrorism security response would evolve and expand in scope.
Effective implementation of the ISPS Code will improve security. What will make it effective is not just the initial enthusiasm for increased security but a dogged determination to continue to exercise review and improve procedures.¹²⁷

(John Astbury, Chief Coastguard, United Kingdom, February 2004.)

(3.1) Introduction:

The previous chapter placed the case study in its immediate historical context arguing that the pursuit of a ‘war on terror’ facilitated the implementation of a series of foreign and domestic policies that were justified by the ‘necessity’ to secure the ‘civilised way of life’ against an existential threat presented as being posed by international terrorism. As counter-terrorism considerations increasingly took centre-stage in terms of policy, and in the United Kingdom (UK) counter-terrorism moved to the top of the domestic policy agenda influencing growing areas of life, maritime infrastructure was itself securitised. Representing a ‘site of securitisation’ where everyone, everything, and all activities associated with this space are presented as requiring securing against presented threats, the policy network responsible for

policy relating to UK maritime infrastructure, which itself extended over multiple levels of governance, produced and reproduced two main narratives presenting that infrastructure as both a ‘target’ and ‘vulnerable node’. These narratives helped facilitate the implementation of emergency measures, specifically the International Ship and Port Facility Security (ISPS) code, which was implemented as a ‘necessary’ response to the presented threat. Representing the clearest manifestation in practice of the securitisation of UK maritime infrastructure in the post 11 September 2001 period, the ISPS code imposed a new security regime on the maritime industry internationally, amongst other things creating restricted zones, requiring Port Facility Security Officers (PFSOs), demanding the design of security plans and introducing a new three tiered threat level system to the maritime environment.

This third chapter represents the beginning of the three-part, detailed examination of the securitisation of UK maritime infrastructure in the context of responses to international terrorism, with particular focus placed on examining the impact of securitisation on the management of that infrastructure by reorienting research emphasis towards the post-securitised environment. It focuses on developments in the 12 month period between 1 July 2004, when the ISPS code formally came in to force, and 6 July 2005, the day before the terrorist attacks in London. The chapter argues that in this period the wider context in which UK maritime infrastructure was securitised remained fundamentally unchanged. The ‘war on terror’ discourse, which captured the macrosecuritisation of the ‘civilised way of life’, remained stable in so far as it remained generally resilient to resistance and unchanged in form. This was also the case in relation to the securitisation of UK maritime infrastructure.
specifically, where both main narratives remained evident and were reproduced widely. There continued to be resistance, but it was predominantly directed at particular counter-terrorism practices rather than against the ultimate rationale for them. What did become clearer in this period however was the way in which both acts of resistance and particular events provided the opportunity for further reiteration of the presented threat from international terrorism and all those narratives that drew upon it.

This stability ensured that the emphasis from the policy network on maintaining constant vigilance and no complacency with regards to the presented threat remained. This in turn energised the continual process of reflection undertaken right along the policy chain in relation to the existing counter-terrorism security response, ensuring perceived weaknesses and gaps related to it were highlighted to be addressed. Specifically discussions centred on how prescriptive the response should be and coalesced around the need to maintain three balances – between security and commercial operations, between security and liberty, and over who had what responsibilities in relation to the response. Subsequently the attention of the policy network primarily fell on further institutionalising the counter-terrorism security response, captured most effectively in the institutionalisation of the ISPS code itself. Institutionalisation here is understood as the process of embedding particular activities, roles, even ideas in day-to-day operations so as they become like second nature. Here, the chapter argues, institutionalisation was pursued primarily through efforts to ensure universal compliance with emergency measures and the harmonisation and improvement of security standards.
By illustrating this emphasis on institutionalisation the chapter sheds further light on the prominent features of the counter-terrorism security response, some of which were raised in the previous chapter. This demonstrates the way in which each chapter in this thesis builds upon the previous one providing additional details and a more complete picture of what, in this case, securitisation did in practice. In particular additional insights are highlighted in relation to the focus on enhancing co-ordination between members of the policy network, at all levels of governance. Beyond this, a clear desire on the part of the policy network to increasingly utilise technology to enhance security became apparent.

Continuing to recognise the way in which the study of the content, delivery and impact of emergency measures is intertwined, the features of the response are elaborated by ensuring the practices themselves remain the focal point of the case study. As chapter one explained the totality of counter-terrorism practice is subdivided in to three broad constituent parts – ‘legislation and regulations’, ‘institutional changes and infrastructure developments’ and ‘working practices’ - with the three cases of Felixstowe, Holyhead and Tilbury acting as individual cases to provide additional focus. The chapter concludes by highlighting how a picture emerges of a counter-terrorism security response that can be said to have three main characteristics to it. First it constantly evolved, second it was layered and third and most prominently it was increasingly expansive in scope as counter-terrorism considerations shaped a growing range of day-to-day activities within UK maritime infrastructure. The response did then seem to mirror the presented threat it was supposed to tackle.
(3.2) Resistance and reiteration – the stability of the ‘war on terror’ discourse:

The continued securitisation of UK maritime infrastructure in this period and the reproduction of the two main narratives relating to it, was to a large extent unsurprising when one takes in to account the mutually reinforcing relationship with the macrosecuritisation of the ‘civilised way of life’ and the stability of this discourse of counter-terrorism. Returning again to the signs of audience acceptance of securitisation, western political leaders reiterated the existential threat presented as being posed by international terrorism. For example, Franco Frattini, Vice President of the European Commission reminded the European Parliament of the zero-sum nature of the threat, arguing that terrorism was “the new tyranny of the 21st century, a tyranny which seeks to limit our freedoms and attack people’s fundamental rights.” In the UK, high-profile government figures such as Home Secretary Charles Clarke told Parliament, despite three years having passed since 11 September 2001, that there remained “a public emergency threatening the life of the nation”.


As 1 July 2004 had approached, wider concern about international terrorism was also evident from members of the general public in the UK. Opinion polling suggested that the fight against international terrorism remained of the highest priority for the public, although this perhaps was not particularly surprising after the recent terrorist attacks in Madrid. A MORI poll published in March 2004, found that 41% of those questioned agreed that ‘defence/terrorism’ was the “top issue facing the country” at the time.\(^{130}\) As company Chairman Sir Robert Worcester noted in his accompanying analysis, this had been the first time since March 2003 (the start of the Iraq War) that ‘defence/terrorism’ had occupied this top spot.\(^ {131}\) Although only a snapshot of opinion at one specific time, a little over a month later a further poll suggested widespread support for a range of counter-terrorism practices that realistically could be described as exceptional in both their content and scale. Support for the indefinite detention of foreign suspects stood at 62%, 59% supported bringing in the death penalty for terrorist offences which killed people, and 66% agreed that immigrants and asylum seekers should be detained until they could be assessed as potential terrorist risks.\(^ {132}\)

Once again it was continued counter-terrorism efforts that provided the clearest evidence that the desire to pursue a ‘war on terror’ remained largely unabated. Internationally, military operations in both Afghanistan and Iraq continued, stabilising post-war Iraq was presented as being a ‘must win’ component of tackling


\(^{131}\) Idem.

the wider threat posed by international terrorism. Regionally, the European Union (EU) continued towards developing its own counter-terrorism strategy. Driven by the Madrid attacks in particular, an updated ‘Anti-terrorism Action Plan’ was written and an EU Counter-terrorism Co-ordinator appointed. A number of additional developments emerged out of this plan in the following months, including the launch of an EU External Borders Agency - Frontex. In the UK the government did, amongst other things, continue to turn to legislation introducing the Civil Contingencies Act, 2004, the Identity Cards Bill, 2004, the Prevention of Terrorism Act, 2005 and the Serious Organised Crime and Police Act, 2005, all of which had some counter-terrorism implications and increased state power.


There remained evidence of resistance, yet as noted in the previous chapter, it was largely directed against particular counter-terrorism practices rather than against the idea that there was an existential threat that required tackling. To more explicitly return to the terminology of the Copenhagen School, resistance was then largely directed at the content of particular emergency measures, how they had been delivered and the perceived negative impact they were deemed to have had, rather than at the idea that emergency measures were necessary in the first place. This form of resistance emerged out of the process of continual reflection which is inherent in all policy making. More specifically the process was framed by questions such as ‘Is the existing counter-terrorism security response working?’ and ‘What, if anything, should come next?’ that in turn facilitated a series of ongoing discussions. This reflection was predominantly undertaken by the relevant policy network and occurs alongside the continual negotiation and contestation of discourse.

Focusing on the UK, specific counter-terrorism efforts were placed under more sustained and public scrutiny. Political leaders, for example, increasingly found themselves being required to defend the progress of operations in Iraq to Parliament. On one occasion in November 2004, amidst rising British military casualties and a US-led attack on the Iraqi city of Falluja, Tony Blair sought to make the case for continued operations stating that, “defeat of terrorism in Iraq is defeat
for this new and virulent form of global terrorism everywhere\textsuperscript{138}. Like Frattini noted earlier, Blair continued to advance his case by dividing the world into two diametrically opposed sides – those who sought to defend democracy and those who sought to undermine it; the ‘war on terror’ discourse then was fundamentally unchanged. He argued that:

\begin{quote}
a democratic Iraq is the last thing the terrorists want to see. It is precisely for that reason—because victory for the terrorists would damage security around the world, including here in Britain—that we have to hold firm, be resolute and see this through, including in Falluja.\textsuperscript{139}
\end{quote}

The reference to Britain reminded a sceptical public of the relevance of operations in Iraq to their daily lives.

Despite such defiance resistance continued. At one point opposition Plaid Cymru MP Adam Price even went as far as launching an attempt to utilise historic powers of impeachment, previously used in 1806, to remove the Prime Minister. The grounds for such action were that he had misled Parliament and the country over the reasons for going to war with Iraq. The attempt eventually floundered, but not before it had garnered considerable media attention and the support of just over 20 MPs.\textsuperscript{140}

Interestingly when compared to the general concern over defence and international terrorism highlighted earlier in this section, a series of ICM polls also showed that

\textsuperscript{138} Tony Blair, ‘EU Summit’, House of Commons, 8 November 2004.


139
over the course of the year public support for operations in Iraq steadily declined. In March 2004 48% of those asked thought that military action was right as opposed to 43% who said it was not. In January 2005 just 38% of respondents felt that the war was justified compared to 47% who felt it was not. In April 2005, a matter of weeks before the UK General Election, a further poll suggested that only 22% of the public regarded the War in Iraq as a success compared to 72% who regarded it as a failure. Despite differences in the specific questions being asked, the broad trend of falling support for this particular conflict was clear.

Resistance was not isolated to the international dimension of the response. There were similar acts of resistance against domestic counter-terrorism efforts which again did not result in any substantial move away from the idea that terrorism posed an existential threat to the ‘civilised way of life’. This distinction in the form of resistance was unwittingly highlighted by an opposition Liberal Democrat MP Mark Oaten, as he criticised the government’s policy on the detention of foreign terror suspects. He stated that:

The Liberal Democrats in no way underestimate the seriousness of the threats facing this country. The fact that we differ from the Government on how to tackle those threats does not mean that we do not recognise that the world has changed since 9/11 and that we now face a different problem of international terrorism.


Another measure resisted was the Identity Cards Bill, a bill which proposed the introduction of a new system of biometric card in the UK. It was critiqued, to provide three examples, on the grounds that it would not have prevented a terrorist attack such as Madrid, that it negatively changed the relationship between the individual and the state, and that the material encapsulated within the card could be tampered with. A third measure resisted was the government’s attempt to seek updated emergency powers through the Civil Contingencies Act to be able to pass and/or amend laws during a state of emergency without the requirement for a full Parliamentary vote. One pressure group described the act as “Britain’s Patriot Act”, yet the law was still ultimately passed.

There was certainly no tipping point then in these twelve months where the individual acts of resistance came together to destabilise the macrosecuritisation in a fundamental way. The continued centrality of counter-terrorism considerations

---


outlined in this section is proof of that. What was also noticeable was how the resistance provided political leaders with increased opportunities to be able to reiterate the presented threat from international terrorism, facilitating the continued emphasis on maintaining constant vigilance and no complacency in relation to it. Demonstrating the way in which counter-terrorism efforts would build upon each other too, this was most apparent in the government’s defence of the Prevention of Terrorism Act in spring 2005. The proposed bill included an adaptation of detention powers that had been encapsulated in the 2001 Anti-terrorism, Crime and Security Act, an act that, as chapter two explained, allowed the Home Secretary to detain without charge foreign nationals suspected of terrorism, who could not be extradited because of human rights concerns. These provisions were struck down by the House of Lords in December 2004. One reason for this decision was that they were deemed to be discriminatory, facilitating as they did the detention of non-British individuals in isolation. Commenting on the Law Lord’s decision, Tony Blair took the opportunity to reiterate the extent of the terrorist threat, telling MPs:

We are desperate to avoid a situation in which, later, people turn round and say, ‘If only you’d been as vigilant as you should have been we could have averted a terrorist attack.’ I think it is right to call this a new form of global


terrorism—it is different. Let us be clear: 200 people died in another European capital city, Madrid, but if the terrorists’ plan had succeeded, they might have killed more than 1,000 people. That is the difficult balance that we are trying to strike. I entirely agree that we have to strike it so that there is respect for civil liberties as well as our security. We have tried to do that.\footnote{Tony Blair, ‘Prime Minister’s Questions’, House of Commons, 2 February 2005, Hansard column 832, accessed September 2010, http://www.publications.parliament.uk/pa/cm200405/cmhansrd/vo050202/debtext/50202-03.htm#50202-03_spnew7.}

The proposed bill shifted emphasis from detention to a new system of control orders, a system that enabled a variety of restrictions to be placed on the movement and activities of both British and foreign nationals suspected of involvement in terrorist activity.\footnote{Individuals could be placed under effective house arrest, be electronically tagged and be prohibited from using mobile phones and the internet. Each control order lasted 12 months but could be renewed indefinitely, a system of security-cleared ‘Special Advocates’ were tasked with representing the interests of the accused in proceedings held in closed-sessions. See ‘Prevention of Terrorism Act’, Royal Assent 11 March 2005. For a description of the system see Dominic McGoldrick, ‘Terrorism and Human Rights Paradigms’, pp. 145-154 and Clive Walker, ‘Keeping control of terrorists without losing control of constitutionalism’, Stanford Law Review, 59:5 (2007), pp. 1408-1446, accessed November 2010, http://heinonline.org/HOL/Page?handle=hein.journals/stflr59&div=44&g_sent=1&collection=journals.} This itself was resisted for being too draconian, a position the then Home Secretary Charles Clarke responded to in unrelenting terms:

> Some believe that the absence in this country of a terrorist outrage such as 9/11 or Madrid means that the terrorist threat has somehow passed us by or failed to materialise. That view is short-sighted, complacent, ignorant of the facts and potentially cavalier in its disregard of the safety of this country.\footnote{Charles Clarke, ‘Prevention of Terrorism’, House of Commons, 22 February 2005, Hansard column 151, accessed September 2010, http://www.publications.parliament.uk/pa/cm200405/cmhansrd/vo050222/debtext/50222-05.htm#50222-05_spmind. Italics added by author to emphasise point.}

As with the Civil Contingencies Act the resistance did not prevent the Bill becoming law although there were concessions.\footnote{The main concession made was to promise that MPs would be able to review, within 12 months, a new counter-terrorism Act that was being drafted. According to the opposition Conservative Party this was the “sunset clause” they had demanded in all but name. ‘Government’s Terror Bill Passed’, BBC News Online, last} It took just 18 days between the government
introducing the bill before Parliament and it gaining Royal Assent, demonstrating the notable sense of urgency once more.\textsuperscript{152} This example also illustrated the intertwined relationship between the impact of securitisation and audience acceptance, emphasising the process in securitisation. Whilst emergency measures can only be introduced or at least become possible if an audience accept that a referent object is existentially threatened, audience reflection on the response can subsequently shape both how that audience acceptance is specifically sought in the future – which dimensions of a presented threat for example are highlighted - and what other measures are implemented.

\textbf{(3.3) UK maritime infrastructure as a ‘site of securitisation’:}

In the 12 months after the ISPS code came in to force then there were very few changes in the wider context whereby the ‘war on terror’ discourse continued to shape the policy environment, placing counter-terrorism considerations centre-stage. Within the UK, counter-terrorism efforts as a whole still, most prominently, featured the introduction of new legislation with counter-terrorism implications that in turn further increased state power, while a notable sense of urgency still underpinned developments. Shifting attention to UK maritime infrastructure in more detail, whilst again acknowledging the multi-levelled governance of the maritime industry, the two

\begin{footnotesize}
\end{footnotesize}
main narratives – ‘target’ and ‘vulnerable node’ – continued to be reproduced in this period by political leaders with some responsible for policy relating to UK maritime infrastructure.

In a speech delivered in May 2005 for example, IMO Secretary-General Efthimios Mitropoulos reiterated how the 11 September 2001 attacks had “shocked and outraged the entire civilized world”, “reminded us of how truly integrated our global society has become” and “brought home to us all the vulnerability of transport networks and the potential they held to be either targets or the instruments of terror.”\(^{153}\) European Commission Vice-President Jacques Barrot argued that “the recent wave of terrorist attacks has demonstrated that no country or business sector is immune to such threats. Whatever their motives may be, these terrorist acts can occur in any place, at any time. The maritime world and port environment do not escape such threats, and we cannot wait for an attack before we take what are essentially preventative measures within the transport policy framework.”\(^{154}\) A UK government White Paper on the future of transport simply noted with considerable brevity that “the tragic attacks in the USA in September 2001 and, more recently, in Madrid in March 2004, have changed forever the context for transport security around the world.”\(^{155}\)


What did become more noticeable however was the way in which these narratives were also reproduced more widely by other members of the policy network. To recap the policy network included those political leaders noted earlier, parliamentarians, civil servants, security professionals both state and privately funded such as the police (particularly Special Branch ports officers) and port private security guards, alongside the maritime industry as a whole, especially port owners and their senior management teams; all with an interest in and some responsibility for the counter-terrorism security response relating to UK maritime infrastructure.

Writing in the security magazine INTERSEC, Henk van Unnik, President of the International Association of Airport and Seaport Police, made his own assessment of the security challenges facing seaports. He reminded his readers of the widespread negative consequences economically an attack on maritime infrastructure could have noting, amongst other things, that “an estimated 80% of international commerce (5.1 billion tons) worth US$5 trillion moves by sea annually”.\textsuperscript{156} Justin Priestly of brokering group Aon was reported as telling a meeting of the International Union of Marine Insurance that the maritime industry was facing adherents willing to die for the cause, and that ports faced both the risk of falling victim to multiple truck bombs and/or cyber terrorism hitting IT systems.\textsuperscript{157} The Deputy Director of the UK Transport Security and Contingencies Directorate (TRANSEC) John Grubb, told an audience at a Transport Institute conference in Japan of three principle threat


scenarios relating to smaller vessels. They could be targets of an attack, they could be used to transport personnel and equipment (either terrorist owned or hijacked), or they could be used as a weapon.\(^{158}\)

The way in which particular events, like resistance itself, created the space for further reiteration of the presented threat was also evident in this period. Briefly raised in the previous chapter, the terrorist attacks in Madrid continued to have an impact. Although they pre-dated this time period and targeted the rail network, they were utilised as a reminder of the difficulties involved in trying to secure open transport networks which are characterised by and even rely upon large-scale, often last minute and unplanned movements of both passengers and cargo.\(^{159}\) Although not open to the extent rail networks are, maritime infrastructure, particularly passenger terminals, rely on the fast turnaround of vessels and being convenient for passengers. There are no airport demands to arrive hours before departure. At the Port of Holyhead for example, passengers can arrive as little as 45 minutes before departure.\(^{160}\) Such relative flexibility was on occasion highlighted as a vulnerability that could be exploited by terrorists. In 2004 the Shadow Homeland Security Minister Patrick Mercer asked the government to confirm the extent to which the Civil Contingencies Act empowered them to be able “to require ports, airports, and local authorities to purchase equipment designed to identify the presence of […]


CBRN material – and to deploy it at ports and airports.” His view was that “with the exception of some areas we are wide open to equipment being brought into this country”.

The 2005 General Election campaign was another event which facilitated discussions over security. The opposition Conservative Party embraced the slogan “It’s not racist to impose limits on immigration” arguing that the government had “lost effective control of our borders”, calling amongst other things, for “24-hour surveillance at our ports” and the restoration of “full embarkation controls”. The links between illegal immigration, international terrorism and maritime infrastructure were suggested more explicitly in the maritime journal Fairplay. It raised questions over continued weaknesses in European port security, positioning openness as a major vulnerability and discussing the “chaos” that could be wielded from the smallest border infiltration:

Most European ports have also made themselves ISPS compliant, although that does not mean they are immune from infiltration by terrorists or criminals: one only has to consider how successfully tens of thousands of asylum-seekers manage to enter Western Europe every year and then disappear into the black economy. And in the case of terrorism, it takes just one person, or a small well-organised team, to slip through the net and create chaos. That’s more likely to happen in or near a port than on a ship plying the high seas. Certainly European Ports have tried hard to comply with the ISPS Code. That’s because their future success, or even their survival, depends upon it.


As with the macrosecuritisation of the ‘civilised way of life’ there was resistance. On the rare occasion it was even directed more explicitly at the presented threat. One UK seafarer in a letter published in the maritime newspaper Lloyd’s List wrote:

is it not time to question the huge cost to the maritime industry and to tax payers if this threat is overstated? Surely the truth is that there has been remarkably little terrorist actions against merchant shipping? [...] Looked at from the potential terrorist viewpoint, there are also clearly much more productive uses for scarce human and financial resources than attacking shipping.\(^\text{164}\)

Although related to international shipping specifically rather than the infrastructure which served it. As inextricably interlinked components of the maritime industry such resistance illustrated the existence of critical voices, voices concerned the threat was being exaggerated. Another seafarer followed a similar line of argument writing:

we in Britain suffered decades of sustained IRA terrorism, yet again I assume the authorities considered the security in place adequate. Now with ‘supposed’ possible terrorist attacks common sense has been sacrificed with a blanket of restrictive legislation.\(^\text{165}\)

As a whole though this form of resistance was rare. Rather again, as with the macrosecuritisation, resistance was largely directed against particular elements of the existing counter-terrorism security response and future proposals relating to them. Here one of the previously quoted seafarers emphasised his concerns over the impact the ISPS code had had on seafarer rights, writing that he had never found himself “so restricted in my freedom of movement”, and arguing he was “yet to come across


anyone who does not believe that the whole matter of port security should lie firmly with the port and not with the under-manned over-worked ship’s staff”. He signed off his letter “Yes God Bless America – land of the free – give me a break”.

(3.4) UK maritime infrastructure – the post-securitised environment:

Further elaborating this resistance against elements of the counter-terrorism security response itself marks the beginning of the transition in this chapter from examining discourse as the focal point towards practice, representing the desired shift in research emphasis towards the post-securitised environment. As with that resistance directed at the UK’s counter-terrorism efforts as a whole, noted in the first section of this chapter, this resistance came out of the continual process of reflection associated with all policy making. It was a process that was energised by macrosecuritisation, the reproduction of the ‘target’ and ‘vulnerable node’ narratives, and the resultant emphasis on maintaining constant vigilance and no complacency in relation to the presented international terrorist threat. Again the two broad questions, ‘Is the existing counter-terrorism security response working?’ and ‘What, if anything, should come next?’ were the starting point for reflection with a series of ongoing discussions emerging from these.

With regards to the ISPS code in particular, which remained the centre-piece of the counter-terrorism security response relating to UK maritime infrastructure in this period, discussions coalesced around the need to maintain three balances. The first

balance was between security and commercial activities, the second was on the need for balanced treatment of seafarers which did in essence represent a call for balance between security and liberty, while the third was for a balance over who had what responsibilities in relation to the implementation of the response, here between shore and ship personnel. The focus on these balances did not suddenly emerge on 1 July 2004, and each continued to be salient well beyond July 2005.167

The first balance between security and commercial activities was particularly prominent as the financial costs of delivering and maintaining the counter-terrorism security response became increasingly clear. Internationally for example there were notable discussions over the extent to which the burden of security costs should and would be passed on along the supply chain. In Asia a ‘Far Eastern Freight Conference’ was called to discuss what, if any, surcharge should be charged by container lines to recoup the monies they were paying to a number of container ports.168 In the UK where the owners of Felixstowe, Hutchison Port Holdings had led the way before 1 July 2004 in introducing a security surcharge, similar discussions and complaints over who met the financial burden of implementing the response were somewhat tempered by the long established ‘user pays’ principle. Despite this there remained an underlying sense of powerlessness on the part of the industry – a

---


feeling that in reality discussion over this issue was far more limited than the media may have suggested. As one UK port manager commented when asked about the domestic debate over ISPS code costs:

there wasn’t very much discussion; it was made very clear that costs lie where they fall. There was no discussion about it; there was lots of media comment but there was no discussion. TRANSEC made it very clear that costs lie where they fall.169

The second balance rested on concerns that in the pursuit of security the freedom of seafarers, to specifically take shore-leave was increasingly being challenged. In November 2004, a Lloyd’s List editorial entitled ‘A Polite Society’ argued, without suggesting a location, that the treatment of seafarers was falling short of what was expected:

On the matter of access controls, there are reports of unpleasant encounters between ship security staff attempting to follow their own procedures and officials behaving like arrogant bullies, refusing to produce identity cards or presenting false ID, refusing escorts, demanding that the whole crew assemble for their inspection and leaving gangways unmanned [...] from reading the reports by shipping organisations, it is notable that so many of these problems stem from sheer bloody-mindedness on the part of brainless officials and put-upon seafarers who are trying to follow procedures.170

The United States (US) was particularly accused of limiting the seafarer right to shore-leave. Both seafaring and ship owner trade unions joined forces to deliver a statement that pledged to utilise the 2004 World Maritime Day to “back the day’s aim of encouraging improved security and to remind governments – especially in the United States – that this is best achieved by working together, not by treating visiting

169 Author’s interview with number 11, 3 March 2010.

seafarers as potential terrorists.”\textsuperscript{171} At one point it was even reported that the UK’s Princess Anne had sought assurance that seafarers did not suffer from the “over-zealous interpretation” of the code.\textsuperscript{172}

The third balance over who had what responsibilities in relation to the counter-terrorism security response, centred on an impression that on certain occasions there had been a lack of understanding between personnel on ships and ashore over their respective interpretation of the ISPS code and required security duties more generally. One director for quality assurance and training at a shipping group even went as far as to argue that in some locations “seafarers do not see the checking of ID cards and bag searching as their job, especially when the port facility security in many ports is laughable. There are numerous reports of ‘superficial’ security measures in many ports.”\textsuperscript{173} There was no specific evidence to suggest that such a fundamental lack of understanding existed in the UK or that security measures in its ports were in any way “superficial”. Yet the existence of such tensions elsewhere serves as an important reminder of the multi-faceted character of the maritime industry. While this case study ultimately focuses ashore in the UK, fully examining the management of UK maritime infrastructure in the context of responses to


international terrorism requires focus to fall on looking beyond the infrastructure itself, to developments outwards to sea in relation to various vessels, within the various states where ships and containers have come from or further inland.

Alongside maintaining the three balances, discussion more generally fell on how prescriptive the counter-terrorism security response should be, although this was most explicitly the case in later years. Emerging out of this reflection and resistance members of the policy network sought to further institutionalise the existing counter-terrorism security response, particularly the ISPS code, in to day-to-day activities, whilst adding to and adapting the response where it was deemed necessary. To do this focus was placed on ensuring universal compliance and the harmonisation and improvement of security standards particularly through efforts to build wider security awareness and improve training.\textsuperscript{174} Overall there were few signs of any reversal in practice. As early as 1 July 2004 itself the IMO had stressed:

\begin{quote}
great emphasis has been placed on the entry-into-force date, but the real challenge is to ensure that, now that date has passed, \textit{we do not allow ourselves to relax and adopt any complacent attitude} [...] It will only be some time after 1 July 2004 that we will be able to establish clearly what the actual situation is and then, if necessary, start taking appropriate action.\textsuperscript{175}
\end{quote}

\begin{flushleft}

\textsuperscript{175} Efthimios Mitropoulos, Secretary-General, IMO quoted in ‘Secretary-General Mitropoulos pays tribute to the efforts made to implement the ISPS Code’, IMO Press Release, 1 July 2004, accessed 17 July 2009, \url{http://www5.imo.org/SharePoint/mainframe.asp?topic_id=848&doc_id=3698}. Italics added by author for emphasis.
\end{flushleft}
In February of the same year the UK’s Chief Coastguard John Astbury told a Maritime Security conference that “effective implementation of the ISPS Code will improve security. What will make it effective is not just the initial enthusiasm for increased security but a dogged determination to continue to exercise review and improve procedures.” On the ground in UK ports, the idea of further institutionalising the response, was for example, closely associated with further strengthening long-standing efforts to improve port safety. One Trade Union representative praised the introduction of greater security on access points, brought about by the ISPS code, for improving wider health and safety. This had occurred by reducing the incidents of individuals randomly wandering in to dangerous areas such as around cranes and heavy equipment. The focus on further institutionalising the existing counter-terrorism security response again demonstrated the element of process to securitisation as the reaction to how emergency measures had been implemented shaped subsequent practice as the national maritime security regulator TRANSEC, senior port management and security professionals in particular sought to address perceived gaps and weaknesses relating to that response.

To elaborate further the impact of securitisation on the management of UK maritime infrastructure, the totality of counter-terrorism practice is now sub-divided in to three constituent parts – ‘legislation and regulations’, ‘institutional changes and infrastructure developments’ and ‘working practices’. Developments in the three

---


177 Author’s interview with number 14, 9 December 2009.
cases of Felixstowe, Holyhead and Tilbury in particular are called upon to provide further depth and consistency to the examination.

(3.4.1) Legislation and regulations:

In legislative and regulatory terms, the ISPS code in particular had demanded a lot from those responsible for the security of UK maritime infrastructure both by formalising a variety of practices that were already taking place in relation to the ship/port interface security, and through additional requirements. At the international level during this 12 month period there was a concern that ports were compliant with ISPS requirements on paper only and that uneven security standards were being met. This was one reason why attention fell on ensuring universal compliance and the harmonisation and improvement of security standards. This approach was maintained domestically despite existing efforts at standardisation and an already mature maritime security regime. This suggested that the assessment of both compliance and standards was relative to a particular location and like counter-terrorism efforts overall, underpinned with the somewhat restless pursuit to do more. In short the response was deemed only to be as strong as its weakest link.


180 This regime was most centrally encapsulated in the ‘Aviation and Maritime Security Act’, Royal Assent 26 July 1990. By the time the ISPS code came in to force it was reported only one UK registered ship and a few port facilities were non-compliant. Moreover those ports which had not gained the necessary security certification had been deemed low risk by TRANSEC. See David Osler, ‘UK ports make ISPS progress’, Lloyd’s List, 31 March 2004, p. 2; Janet Porter, ‘UK admits some terminals miss deadline’, Lloyd’s List, 1 July 2004, p. 1 and David Osler, ‘UK vessel failed ISPS deadline’, Lloyd’s List, 11 March 2005, p. 7. All accessed IMO Knowledge Centre 13-14 October 2008.
A regulatory framework that sought to enhance the breadth and depth of information available to regulators on the current status of implementation was pursued. For example, in line with SOLAS Regulation XI-2/13, the IMO Secretariat continued to operate and develop a database of information, putting on a more permanent footing the collection and retention of the types of data that had been amassed from the range of surveys the organisation conducted in the run-up to 1 July 2004.\textsuperscript{181} On the same lines regulators also embraced a more interactive form of information collection encapsulated in the introduction of a multi-layered inspection programme to audit industry security operations. These external audits effectively capture the emphasis on further institutionalising the existing counter-terrorism security response as ‘paper compliance’ was superseded by an emphasis on ensuring concrete developments were in place in ports.

The idea of inspecting ISPS code compliance had been around as the code was first developed, but as the in-force date had drawn ever closer, focus had increasingly turned towards setting out the mechanics of such a programme. It had been decided that external inspections for UK ports was to be undertaken by a combination of European Union (EU), TRANSEC and Maritime and Coastguard Agency (MCA)

inspectors. The specific nature of the EU’s role had been the subject of debate. There had been a dividing line between the Council of Ministers who sought merely a limited screening role for EU Inspectors, checking documents without any need for physical presence in ports, and the European Parliament and Commission that sought a far more substantial and active role.\textsuperscript{182} For the industry itself, concerns here centred on the logistical strains that could accompany multiple inspections. As Patrick Verhoeven of the European Sea Ports Organisation commented:

\begin{quote}
we do not mind commission inspectors if they help to ensure a level playing field, but we are concerned about having a multitude of inspectors which could lead to a situation where you have an inspector from the commission one day, from the member state the next day and from the US the following day.\textsuperscript{183}
\end{quote}

These disagreements serve as a reminder of the tensions that can arise between different actors along the policy chain as each seeks to defend and advance their own interests. Eventually the system that was negotiated edged more towards that sought by the European Parliament and Commission. Member state inspection teams had primary responsibility for assessing compliance and standards within their territory, yet European inspectors were to undertake more than a ‘screening role’ empowered to visit member state ports and go aboard European registered vessels themselves. The specific purpose of European inspections was “to verify the effectiveness of national quality control systems and maritime security measures, procedures and


158
This dual emphasis on inspecting port security operations and ensuring the standard of national inspection programmes again illustrates the interconnected nature of the maritime industry and the belief held by regulators that greater cross-border harmonisation helped reduce the likelihood of gaps in security coverage.

The specific EU inspection procedures were laid down in ‘European Commission regulation 884/2005’ published on 10 June 2005. The Commission was to conduct inspections with both its own group of officials and by essentially seconding, temporarily, national inspectors to their teams. Technical advice and support was to be provided by the European Maritime Safety Agency (EMSA) in order to ensure that the inspections were “conducted in a transparent, effective, harmonised and consistent manner.” It was the responsibility of member states to ensure that Commission inspectors could work in various ports even if, as the three UK cases were, privately owned. The member state was required “by any means within their legal powers [to] assist the Commission to accomplish in full its task”. The Commission was required to provide member states with at least six weeks’ notice of the arrival of any inspection team, and in return there was a requirement to “take all

---


186 Ibid., Chapter I, Article 1.

187 Ibid., Chapter II, Article 4,3.
necessary steps to ensure that notification of an inspection is kept confidential in order to ensure that the inspection process is not comprised.”  

Frameworks were also laid down to govern the conduct of Commission inspectors while on site and the structure of their reports. In the latter, inspectors were required to mark ISPS compliance according to one of six classifications:

(a) in conformity;

(b) in conformity, but improvement desirable;

(c) non-conformity;

(d) major non-conformity;

(e) not applicable;

(f) not confirmed.

In the event of ‘non-conformity’ and/or ‘major non-conformity’ the Commission was empowered to initiate a series of sanctions ranging from demanding further explanation from the member state for deficiencies, to conducting a follow-up inspection, to initiating “an infringement procedure in respect of the Member state concerned”. Furthermore, cases of ‘major non-conformity’ could result in the Commission informing other Member states of a partners security failings, seeking

---

188 Ibid., Chapter III, Article 8, 1.
189 Ibid., Chapter III, Article 11 (5).
190 Ibid., Chapter III, Article 13 (1c).
compliance through naming and shaming. The emphasis then was very much on ensuring procedures were in place to govern any situation that could arise.

The prospects of implementing a security regime similar to that put in place through the ISPS code but beyond the ship/port interface, also continued to be investigated in this period. It was evident that amongst some political leaders, specifically at the international and regional level, and even as the ISPS code was being written, that a view was held that more could still be done to extend its reach. Demonstrating the policy time lag, the International Maritime Organization (IMO) and International Labour Organization (ILO) code of practice on port security highlighted in the previous chapter and developed in 2003, would be approved and published in 2004. A non-binding code it did not intend to replace the ISPS code but rather extend “the consideration of port security beyond the area of the port facility into the whole port.”

The EU took this approach onwards laying the groundwork through reports, debates and consultations for a new directive. UK ports were encouraged by the Department for Transport (DfT) to offer their views on the proposed directive and were left in little doubt they had to prepare for further developments in the future.

191 Idem.


194 The Department for Transport (DfT) conducted a consultation process with a range of actors including other government departments, port operators and union representatives. See Department for Transport, ‘Proposal for an EU Directive on Enhancing Port Security’, Consultation Letter, 24 February 2004, accessed 18 September 2010,
This was not to be the only move towards expansion in this period. On 1 July 2005 smaller ‘Class A’ vessels and those port facilities which served them fell under an ISPS regime under the terms of the 2004 EU directive that had first introduced the ISPS code in to EU law.\(^{195}\)

Although the ISPS code remained the centre-piece of the post 11 September 2001 counter-terrorism security response in relation to UK maritime infrastructure, and was conceived with maritime infrastructure firmly as it focal point specifically through its emphasis on the ship-port interface; other security developments continued to take place which impacted upon the management of that infrastructure in what can described as a more associative way. Here maritime infrastructure security both internationally and in the UK was more often than not shaped by measures that were not designed with that infrastructure as their central focus. Rather, it was impacted upon by general counter-terrorism and civil contingency legislation, and by measures designed to enhance the security of the wider supply chain, transport network and UK border, all of which maritime infrastructure was part.\(^{196}\) This demonstrates maritime infrastructure’s position as an example of critical


\(^{196}\) As it was noted in Chapter Two, in the UK general counter-terrorism legislation such as the ‘Terrorism Act, 2000’ had an impact on UK maritime infrastructure in so far as those SB ports officers working within a site could detain individuals under the Act. Ports and harbours were also just some of the key sites for which emergency plans had to be kept in place as part of the ‘Civil Contingencies Act, 2004’. See ‘Civil Contingencies
national infrastructure. The ISPS code then still dominated activities in this period, but in later years as the ISPS code was further institutionalised, the space was created in which the impact of other measures became more visible and prominent.

In terms of the wider supply chain there was, for example, an acknowledgement from senior European officials that a big bang approach to regulation was “rather unlikely and not the best possible solution”. Rather voluntary compliance, emphasising the benefits to trade and ensuring that one part of the supply chain avoided undertaking disproportionate security work were deemed to be the key components of a necessary response. The World Customs Organization (WCO) for example agreed new non-binding standards for security that included a rule requiring shippers to supply authorities in the destination country with details of cargoes 24 hours before they were loaded at a foreign port. This 24 hour manifest rule had already influenced some UK ports as the US demanded the manifests of container ships heading to it were also fully declared in advance of departure. To help facilitate this, the US had launched a Container Security Initiative (CSI) positioning customs officials within selected foreign ports including Felixstowe to enhance

---


intelligence. The 24-hour rule was closely associated with efforts to tackle concerns that weapons of mass destruction could be transported via sea and enter a state through one of its ports. Here the UK launched Project Cyclamen, an initiative to introduce additional CBRN scanning capabilities into some UK ports, and set up the Government Decontamination Service in October 2005 to co-ordinate a UK response to any attack.

(3.4.2) Institutional changes and infrastructure developments:

Institutional changes and infrastructure developments often, though not always, emerged out of the legislation and regulatory frameworks that had been introduced. As the previous chapter acknowledged it had been because of the ISPS code that in the run-up to 1 July 2004 certain UK ports had been required to erect new fencing, install better CCTV systems, introduce access controls to secure areas and recruit a

---


PFSO. In this period however the combination of having such ISPS requirements in place and because of the early stage of implementation of the regulatory agenda outlined in the last sub-section, there were somewhat fewer visible developments here. In terms of the external inspection regime for UK maritime infrastructure, the agency that helped co-ordinate EU inspections, the European Maritime Safety Agency (EMSA), had been established back in 2003. In the United Kingdom the MCA and TRANSEC were long-established. Within UK ports the preparation for inspections were to be co-ordinated by senior port managers, specifically Port Facility and Company Security Officer’s (CSO), who had been in place as the initial implementation of the ISPS code was being undertaken.

In institutional terms then attention fell on maintaining the security regime the ISPS code brought about. Here the process of holding regular, usually monthly port security committee meetings was well under way. These meetings were arguably one of the clearest signs of the emphasis on enhancing co-ordination between members of the policy network, providing the opportunity for security issues to be discussed and plans to be made. That said, in one port a trade union representative expressed frustration that his union were not always incorporated within these more formal gatherings. The assumption made for this absence was that port senior management were wary of having their dirty washing about operations more


203 Author’s interview with number 7, 18 March 2009.

204 Author’s interview with number 14, 9 December 2009.
generally aired in front of other stakeholders.\textsuperscript{205} Despite moves towards enhanced co-ordination it was certainly the case that more strategic decision-making in relation to security within UK ports, continued in this period to be wielded by a relatively small group of people. More specifically this included representatives from central government, mainly from TRANSEC, Special Branch (SB) ports officers, local Home Office force representatives, ports police and senior port management.

In terms of infrastructure developments, the port of Felixstowe in particular had very much begun to consider the possibilities offered by new technology in relation to the counter-terrorism security response. Specifically in this period they focused energy on developing a new IDentification and Access Control System (IDACS) to aid in the monitoring of both cargo and people.\textsuperscript{206} Such developments were described as not simply being about trying new ideas but rather rested on an acknowledgement that “security is here and it has to be operationally beneficial.”\textsuperscript{207} Besides demonstrating an acceptance that the counter-terrorism security response introduced post 11 September 2001 was to be a part of day-to-day port operations, this view also illustrated the desire to maintain the balance between security and commercial interests. In following years Felixstowe further expanded its use of technology to help meet and surpass the security requirements placed upon it.

Ultimately, the relative lack of institutional changes and infrastructure developments allowed the maritime industry to reflect further on the total costs of implementing

\textsuperscript{205} Idem.

\textsuperscript{206} Ascertained during an interview.

\textsuperscript{207} Ascertained during an interview.
and maintaining the existing response. The Port of Tilbury followed Felixstowe in introducing security charges, but also charged port tenants alongside shipping lines and agents. Justifying the inclusion of tenants, operator Forth Ports Managing Director Perry Glading stressed the collective benefits of enhanced security and the importance of financial burden sharing. “To minimise the effect on shipping lines and agents we have said to tenants, you will benefit from enhanced security of the port [...] That means that everyone within the port perimeter will have to pay a contribution to the enhanced costs.” In doing so many more port users were firmly tied in to the process of maintaining security as stakeholders.

(3.4.3) Working practices:

There was little doubt that the most visible developments in this period occurred in terms of working practices. This was primarily the case because the process of further institutionalising the existing counter-terrorism security response, particularly the ISPS code, had been pursued through the emphasis on universal compliance and harmonising and improving security standards. The international legislative and regulatory frameworks provided the overarching framework and a set of minimum security requirements here, and the majority of implementation remained the concern of the individual state and their ports respectively. In terms of compliance and inspections UK ports found their working practices shaped by the need to be at a constant state of readiness, not only from EU inspection teams, but from TRANSEC

---

inspections that were themselves external in the sense that they were conducted by agents from outside of the port.

For TRANSEC compliance was understood as “the consistent and effective application of security regimes by industries” that they regulated. It utilised several different approaches to assess compliance and was amongst other things “focused on outcomes”, “an appreciation of the industry perspective” and “a desire to have a strong working relationship with industry”. These approaches included standard audits (full security assessments taking several days), programmed inspections (looking at one aspect of security over a day/half-day), thematic audits (an assessment of a particular function/aspect of security), thematic inspections (like thematic audits but across more than one location), mini-audits (across more than one location, but covering less than a standard audit), and desktop assessments (where information is submitted and site visits are not necessarily required) were all undertaken. The specific use of each approach was shaped by a continual assessment of the threats posed to each mode of transport. Moreover the inspections were both announced and unannounced, while information ascertaining to possible breaches of security were investigated as they arose.

As with European Commission inspections, publicly available information about the specific checks made by UK inspection teams is limited. Yet TRANSEC


210 Idem.

211 Idem.
acknowledged an interest, amongst other things, in ensuring “that ‘Restricted Areas’ within port facilities are clearly marked and that the signage meets the relevant criteria”.\(^{212}\) They also sought to “work closely with operators to ensure that the measures set out in approved Port Facility/Ship Security Plans are operating effectively.”\(^{213}\) As noted in the previous chapter, Part B of the ISPS code advised that Port Facility Security Officers review their Port Facility Security Plan at least once every six months, one measure the EU made mandatory.\(^{214}\) Finally TRANSEC expressed an intention to undertake covert inspections stimulating “security incidents and other unlawful acts to test the effectiveness of security measures.”\(^{215}\) These were justified on the grounds that:

> inspection activity can establish whether security measures are being implemented, but may not necessarily confirm either the quality of implementation or the adequacy of the measure itself [...] Effectiveness of implementation and adequacy of the measure can be objectively established only by realistic covert tests of transport security.\(^{216}\)

TRANSEC emphasised a stepped-approach to ensure that deficiencies found within ports were tackled, with Deficiency and Enforcement notices representing the most prominent steps available to them. This approach is outlined in the table on the following page. Published on the Department for Transport’s official website, the


\(^{213}\) Idem.


table was written for those with an interest in the department’s policies for ensuring industry compliance with regulations.

Table 1 – The TRANSEC approach to compliance:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Advise</td>
</tr>
<tr>
<td></td>
<td>(TRANSEC provides guidance to an organisation on how to solve the problem)</td>
</tr>
<tr>
<td>2</td>
<td>Persuade</td>
</tr>
<tr>
<td></td>
<td>(Here inspectors take a stronger line, making an organisation aware of its failings, stopping short of formal enforcement action.)</td>
</tr>
<tr>
<td>3</td>
<td>Deficiency Notice (D-Notice)</td>
</tr>
<tr>
<td></td>
<td>(Formal action commences if the first two steps have failed or the breach is regarded as serious enough to require a more formal response. Taking the form of a letter, the D-Notice elaborates deficiencies and reminds the organisation of its responsibilities.)</td>
</tr>
<tr>
<td>4</td>
<td>Formal Interview</td>
</tr>
<tr>
<td></td>
<td>(Following two or more D-Notices for a specific deficiency or a range of deficiencies, senior TRANSEC management can request that an organisation’s senior management come to the Department for discussions. Here the organisations responsibilities will be elaborated and the consequences of continued deficiency outlined.)</td>
</tr>
<tr>
<td>5</td>
<td>Enforcement Notice (E-Notice)</td>
</tr>
<tr>
<td></td>
<td>(Empowered by legislation TRANSEC can then issue an E-notice to an organisation for failing to comply with a “general” requirement/instruction. Such a notice will usually be drafted in co-ordination with Legal advisors.)</td>
</tr>
<tr>
<td>6</td>
<td>Prosecution</td>
</tr>
<tr>
<td></td>
<td>(Failure to comply with an E-notice may result in legal proceedings commencing against the organisation for non-compliance. In exceptional circumstances prosecution may take place without an E-notice being issued.)</td>
</tr>
</tbody>
</table>

Broadly speaking the inspection of ISPS code compliance in the UK during this period took place without publicity. One exception came during summer 2005 when it became public knowledge that the Home Office, in co-operation with TRANSEC

---

had embarked upon a security review of six ports.\textsuperscript{218} This review went beyond assessing ISPS Code compliance alone and was part of a wider Multi-agency Threat and Risk Assessment (MATRA) initiative around airports.\textsuperscript{219} MATRA had been introduced as a result of the 2002 Wheeler Review of Airport security and represented another example of UK authorities encouraging and developing joint working between different members of the policy network right along the policy chain.\textsuperscript{220}

The requirement to maintain a constant state of readiness in case of external inspection did in part justify the regular internal security audits UK ports themselves conducted.\textsuperscript{221} The specific characteristics of these internal checks varied from port to port but there were commonalities. Felixstowe, Holyhead and Tilbury for example all employed a growing number of private security personnel to undertake regular patrols to check perimeter fencing, conduct vehicle searches and organise regular security meetings.\textsuperscript{222} There was a clear sense of self-awareness from some of those responsible for port security of the limits of relying on one mechanism to enhance port security. One port manager acknowledged the relative weaknesses of fencing


\textsuperscript{219} Idem.


\textsuperscript{221} The importance of building security awareness was highlighted in author’s interview with number 11, 3 March 2010. The need for regular drills in author’s interview with number 7, 18 March 2009.

\textsuperscript{222} Information gathered during site visits and from author’s interviews with number 7, 18 March 2009 and number 10, 24 March 2010.
commenting, “at the end of the day a fence is just a deterrent. They are measured in seconds – how long it takes to get through them”.

Beyond routine security checks, attention was also placed on ensuring better compliance by building and maintaining security awareness. There was an acknowledgement from those in port management of the need to elaborate in greater detail to both staff and users, who had busy working lives and multiple demands on their time, both greater specifics in relation to the presented threat faced and the counter-terrorism requirements imposed upon them. This was deemed particularly necessary because the scale and urgency with which changes had been introduced as the ISPS code formally came in to force - most notably the increase of vehicle searches by private security personnel - had been such, that for many, particularly lorry drivers, there had been notable wariness and unease about just what the developments meant for their working lives. The core objectives then were to encourage constant vigilance and no complacency regarding the presented threat, help explain daily procedures, and to facilitate the more effective recognition and treatment of perceived gaps in the existing counter-terrorism security response.

To some extent the expectation held by port managers was that this security awareness would simply grow as a result of individuals being exposed to security requirements such as showing identification at certain designated points. Yet a

---

223 Author’s interview with number 7, 18 March 2009.
224 Idem.
225 Idem.
more proactive role was also taken here to ensure the existing response was further institutionalised and increasingly became second nature. References to security were visible throughout the sites, below is one example of a sign at the Port of Holyhead.

*Image 1 – Security level sign.*

The sign itself is one requirement of the ISPS code. ‘Security Level 1’ is a reference to one of the three levels of security - in essence states of readiness – also introduced by the code. This level determines the nature of security activities undertaken, such as the minimum percentage of port users who should be searched. TRANSEC sets the relevant security level for UK maritime infrastructure after discussions with relevant parties. The sign is particularly interesting because although level 1 represents the lowest required state of readiness, the sign nevertheless serves a

---

226 Image 1 – ‘Security Level Sign’, taken by author on site visit.
constant reminder to staff that ‘security’ is something they have to be aware of, that they should always be alert for possible changes. Its prominent position outside the office of the Harbour Master, who serves as PFSO - the management centre for the port – is also a mechanism through which the port owners and management can illustrate the way in which they take security seriously. Finally the addition of a padlock preventing unauthorised changes to the security level, serves to emphasise further that the security level is deemed to be of such importance that it should not be tampered with or changed lightly and that there are consequences to any change.

Port managers were also aware of the particular demands in relation to implementation created by their specific environment. Beyond signage a range of security awareness posters were placed in prominent positions to inform staff and users of particularly relevant legislation/regulations and the need for constant vigilance. Such practices again illustrate how implementation did not simply take place in one-off events but rather was continual and had multiple stages. The Port of Felixstowe designed posters encapsulating a new port motto – ‘Serious about Security’ - which included a direct line telephone number for concerns to be reported. Like the security sign, the use of a motto, that also was included in some of the port’s correspondence, both reminded staff and users to be aware of security and served a public relations role showing outside parties that as a port Felixstowe took its wider security responsibilities seriously.
This poster was one of those developed and displayed in the port. By utilising images to advance awareness, it serves as a reminder of how the presented threat drawn upon in the two main narratives could also be reproduced visually. The language included on the poster served as an important mechanism to give the image wider meaning, the image itself provided an insight into the way in which managers sought to emphasise that security was everyone’s responsibility by using the drawing of an ordinary port worker as Felixstowe’s representative. For added clarity the tagline reminded staff of their responsibilities, the inclusion of the dubious looking

---

227 Image 2 – ‘Port Security Poster’, taken by author on site visit. Contact phone number removed by author for the purposes of anonymity.
individual skulking away from the scene reiterated the sense of an ‘Us Vs Them’
dichotomy associated with the macrosecuritisation and captured in the ‘war on
terror’ discourse, the departure from a ‘private area’ emphasised a distinction
between open and closed space, while the use of the one word ‘Suspicious’ with the
affixed question mark provided an additional reminder that an inquisitive mind was
what was sought.

Alongside such posters, internal publications such as newsletters were also utilised
to advance awareness. They provided regular information explaining the justification
for infrastructure developments within a port such as new fencing, and offered an
additional platform for managers to emphasis the kind of message encapsulated in
the posters.\textsuperscript{228} In one port, a newsletter concluded with the following passage:

\begin{quote}
Security is here to stay. The need for enhanced maritime security is accepted
worldwide and the efforts of all concerned in implementing the ISPS Code
contributes significantly to improving the security of personnel and
infrastructure. Although Port Police and Port Security Officers are tasked with
implementing the new security measures it is \textbf{essential that everyone is aware
of their responsibilities} with respect to security. The best security guard is the
person who notices something unusual or unexpected. The best person to do
that in your work place is...YOU.\textsuperscript{229}
\end{quote}

With a certain sense of fait accompli being displayed in this extract about the need
for enhanced maritime security, it also serves as a further reminder of how such
ideas were reproduced widely and by different members of the policy network.

Alongside those efforts at building and maintaining awareness about security in UK
maritime infrastructure, the demand for the harmonisation and improvement of

\textsuperscript{228} ‘Security Update’, Internal Newsletter, December 2004.

\textsuperscript{229} Idem. Emphasis in original.
security standards also resulted in a specific focus on improving port training programmes. This occurred out of the process of policy reflection as perceived gaps and weaknesses in the existing counter-terrorism security response were highlighted to be addressed. Internationally, in addition to the IMO’s Global Technical Co-operation Programme on Maritime Security, the organisation launched a Train the Trainer programme. Its primary objective was to utilise IMO model courses for Ship, Company and Port Facility Security Officers to improve standards amongst instructors. As an organisation the IMO invested a substantial amount of money – approximately $2.645 million - in its capacity-building programme between 2002 and 2005. An International Maritime Security Global Trust Fund was also set up to institutionalise such support. By April 2005 the fund stood at $557,391.99, of which the UK had provided $327,879.00, the most significant contributor.

Ultimately however IMO training programmes had little direct bearing on operations within UK ports beyond illustrating the seriousness with which training and standards were being taken. The assumption was that security standards within


231 As was noted in Ibid., pp. 3-4, paragraph 15, “this form of “cascade training” should result in a significant increase in the number of people trained to a standard consistent with IMO expectations and will be a cost effective use of funds”. Early versions of these courses included, International Maritime Organization, Company Security Officer (Model Course 3.20) (London: International Maritime Organization, 2003) and International Maritime Organization, Ship Security Officer (Model Course 3.19) (London: International Maritime Organization, 2003).

232 Ibid., p. 4, paragraph 18.

regions such as Europe were broadly high, while the financial costs of ISPS implementation in the UK had, as it has been noted, largely been placed on the industry itself. Of greater relevance were international and regional efforts to develop additional guidelines to enhance security standards. These efforts illustrated those discussions over how prescriptive the response should be. To demonstrate with an example, in October 2004 the US submitted to the IMO, as a basis for new international guidelines, a document outlining what it saw as the necessary Knowledge, Understanding and Proficiencies (KUP’s) relevant to the Company Security Officer (CSO) and Port Facility Officer (PFSO) roles.\(^{234}\) The International Shipping Federation (ISF) however questioned whether the IMO had the necessary experience to develop such guidance arguing that it should “allow companies the flexibility to set up their own ISPS arrangements and training ashore.”\(^ {235}\) The IMO’s response was to follow the approach embraced with the ISPS code and combine central guidance through publication of its own guidelines, whilst maintaining that member states had the right to develop their own specifics within particular parameters.

This mixture of ‘centralised framing and localised delivery’ was also mirrored within the UK where TRANSEC offered guidance and established a broad framework of requirements, yet allowed individual ports relative flexibility with regards to day-to-day issues.

---


day implementation. For example TRANSEC had out-sourced the delivery of IMO model training courses for roles such as the PFSO to private companies it accredited. In this twelve month period TRANSEC continued organising maritime security awareness events. These followed on from a series of ISPS code roadshows they had delivered to UK ports pre-July 2004 in order to elaborate the content and implications of the code. With regards to training in UK ports some form of security training had of course been a long established tradition especially where the Aviation and Maritime Security Act, 1990 (AMSA) had had an impact. As the in-force date for the ISPS code had drawn closer, this provision had expanded considerably. In Felixstowe for example senior port managers spent a number of weeks in the classroom informing staff about the impending changes.

In one UK port all managers were required to undertake a one and a half hour session on security as part of their induction, while the general staff induction

---

236 ‘A brief overview of the United Kingdom National Maritime Security Programme’, Department for Transport. Demands placed on ports by TRANSEC regarding the standard of fencing required were noted in ‘Security Update’, Internal Newsletter, December 2004 and was raised as one example in an interview conducted by the author.


239 Both the Port of Felixstowe and the Port of Tilbury had their own private port police force that pre-dated both the ISPS code and ‘Aviation and Maritime Security Act’.

240 Ascertained during interview. The objective had been to provide greater information to staff about the perceived threats posed to maritime infrastructure and the required response to them.
stressed the importance of asking others to go through a three-tiered identification process - to prove who they were, show who they were and explain a reason to be there. Various images of the 11 September 2001, 7 July 2005 terrorist attacks and the incidents involving the USS Cole and Achille Lauro were deployed in presentations in order to illustrate the presented terrorist threat to maritime infrastructure and to justify the introduction of the ISPS Code.\textsuperscript{241} Such an emphasis illustrates how terrorism remained a top security concern. At another port, the port operator even developed a compulsory e-learning package to assist the education process in relation to the ISPS code. It systematically required all staff, including private security to undertake and pass a series of tasks which assessed their level of knowledge of the code before their training was regarded as complete.\textsuperscript{242}

With regards to these private security staff, they also undertook broader counter-terrorism training in addition to their ordinary training programmes. In one port, training for private security personnel was very much a multi-stage process. Once staff had gained the necessary police vetting they went on a residential course to complete a security training course. With this successfully complete they undertook a four day basic ‘Security Man Guarding’ programme which concentrated, amongst other things, on effectively manning port access points, including restricted areas, and conducting vehicle and personnel searches. Staff also learnt about conflict management to assist in working with others on a daily basis before undertaking two days of ISPS classroom training with a test at the end. After all this the member of

\textsuperscript{241} Idem.

\textsuperscript{242} Author’s interview with number 12, 24 March 2010.
staff then undertook on-site training and monitoring. The whole process lasted between 12 and 15 weeks.\textsuperscript{243}

The selection of photos below illustrates a range of activities private security personnel carried out within one port:

\textit{Image 3 – Port personnel search:}\textsuperscript{244}

\textsuperscript{243} All this information was outlined in author’s interview with number 10, 24 March 2010.

\textsuperscript{244} Image 3 – ‘Port Personnel Search’, reproduced with permission of an interviewee. The image was cropped by the author to remove one individual whose face could be seen. This was done in the interests of anonymity.
Image 4 – Port Vehicle Search.\textsuperscript{245}

Image 5 – Port Entry/Exit Point.\textsuperscript{246}

\textsuperscript{245} Image 4 – ‘Port Vehicle Search’, reproduced with permission of an interviewee. This image was also cropped by the author to remove one individual facing the camera. This was done in the interests of anonymity.

\textsuperscript{246} Image 5 – ‘Port Entry/Exit Point’, reproduced with permission of an interviewee. Port Operator name, vehicle registration plate and part of one sign covered over by author in the interests of anonymity.
The emphasis on further institutionalising the ISPS code meant learning about security was increasingly regarded as something that had to be a continual process and not just reserved for inductions. As one port manager explained, his objective was to ensure that individuals knew that “security is not just for Christmas; it is here to stay”.247 This trend particularly materialised itself in the use of regular security drills. Part B of the ISPS code had suggested that some form of drills should take place every three months to “ensure the effective implementation of the provisions of the port facility security plan”.248 In one UK port this served as just the start as the private port police force conducted a minimum of eight drills per year. As a senior officer explained “I am a great believer you should train hard and fight easy”.249 This explanation illustrated how more militaristic language – where the friend/enemy distinction is a central feature – filtered through in to the mentality with which some port working practices were approached. In each of the three UK cases examined there was at least one individual interviewed with a military background working in the port.250 On a wider level this serves as a reminder that an individual’s background can shape not only their own actions and reactions, but the actions and reactions of a wider community, particularly if they are in positions of power.

The focus on security drills was a further illustration of the emphasis placed on enhanced co-ordination between agents of implementation at every level of governance with regards to the counter-terrorism security response. As one senior port manager noted “[We] don’t have to co-operate; but it’s good that we do. At the

247 Author’s interview with number 11, 3 March 2010.
248 IMO, ISPS Code, p. 98, paragraph 18.4.
249 Author’s interview with number 7, 18 March 2009.
250 Numbers 7, 10 and 14.
end of the day we all have the same goals.” Yet as it was noted previously, security decision-making of a more strategic nature still remained the preserve of a relatively small group. Particular concerns and tensions revolved around the role of the private sector, which played an increasingly prominent role in security from manning port access points to delivering security training as TRANSEC accredited providers. Despite the perceived importance of the work then, enhanced co-ordination still took time to mature as both trust and job skills developed. The issue of the quality of the private security personnel utilised was raised, with one interviewee acknowledging that in his port the private security guards were occasionally omitted from port security drills. One private security guard had lost their job because of lapses in conducting checks leaving the officer to acknowledge it inevitably took time for private security contractors to be fully accepted.

Similarly a trade union representative at another port expressed his concerns that the difference in capability between private security staff was substantial. Emphasising the perceived value of a military background he commented:

some are very good, I think there are a lot of ex-Ghurkhas, and no one will doubt their capabilities. But you have others who won’t get out of their private car; they don’t stand in their security box. You are thinking you might as well put a crash test dummy in that car because they ain’t doing any good.

One interviewee also raised the issue of pay, commenting that as private contractors were invariably paid substantially less than their colleagues in the Police it was, in his view, ultimately be “down to the motivation of that individual as to how well

251 Author’s interview within number 7, 18 March 2009.

252 Information ascertained from an interview conducted by the author.

253 Idem.

254 Author’s interview with number 14, 9 December 2009.
Similarly concerns were also expressed about the role of agency workers and the extent to which they bypassed the necessary training requirements.\textsuperscript{256}

\textbf{(3.5) Conclusion:}

Those developments witnessed in the 12 months between 1 July 2004 and 6 July 2005 help to shed further light on the securitisation of UK maritime infrastructure in the context of responses to international terrorism. The wider context in which maritime infrastructure was securitised did remain largely unchanged as the macrosecuritisation of the ‘civilised way of life’ remained stable and the ‘war on terror’ discourse within which it was captured continued to frame large swathes of policy. What did become evident however was the way in which different members of the policy network, beyond those political leaders with some responsibility for policy relating to UK maritime infrastructure, also reproduced the two main narratives relating to that infrastructure. The reiteration of the presented threat posed by international terrorism by say, security professionals, often through the maritime media, served to illustrate the broad extent to which concern about the dangers inherent in lax coastal vigilance had pervaded popular discourse.

Additional insights about resistance to the securitisation also emerged in this chapter. Developments in this period illustrate the way in which, during the implementation of emergency measures, a continual process of reflection takes place where members

\textsuperscript{255} Author’s interview with number 2, 28 July 2009.

\textsuperscript{256} Author’s interview with number 14, 9 December 2009.
of the relevant policy network specifically discuss the counter-terrorism security response. This reflection can centre on the content of emergency measures, how they are delivered and/or their broader impact and can be captured in two broad questions, ‘Is the existing counter-terrorism security response working?’ and ‘What, if anything, should come next?’ These questions facilitate a series of ongoing discussions, which then shape future discourse and practice, demonstrating further the element of process to securitisation. Here those discussions centred on the need to maintain three balances – between security and commercial activities, between security and liberty, captured in the call for fair treatment of seafarers, and over who had what responsibilities in relation to the implementation of the response, particularly between ship and shore personnel. Beyond this a discussion over how prescriptive the counter-terrorism security response should be was captured in those debates within the IMO over whether US plans for KUP’s for PFSO’s and SSO’s were an appropriate way forward.

Although it was argued in chapter one this reflection is a perfectly natural part of the policy-making process, a few points are worthy of further elaboration. The first is that developments in this period illustrate how reflection and resistance run parallel to each other. Defined as ‘an overt challenge’ in this thesis, resistance emerges out of the process of reflection. To return to the previous example to elaborate, the resistance to the idea of KUP’s from the International Shipping Federation emerged out of wider discussions over how best to improve the activities of PFSO’s and SSO’s. Second, particular events can prompt additional reflection/resistance. This chapter has shown how both the terrorist attacks in Madrid in March 2004 and the General Election in the UK in 2005 were able to place renewed focus on the
presentation of the threats deemed to be posed to open transport networks and because of open borders respectively. Both these examples emerge out of maritime infrastructure’s position as an example of critical national infrastructure.

Finally, as it was noted in passing in the previous chapter but becomes even more apparent here, there are different forms of resistance which are directed at different targets. A recurring example of resistance in this period was that directed towards the way in which some states were deemed to be restricting the freedom of seafarers through over-zealous implementation of measures such as the ISPS code. This resistance then was directed at a particular element of the counter-terrorism security response and the impact of it. It was not though explicitly directed at the rationale for the response, namely the idea that in the context of a ‘war on terror’, maritime infrastructure needed to be ‘secured’ against a threat posed by international terrorism. There were occasional glimpses of such resistance in relation to maritime infrastructure, as the accusation of an over-reaction from a couple of seafarers demonstrated, but these were relatively rare. With emergency measures still being implemented this more direct resistance also seemed to lack noticeable impact.

Turning to the impact of securitisation on the management of UK maritime infrastructure, which was clearly substantial, those prominent features of the counter-terrorism security response in relation to UK maritime infrastructure that had been evident in the period between 11 September 2001 and 1 July 2004, were again witnessed. Members of the policy network continued to turn to legal instruments, specifically in the form of regulations to enhance the security of maritime
infrastructure. The EU regulation which put in place the community-wide inspection regime for ISPS code compliance was the most notable example. This regulation indirectly empowered the British state through TRANSEC to facilitate European Commission inspections of UK maritime infrastructure. With the EU gaining some degree of oversight over ISPS compliance as well, coupled with ports introducing their own internal training and audit processes, a wider group of actors could be said to have increased their power too in this period.

Beyond the continued propensity for members of the policy network to turn to legislation/regulations to secure UK maritime infrastructure, an element of complexity was also apparent to the relationship between members of the policy network. The emphasis continued to be on enhancing co-ordination in an effort to enhance security and a ‘centralised framing and localised delivery’ model was evident where there was an acknowledgment of the need to let those on the ground within UK maritime infrastructure, utilise their experience and knowledge of their environment to improve implementation. This mirrored the UK’s ‘lead department’ model to counter-terrorism, but on a smaller basis, and was seen in the way in which TRANSEC was willing to outsource PFSO training and let ports develop their own internal compliance systems. Yet despite the acknowledgement of shared goals between members of the policy network, it was clear that trust was deemed to play a big part in effective implementation.

Concerns over the effectiveness of private security personnel, expressed by a SB ports officer and trade union representative respectively, provide one example of this
situation. More specifically still, the development of trust rested in part on impressions of competency. The praise allocated to former Ghurkha soldiers and the emphasis on ‘training hard and fighting easy’, suggested that a particular form of experience - that gained in the military – was deemed to be of particular high value in gaining competency in relation to security. This was then a further example of the way in which militaristic characteristics could be seen in the counter-terrorism security response. Alongside this the regularity and quality of training, and even the extent to which an individual had appropriate incentive, captured in the level of pay, were also deemed to contribute to competency.

The issue of trust between members of the policy network also underpinned those concerns expressed by a trade union representative over his exclusion from the regular port security committee meetings. This exclusion, however explained by those involved, was evidence that strategic-decision making was still the preserve of a relatively small number of the total individuals with security responsibilities in relation to UK maritime infrastructure. Even between those TRANSEC officials, SB ports officers, local police, ports police, senior port managers and other representatives who attended such meetings, detailed intelligence was not widely shared and discussed because of issues of confidentiality. There was then an inner circle within the inner circle where those state security professionals had access to additional information.

This demonstrates the secrecy associated with securitisation, secrecy which restricted the parameters of debates even in regular port security meetings. This restriction of
debate was also captured in the sense of powerlessness expressed by one senior port manager who highlighted the fait accompli within the UK over who financed many counter-terrorism practices within UK maritime infrastructure. With regards to spending, the growing use of technology to enhance security both illustrates the continued propensity for security budgets to grow, whilst highlighting an additional feature of the counter-terrorism security response. The use of systems such as IDACS to help monitor the movement of people and goods within Felixstowe, illustrated a willingness on the part of port owners to look beyond the use of private security professionals in isolation to secure their sites.

The cumulative effect of this examination of practice, and the continued elaboration of a number of the most prominent features of the counter-terrorism security response, is that a clearer picture begins to emerge as to what that response’s main characteristics are. More specifically the response can be said to (i) constantly evolve, (ii) be layered and (iii) increasingly expansive in scope. The evolution of the response is captured most clearly in the way in which there was an emphasis on institutionalising the ISPS code, embedding it further in day-to-day operations so it became like second nature. The willingness to add to the response where necessary, say, through the agreement of new non-binding rules on wider supply chain security, the increased scanning of containers for CBRN materials, and the use of technology more widely, demonstrates the numerous layers to the response. If one measure failed another would be in place. The expansive scope of the response is illustrated in the way in which a growing range of day-to-day activities within UK maritime infrastructure, such as the induction and training of new staff, were framed by counter-terrorism considerations. In short the response seemed to mirror the
presented threat it was designed to tackle which was deemed to constantly evolve, be layered and expansive in scope.

To elaborate further these main characteristics of the counter-terrorism security response, attention is turned in the next chapter to examining developments in the two years between 7 July 2005 and 26 June 2007. Heavily influenced by the terrorist attacks in London, after a period of intense introspection the ‘war on terror’ discourse would be energised as concern about the threat posed by international terrorism was renewed. In terms of practice the combination of policy reviews after the London attacks and the relatively well institutionalised position of the ISPS code led to a shift whereby a large proportion of those counter-terrorism practices with an impact upon the management of UK maritime infrastructure, emerged out of broader efforts to secure the wider supply chain, transport network and UK border respectively, all of which UK maritime infrastructure was part. The impact of securitisation then continued to grow.
Chapter Four

Beyond the ISPS code: securing UK maritime infrastructure after the London 2005 terrorist attacks

When they try to intimidate us, we will not be intimidated, when they seek to change our country, our way of life by these methods, we will not be changed. When they try to divide our people or weaken our resolve, we will not be divided and our resolve will hold firm. We will show by our spirit and dignity and by a quiet and true strength that there is in the British people, that our values will long outlast theirs.¹

(Tony Blair, Prime Minister, United Kingdom, 7 July 2005.)

(4.1) Introduction:

The previous chapter examined developments in the immediate twelve months after the International Ship and Port Facility Security (ISPS) code formally came in to force. It argued that the ‘war on terror’ discourse of counter-terrorism which captured the macrosecuritisation of the ‘civilised way of life’ remained stable, counter-terrorism considerations remained prominent, and that within this context the United Kingdom’s (UK) maritime infrastructure remained a ‘site of securitisation’. Here both the main narratives which drew upon the macrosecuritisation in relation to UK maritime infrastructure were widely

reproduced, and as such the emphasis continued to be placed on maintaining constant vigilance and no complacency with regards to the presented terrorist threat. This further energised the continual reflection with regards to the counter-terrorism security response, a process which was framed by questions such as - ‘Is the existing counter-terrorism security response working?’ and ‘What, if anything, should come next?’, and which included a series of ongoing discussions that broadly focused on how prescriptive the response should be and coalesced around the need to maintain a series of balances in terms of practice.

The overall result, it was argued, was that focus largely fell on ensuring the existing counter-terrorism security response, particularly the ISPS code, was further institutionalised in day-to-day activities specifically through the pursuit of universal compliance and the harmonisation and improvement of security standards. By elaborating this scenario through a detailed examination of practices and by making reference to three UK cases, the prominent features of the response first highlighted in chapter two were illustrated in more depth. To name just three examples, legislation and regulations continued to be turned to in order to strengthen the response, the focus remained on seeking enhanced co-ordination between members of the policy network, and there was a growth in investment in security-related activities as money was spent on training staff and utilising new technology. One feature that became increasingly apparent in the year after the ISPS code came in to force was the way in which the policy network increasingly utilised technology in order to enhance security. The chapter then concluded by suggesting that a picture had emerged of the main characteristics of the counter-terrorism security response.
Like the presented threat it was designed to tackle, it constantly evolved, was layered, and increasingly expansive in scope.

This fourth chapter turns to examine developments in the period between 7 July 2005 and 26 June 2007. It was a period framed by the terrorist attacks in London where four suicide bombers detonated on three underground trains and one bus killing 52 and injuring 750.\(^2\) The chapter argues that these attacks marked the beginning of a particularly public and more sustained period of reflection over, yet ultimately a renewal of, the ‘war on terror’ in the UK. In the aftermath of the terrorist attacks in London, political leaders and parliamentarians in particular, questioned the pursuit of the ‘war on terror’ and those practices associated with it in an arguably more sustained and public way than at any time since the months immediately following 11 September 2001. Yet while this reflection lead to resistance, directed again most prominently against particular counter-terrorism practices, but also increasingly at the terminology of ‘war’, there were limited signs that the grip which the macrosecuritisation of the ‘civilised way of life’ held over policy had significantly reduced. In the case of the latter form of resistance, discussion over the extent to which the terminology utilised was appropriate was not matched by any fundamental movement away from the reproduction and acceptance of the idea that the ‘civilised way of life’ required securing against an existential threat from

international terrorism. This macrosecuritisation was most evident in the way in which counter-terrorism considerations remained centre-stage.

Recognising the mutually reinforcing relationship between the macrosecuritisation and the securitisation of UK maritime infrastructure, this wider context ensured that infrastructure remained a ‘site of securitisation’. The emphasis on maintaining constant vigilance and no complacency with regards to the presented threat from international terrorism more widely ensured a similar emphasis was maintained in relation to UK maritime infrastructure specifically. The ‘target’ and ‘vulnerable node’ narratives were still reproduced widely, although it was noticeable how different dimensions to the presented threat were highlighted as being particularly salient. Here the threat relating to smaller vessels, smaller ports and harbours was noticeably raised. This focus emerged out of policy reflection, a process which also led members of the policy network to acknowledge some of the nuances surrounding the presented threat relating to maritime infrastructure, and to resistance against particular elements of the counter-terrorism security response. In the case of the former there was an emphasis on making the distinction between the level of threat faced by different modes of transport. In the case of the latter, proposals by the United States (US) to demand the scanning of 100% of inbound containers, which would have international ramifications, were most notably the subject of resistance. Overall however the central idea that UK maritime infrastructure required ‘securing’ remained firmly held by the policy network.

The result was that in terms of practice members of the policy network continued to focus on the need to institutionalise further the existing counter-terrorism security
response, including the ISPS code, with the sharing of best practice increasingly evident. However as the code and its associated practices had become further embedded in day-to-day operations, and because of the impact of the London 2005 terrorist attacks, the prominence of the ISPS code waned relative to other developments. Here institutional changes and infrastructure developments were particularly notable in this period, while measures were implemented that had what the previous chapter described as a more associative impact on UK maritime infrastructure, in so far as they were not necessarily designed with the infrastructure itself as their focal point, certainly to the extent to which the ISPS code had been. In particular the management of UK maritime infrastructure was shaped then by measures designed to enhance the security of the wider supply chain, transport network and UK border, all of which maritime infrastructure was part.

In examining these developments the chapter continues the process of reorienting emphasis towards the post-securitised environment, charting what securitisations ‘do’ in practice. The prominent features of the counter-terrorism security response in relation to UK maritime infrastructure also continue to be illustrated in greater detail with the focus on enhancing co-ordination between members of the policy network, and the use of technology to secure that infrastructure the subject of specific attention. In the case of the former, co-ordination was formalised through a new Police National Maritime Security Strategy (PNMSS), a strategy that encapsulated the ‘centralised framing and localised delivery’ approach. In the latter case, the UK government itself embraced technology through its e-Borders programme. In doing this, the three main characteristics of the response first highlighted in the previous chapter are more firmly established. In particular, a spatial dimension to the
increasingly expansive scope of the response was evident as security focus fell on the whole port area and beyond territorial borders themselves.

(4.2) Reflection and renewal – the ‘war on terror’ after the London 2005 terrorist attacks:

The ability of particular events to influence securitisation by say, creating the space in which further reiteration of presented threats can take place, was briefly highlighted in the previous chapter in relation to both the terrorist attacks in Madrid in 2004 and the UK General Election in 2005. Arguably, the terrorist attacks in London in July 2005 had a more pronounced impact. On one level this impact was somewhat inevitable, as the attacks represented one of the deadliest terrorist attacks in the UK. The timings of the attacks and their form also contributed here. In terms of timing, the attacks occurred just 24 hours after both London and the UK had celebrated winning the 2012 Olympic Games. A poignant contrast of emotions between joy and distress was therefore illuminated. Moreover while it had been widely accepted that international terrorism posed an existential threat to the ‘civilised way of life’, these specific attacks themselves had largely been unexpected. In January 2007 it was reported that the then head of the Security Service (MI5) Dame Eliza Manningham-Buller had told senior Labour Party MPs on 6 July 2005 that there was no imminent terrorist threat to London.3 In terms of the form of attack, the use of suicide bombers represented a stark departure from those

---

witnessed in the case of Northern Irish related terrorism. That the attackers were not foreign nationals, but British citizens, served only to heighten shock.

Internationally, the condemnation of the terrorist attacks began as early as 7 July itself as G8 leaders were meeting in Scotland. Western political leaders internationally remained the securitising actors reiterating that international terrorism posed an existential threat to the ‘civilised way of life’. For example, in an interview for the BBC, US Secretary of State Condoleeza Rice emphasised “this is a worldwide war against ideals. There is no separate peace to be made with terrorism. *They are after our way of life and we have to deal with them. There is no other way other than with strength.*” European Commission President Jose Manuel Barroso declared “this criminal act [is] not only against Britain, against the British people, but against all civilised people in the world that do not tolerate these kind of crimes.” Tony Blair emphasised how the British “way of life” was being challenged but that those values would outlast the terrorists. Mayor of London Ken Livingstone struck a defiant tone telling the supporters of terrorism, “nothing you do; however many of us you kill will stop that life. *Where freedom is strong and people can live in harmony, whatever you do, however many you kill, you will fail.*”

---


6 ‘In Quotes: World Reaction’, *BBC News Online*. Italics added by author for emphasis.


This discursive stability, as has been noted previously, represents evidence of an implicit form of audience acceptance of the macrosecuritisation, suggesting that securitising actors perceived that the ideas captured in the discourse remained both salient and coherent enough to warrant reiteration. Immediately after the terrorist attacks Tony Blair initiated a process of dialogue with opposition parties to try and find common ground on the appropriate response. This initially resulted in the announcement of a 12 point action plan against terrorism on 5 August 2005.\(^9\) There was also a specific resolve to enhance European counter-terrorism efforts, a process the UK drove forward as President of the Council of Europe in the second half of 2005.\(^10\)

This was not to say political leaders didn’t feel the need to further clarify the dimensions of that presented threat, for that they did. The home-grown dimension to the 2005 London attacks in London ensured they re-emphasised the need to differentiate between a moderate, law-abiding majority of Muslims and an extremist minority who sought refuge in committing terrorist acts. This ensured the defining characteristics of the ‘them’ in the ‘Us versus Them’ dichotomy was made clear.\(^11\) In

---


\(^11\) From 11 September 2001, western political leaders consistently sought to emphasise that the ‘war on terror’ was not a war on Islam. For example, in his State of the Union Address in 2002 President Bush reminded his audience that Islam’s history was rich: “with its centuries of learning, and tolerance, and progress” and as such it connected with the values he presented as being threatened. See ‘Bush State of the Union Address’, *CNN.com Inside Politics*, 29 January 2002, accessed 10 March 2010, [http://edition.cnn.com/2002/ALLPOLITICS/01/29/bush.speech.txt/](http://edition.cnn.com/2002/ALLPOLITICS/01/29/bush.speech.txt/). Tony Blair made a similar argument in his
a statement outlining the government’s action plan against terrorism, Tony Blair stressed:

Time and again, over the past few weeks, I have been asked to deal firmly with those prepared to engage in such extremism; and most particularly those who incite it or proselytise it. The Muslim community have been and are our partners in this endeavour. Much of the insistence on strong action to weed out extremism is coming most vigorously from Muslims themselves, deeply concerned lest the activities of the fanatical fringe should contaminate the good reputation of the mainstream Muslim community in our country.12

On a more practical basis this emphasis represented an implicit acknowledgement that particular counter-terrorism practices, specifically the mechanisms of countering radicalisation domestically, needed refining. It was an illustration of how discourse and practice influence each other, further demonstrating the process aspect of securitisation.

Over time, further reiteration of the macrosecuritisation was evident in the UK. The Home Secretary, Charles Clarke, talked about how the 2005 attacks had

---

demonstrated again the “different kind of threat being faced”. The Chairman of the Home Affairs Select Committee, John Denham, suggested that the threat posed by terrorism would last for at least 30 years. While in one report, the House of Commons Foreign Affairs Select Committee argued that despite progress being made in dismantling the Al Qeada leadership, the network still posed a significant threat. This also illustrated a tendency to continually highlight new dimensions to the presented threat. Later other events also resulted in reiteration. For example, after a foiled plot in August 2006 to blow-up approximately 10 trans-Atlantic aircraft, the newly appointed Home Secretary, John Reid, argued in a speech to the think tank Demos that Britain was facing “probably the most sustained period of threat since the end of the second world war”, accusing the government’s critics of not understanding the threat faced.

---


14 Ibid., Charles Clarke reply to Q30 and John Denham Q3.


Beyond discourse, continued counter-terrorism practice also demonstrated acceptance of the macrosecuritisation. For example, the emphasis on enhanced co-ordination between those responsible for counter-terrorism led to further institutional changes. The Commissioner of the Metropolitan Police (MET) Sir Ian Blair confirmed that plans for institutional re-organisation in the form of an amalgamation of his force’s Anti-Terrorist Branch (SO13) with its Special Branch (SO12) to form a new single Counter Terrorism Command (SO15), were to be speeded up in the aftermath of the London 2005 attacks. Its broad functions remained largely unchanged, with intelligence gathering performed by those with a Special Branch (SB) background and investigational work by those former Anti-Terrorist branch officers. The new Command, that formally began work on 2 October 2006, had a workforce of approximately 2000 officers, an increase of 500 on previous combined staffing levels. Alongside this there was also a greater emphasis placed on bolstering regional counter-terrorism capabilities to enhance co-ordination when countering the presented threat. Counter-terrorism budgets also continued to


19 Steve Hewitt, The British War on Terror, p. 96.

20 Idem.

21 Such moves had begun according to Assistant Commissioner of the Metropolitan Police (MET) Andy Hayman over the previous 12-18 months. See Home Affairs Committee, ‘Hearing on Counter-terrorism and Community Relations’, 13 September 2005, Reply to Q57. The need to move towards greater regional Special Branch (SB) capabilities was raised in Her Majesty’s Inspectorate of Constabulary, A Need to Know: HMIC Thematic Inspection of Special Branch and Ports Policing (Home Office Communication Directorate, January 2003), pp.
grow. A parliamentary report noted that the total sum allocated for counter-terrorism operations by UK police specifically had risen from £59 million in the year 2002/03 to £249 million in 2007/08.

The introduction of legislation with some counter-terrorism implications remained a central feature of counter-terrorism efforts. Legislative changes occurred on such a widespread basis and with such relative urgency that Lord Carlile, the government’s independent reviewer of terrorism legislation, commented that “those of us involved on a frequent basis in the effects of the TA 2000 [Terrorism Act, 2000] find it difficult to keep up with [the] changes”. An Immigration, Asylum and Nationality Act became law in 2006, as did an Identity Cards Act, a Police and Justice Act and a new Terrorism Act. The latter created additional criminal offences relating to terrorism including encouragement of terrorism and disseminating terrorist publications, and increased the period an individual suspected of terrorism could be

13-14, 31-35 and 39-40 specifically. Two main forms of unit emerged out of this process, the regional counter-terrorism unit (CTU) and regional counter-terrorism intelligence unit (CTiU). Each drew upon staff from both within and outside of the Police, including SB officers. The different between the former and the latter was that the latter were smaller units and therefore focused on the development of counter-terrorism intelligence rather than on conducting investigations of offences. See ‘Memorandum submitted by Association of Chief Police Officers (ACPO)’, published in House of Commons Home Affairs Committee, Project CONTEST: The Government’s Counter-Terrorism Strategy (Norwich: The Stationery Office Ltd, 7 July, 2009), Ev 44-48, accessed 20 November 2010, http://www.publications.parliament.uk/pa/cm200809/cmselect/cmhaff/212/212.pdf. Similarly MI5 began to set up regional offices see Antony Field, ‘Tracking Terrorist networks’, pp. 1001-1004.

22 It had been estimated that the additional costs incurred by the Metropolitan Police between 7 July 2005 and the 1 September 2005 had amounted to £60 million and counter-terrorism expenditure would continue to rise. Home Affairs Committee, ‘Hearing on Counter-terrorism and Community Relations’, 13 September 2005, Reply to Q20.


detained without charge from 14 to 28 days.\textsuperscript{25} This was one measure it is hard to imagine would have been possible to implement without continued macrosecuritisation and represented a further example of increased state power.\textsuperscript{26}

Despite all this the London 2005 terrorist attacks also marked the beginning of a particularly public and more sustained period of reflection, with accompanying moments of resistance, in relation to the presented international terrorist threat and UK response to it. Those who had rejected outright the idea of a ‘war on terror’ and the macrosecuritisation it captured, highlighted in chapter two, remained vocal. In the days after the attacks for example, George Galloway expressed his view that the increased threat of terrorist attack in Britain had been the result of UK military action in Afghanistan and Iraq, both elements of the ‘war on terror’.\textsuperscript{27} According to the BBC Galloway challenged the way in which the west continued with “war and occupation as the principal instrument of our foreign and defence policy”\textsuperscript{28}

\begin{footnotesize}
\begin{enumerate}
\end{enumerate}
\end{footnotesize}
More widely while UK political leaders had never utilised the phrase ‘war on terror’ or variants of it to the extent witnessed in the US, there was further discussion in this period over the appropriateness of the terminology used. A report by the House of Commons Foreign Affairs Select Committee in 2006 stated, “we have come to the conclusion that the phrase ‘war against terrorism’ is inappropriate”, while in the media the difficulties with undertaking a ‘war’ on a tactic were noted. The extent to which this also represented resistance to the idea of a ‘war’ being an appropriate response to the presented threat was less clear. Certainly military solutions continued to be pursued in Afghanistan and Iraq, while the blurring of the divide in relation to domestic counter-terrorism efforts between a military and criminal justice approach continued to be evident, most prominently in the government’s focus on expanding pre-charge detention powers.

Ultimately, as has already been argued in this thesis, it is the grammatical structure of “existential threat, point of no return, and a possible way out” that is significant. In short, while there was increased discussion over and resistance to the use of the phrase ’war on terror’, and even the idea that a military response was appropriate, the

---

29 Foreign Affairs Committee, *Foreign Policy Aspects of the War against Terrorism*, p. 15. In terms of media commentary Daniel Keohane quotes the Financial Times Columnist Martin Wolf as arguing that, “a war against terror is absurd. One cannot fight abstract nouns. To declare war against any or all terrorists is lunacy.” Martin Wolf quoted in Daniel Keohane, *The EU and counter-terrorism* (London: Centre for European Reform Working Paper, May 2005), p. 7, accessed 14 November 2010, [http://www.cer.org.uk/pdf/wp629_terrorism_counter_keohane.pdf](http://www.cer.org.uk/pdf/wp629_terrorism_counter_keohane.pdf). Outside of the UK, in late July 2005 leading US government figures such as Defence Secretary Donald Rumsfeld also began to utilise different terminology including phrases such as “a global struggle against the enemies of freedom”. Abandonment of the phrase though was not universally pursued in the United States (US) and as Rumsfeld’s new terminology suggested there had not been a sudden departure from the view that terrorism represented an existential threat to the ‘civilised way of life’. See Donald Rumsfeld quoted in ‘New name for ‘War on Terror’’, *BBC News Online*, last updated 27 July 2005, accessed 9 November 2010, [http://news.bbc.co.uk/1/hi/world/americas/4719169.stm](http://news.bbc.co.uk/1/hi/world/americas/4719169.stm).

'war on terror' discourse remained stable because the macrosecuritisation which it captured continued to be reiterated and accepted. This can be seen in the emphasis on the emergency facing the UK, the calls to defend freedom and “civilised people” noted earlier in this section and the continued prominence of counter-terrorism on the policy agenda.

Alongside this, reflection and resistance remained largely directed at particular counter-terrorism practices. In the immediate aftermath of the London 2005 terrorist attacks, a variety of parliamentary committees’ organised evidence gathering sessions during the course of writing official reports to examine issues relating to terrorism and counter-terrorism.  The questions asked remained the same, ‘Was the existing counter-terrorism security response working?’ and ‘What, if anything, should come next?’ The nature of events meant associated discussions increasingly fell on the radicalisation of a minority of British Muslims, the links between domestic and foreign policy and the issue of transport security.  In terms of the


existing response, Lord Carlile, critiqued the application of some 2000 Terrorism Act powers. Focusing on the use of Section 44, he wrote:

Above all, it is now recognised as important that police officers on the ground (in sometimes challenging situations) must have a fuller understanding of the differences between the various stop and search powers open to them. The aim should be that in all circumstances they stop and search in appropriate circumstances only, and that they use the powers most fit for purpose. If that does not apply, the kind of inappropriate use of the section 44 powers such as occurred at the 2005 Labour Party conference in relation to Walter Wolfgang will recur.33

In relation to proposed emergency measures, the plans to introduce ID cards, which had long been an issue of political contention, led to a breakdown of cross-party consensus in Parliament in this period.34 Resistance however was most prominently directed at the Terrorism Act, 2006 and its pre-charge detention component specifically. There were also growing concern over whether the UK had been involved in the process of ‘extraordinary rendition’ - where certain terrorist suspects were flown by the US to countries which could utilise methods recognised as torture during questioning - by allowing flights to utilise its airspace, airports, and by sending questions for suspects to the country where the questioning was taking place.35


35 In November 2005 the Association of Chief Police Officers (ACPO) launched an investigation in to accusations that the UK had been complicit in extraordinary rendition. In June 2007 Chief Constable Michael
In terms of pre-charge detention the government’s initial plan after the London 2005 terrorist attacks had been to increase the pre-charge detention period from 14 to 90 days. Pre-charge detention had long been a controversial issue in the UK, yet the Prime Minister remained convinced that in the aftermath of the London bombings circumstances had changed, commenting “for obvious reasons, the mood now is different. People do not talk of ‘scaremongering’”. Blair suggested that he had public support, yet despite this the proposal was not universally popular amongst parliamentarians. On similar lines concerns were also raised that leading police officers had played an unusually proactive role in supporting the government’s pursuit of the proposal. One submission to the Home Affairs Select Committee


suggested that senior police officers may have been involved in lobbying MPs, challenging the norm of non-involvement by Police in political discussions. In an exchange during one evidence session, the then Assistant Commissioner of the MET Andy Hayman resisted a suggestion by David Winnick MP that his argument was that MPs should accept the 90 day extension simply because the police as specialists supported it.

The 90 days detention proposal was resisted on a number of different grounds. Organisations such as the Campaign Against Criminalising Communities (CAMPACC) argued that the proposals risked extending the scope for further abuse of state powers, while the resistance even directly chimed with the language of securitisation itself. When asked if she could envisage any scenario where extended pre-charge detention would be acceptable, the Director of Liberty Shami Chakrabati explained:

What I would say about those sorts of cataclysmic moment, the moment where those in power declare the state of exception where, for a time, the rulebook is truly put aside is that if moments of that kind are adopted too easily and in an unending war or an unending emergency, that is incredibly dangerous indeed and that is effectively the end of our society. Moments of that kind should only be entered into as the very, very last resort, not just because we have been attacked, not just because people's lives have been lost, but because the State effectively cannot function.

38 Ibid., Memorandum submitted by Mr Evan Price, Appendix 12, Ev 98-99.
39 Ibid., Ev 37-38. This was not the first time the police’s role in relation to supporting legislation was highlighted. Steve Hewitt makes a similar point relating to the aftermath of the ricin plot in 2003. Steve Hewitt, The British War on Terror, pp. 43-44.
40 Ibid., Ev 77.
Chakrabati would make a similar point about the dangers of a sustained period of exceptionalism in a later committee appearance, yet acknowledged that the terrorist threat was real and could be long term.42 Another witness to the Home Affairs Committee utilised a hypothetical conversation with the families of the victims of the London 2005 terrorist attacks to advance his case. He suggested he would tell them that, “it is very important for us to continue to safeguard the values under which they lived and not to give way to legislative panic, not to give way to hasty measures which actually have the effect of undermining everyone's freedoms”.43

As with particular events this reflection and resistance also created the space in which further reiteration of the macrosecuritisation through the reproduction of the ‘war on terror’ discourse could take place. This further energised the calls to maintain constant vigilance and no complacency with regards to the presented threat. After the London 2005 terrorist attacks, Charles Clarke suggested previous warnings about terrorism had gone unheeded, yet had tragically come true.44 He challenged critics to offer up their own solutions, positioning his own proposals as the only viable option available. He told the House of Commons:


44 Home Affairs Committee, Counter-terrorism and Community Relations, Ken Livingstone, Reply to Q79. The Transport Secretary Alastair Darling made a similar point relating to emergency planning preparations in transport when he said: “A lot of this work was treated with considerable scepticism by some commentators at the time. They said it wasn’t necessary, that we were scaremongering. We saw that here when we tested more kit in 2003: men in space suits on the front pages. Most people saw the sense of it. But some didn’t”. Alastair Darling, ‘Anti-Terrorism in Public Transport’, International Association of Public Transport (UITP) security conference, 14 November 2005, accessed 15 May 2008, http://webarchive.nationalarchives.gov.uk/+/http://www.dft.gov.uk/press/speechesstatements/speeches/dealingwiththeterroristthreat.
We can decide at the end of the day we do not care what the police think, we can decide at the end of the day we do not mind tying our hands behind our back when dealing with a terrorist threat and that situation, but that is not a position I can adopt. [...] I can understand, I suppose, that people can look at it very carefully and reject that, but I then think they have an obligation in their abhorrence of terrorism to say what they would do to contest this organisation. The 'let's hope it's all right on the night’ school is one that I cannot go along with.

Yet ultimately the opposition triumphed over the government on 90 days detention. In one of the few Parliamentary defeats of Tony Blair’s time in office, the government settled for a figure of 28 days pre-charge detention.

Beyond the rather obvious point that this example illustrates how the implementation of emergency measures is not a smooth process, two additional insights are evident. First, while securitisation requires audience acceptance that a response is a necessity which in turn imbues the policy process with urgency, there remains an element of negotiation over the specific content of emergency measures and how they are delivered. This represents the distinction, highlighted in the first chapter, between being able to accept that securitisation has a general result, namely the politics of emergency, while still acknowledging that the specific nature of that emergency is open to further investigation.

45 Charles Clarke, ‘Draft Terrorism Bill’, Home Affairs Committee, Reply to Q56.

46 Government defeat came at the Report Stage of what became the Terrorism Act. 322 MPs voted against ninety days against 291 who supported it. MPs subsequently supported an amendment to increase the maximum period to 28 days by 323 votes to 290. See: (Division No. 84 & No. 85) ‘Terrorism Bill’, House of Commons, Hansard starting column 378, 9 November 2005, accessed 20 November 2010, http://www.publications.parliament.uk/pa/cm200506/cmhansrd/vo051109/debindx/51109-x.htm.
Second, there is a clear need to place those measures which are eventually implemented in their wider context, reminding us of why, despite this case study examining developments in three parts, it is the overall trends over five years that are of greatest significance. The result here then, a doubling of the pre-charge detention period, further illustrates how the boundaries of acceptable practice had undoubtedly shifted from those of pre-September 2001 or even pre-July 2005. 28 days pre-charge detention then was far less than the government had sought, but it represented a substantial increase on practice just five years earlier. Moreover the debate had largely been about how long an individual should be detained without charge, not whether the practice was in principle desirable. Even if this resistance strategy was a practical one, in the sense that slowly, in small steps, those resisting sought policy change, it suggested a continual lack of belief, and unwillingness, perhaps an inability to directly resist the idea that terrorism posed an existential threat. Securitisation still restricted the parameters of debate.

(4.3) UK maritime infrastructure as a ‘site of securitisation’:

Despite the greater level of introspection after the London 2005 terrorist attacks with acts of resistance emerging, the previous section demonstrated how the ‘war on terror’ discourse and the macrosecuritisation of the ‘civilised way of life’ which it captured remained stable. The terminology of ‘war’ may have been jettisoned even further, yet the idea that international terrorism posed an existential threat which needed tackling remained accepted. The continued reiteration of the presented threat

---

47 Tony Blair continued to reiterate his belief that a longer period of detention without charge, possibly up to 90 days, was still necessary. ‘Blair pushes for 90-days detention’, BBC News Online, last updated 16 November 2006, accessed 9 November 2010, http://news.bbc.co.uk/1/hi/uk_politics/6153488.stm.
by western political leaders and others, alongside the continued implementation of emergency measures illustrated this acceptance. Recognising the mutually reinforcing relationship between the macrosecuritisation of the ‘civilised way of life’ and the securitisation of UK maritime infrastructure illustrated throughout this case study thus far, it was not a surprise that in the aftermath of the London 2005 terrorist attacks and the following two year period, maritime infrastructure continued to be securitised. Commenting on the London 2005 terrorist attacks, the maritime industry newspaper Lloyd’s List, in an editorial, argued that the attacks were:

> a reminder of the need for vigilance, for improving contingency plans and perhaps rather less scepticism of whether security precautions are ‘over-the-top’ or an unnecessary burden to normal urban life.  

The reproduction of both the ‘target’ and ‘vulnerable node’ narratives relating to UK maritime infrastructure, which drew upon the macrosecuritisation and had been witnessed consistently in the previous years, continued to be take place. Internationally the Secretary-General of the International Maritime Organization (IMO), Efios Mitropoulos, opened a policy meeting of his organisation with a reiteration of the macrosecuritisation, noting the urgency of the situation despite nearly three years having passed since the IMO had first agreed the need for the ISPS code. He argued that it was:

> a sign of the turbulent times in which we live nowadays that the scourge of terrorism has come to dominant the international agenda; and, as a result, the great majority of us who form civil society must, as a matter of great urgency,

---

do all that we can to thwart the efforts of those who seek to *distort the fabric of society and eventually disrupt our daily life or destroy our world.*

At the regional level of governance the relationship between macrosecuritisation and securitisation of maritime infrastructure generally was encapsulated in a European Union (EU) directive that introduced an ISPS-inspired regime from the port/ship interface to the entire port area. It noted in its introduction that:

> Security incidents resulting from terrorism are among the greatest threats to the ideals of democracy, freedom and peace, which are the very essence of the European Union. [...] People, infrastructure and equipment in ports should be protected against security incidents and their devastating effects. *Such protection would benefit transport users, the economy and society as a whole.*

Within the UK it was increasingly visible how the narratives were reproduced as part of discussions relating to the security of the wider supply chain, transport network and UK border, all of which maritime infrastructure was regarded as part in its position as an example of critical national infrastructure.

---


The idea that UK maritime infrastructure may be a target of terrorism and/or a vulnerable node that could be exploited by terrorists, with all the ramifications associated with this, was raised, often indirectly, in reviews over UK immigration policy, border controls and in a House of Commons report into transport security to name just three examples.\textsuperscript{52} Perhaps unsurprisingly, taking into account the nature of the London 2005 terrorist attacks, it was the focus on transport security that was most prominent. One preliminary transport security report opened with the comment that, “more recent outrages closer to home, the fatal bombings in London on 7 July 2005, and the events of 21 July, have propelled transport security, and the vulnerability of the UK’s transport networks to such attacks, into the forefront of British public consciousness.”\textsuperscript{53} The threat to UK transport systems was described as “formidable” and long-term with the Transport Select Committee adding, “we have no reason to challenge the Secretary of State’s sombre view of the present risk that ‘it is one that we are going to be living under for the rest of our lives and probably our children’s lives as well’”\textsuperscript{54}.

Different dimensions to the presented threat also found prominence, while perceived weaknesses and gaps in the existing counter-terrorism security response continued to


\footnotesize{\textsuperscript{53} Transport Committee, ‘UK Transport Security’, p. 5.}

\footnotesize{\textsuperscript{54} Ibid., p. 6.}
be highlighted as implementation was ongoing. More specifically concerns were expressed over the threats posed by terrorists to small vessels (including pleasure craft) and to smaller ports and harbours. In mid-2006 Lord Carlile told BBC Radio Four that there were holes in the border security shield, questioning whether there were enough Immigration and Customs officials within smaller ports to offer adequate protection.\(^55\) At the 82\(^{nd}\) meeting of the IMO Maritime Safety Committee in September 2006 similar concerns over small vessels were reiterated, while the threat posed by terrorists to both on and off-shore energy terminals was noted in the media.\(^56\) On similar lines it was not unusual for members of the policy network interviewed in the course of researching this case study to highlight particular dimensions of the presented threat and perceived weaknesses and gaps in the existing response. References to certain issues as representing the “soft underbelly” of security or a particular location as a “back-door” in to the United Kingdom were made.\(^57\) Each was a further example of the way in which the reproduction of


\(^56\) In a submission to the IMO, the US argued that: “smaller ships present different security challenges which may be best addressed by a different set of standards. Such ships can be serve as a conveyance of a weapon, prohibited cargo, or prohibited person from one place to another, offering the potential to compromise the integrity of the global supply chain and introduce additional risk to the receiving port. [...] Small ships, by virtue of their relatively small size, potential for high speed, and keen manoeuvrability characteristics, are more likely to be used as a weapon against larger vessels or critical shore-side infrastructure.” Submission by the United States, ‘Enhancement of the security of ships other than those already covered by SOLAS Chapter XI-2 and the ISPS Code (MSC 82/4/4)’, Maritime Safety Committee, International Maritime Organization, 27 September 2006. The “nightmare scenario” of one maritime security expert was described as “two fishing boats being hijacked, filled with explosives and then rammed into one or more North Sea platforms”. Commander Mike Mason, Maritime Security Programme Co-ordinator, Centre for Defence and International Security Studies quoted in Denzil Stuart, ‘Warning that UK offshore sector may be vulnerable to terrorism’, Lloyd’s List, 14 July 2005, p. 2. Also see David Osler, ‘Keeping the pin in the oil and gas timebomb’, Lloyd’s List, 11 August 2005, p. 5; David Osler, ‘Chemical Facilities may be targets, warns terror expert’, Lloyd’s List, 13 October 2006, p. 6 and ‘Experts submit Europe port security plan’, Lloyd’s List, 17 October 2006, p. 3. All accessed IMO Knowledge Centre 19-21 October 2009.

\(^57\) Author’s interview with number 4, 1 April 2009 and other more informal discussions during site visits.
narratives and in turn the reinforcement of the securitisation of UK maritime infrastructure took place.

In terms of reflection and resistance in this period, it remained largely directed at the response as will be elaborated in the following section. Regarding threat perception internationally, considerable controversy surrounded a challenge made by Democratic politicians in the US Congress in particular to prevent the Dubai-based group DP World taking over a number of American ports owned by P & O on a number of grounds including fears over national security. Many, including the Bush administration itself, felt Congressional concerns were misguided.\(^{58}\) The maritime journal Fairplay for example was stark in its criticism, arguing the national security dimension was being exaggerated and suggesting the words of journalist HL Mencken were appropriate:

‘The whole aim of practical politics,’ he once observed, ‘is to keep the populace alarmed (and hence clamorous to be led to safety) by menacing it with an endless series of hobgoblins, all of them imaginary.’ And the rhetoric surrounding the DP World controversy fits that category nicely, being based largely on paranoia, ignorance and just a slight tinge of racism.\(^{59}\)


\(^{59}\) Editorial, ‘What’s to fear?’, Fairplay, 23 February 2006, pp. 1-2, accessed IMO Knowledge Centre 19-21 October 2009. The editorial also asks “Who is the bigger threat: Al-Qaeda or Al Capone?” as it raises concerns about mafia control of waterfront unions.
In the UK what was increasingly noticeable was how the policy network demonstrated an awareness of nuance in relation to the presented threat. Discussing transport security more generally, the Transport Secretary Alastair Darling acknowledged that there were obvious difficulties in implementing an aviation-style system of security in an open, mass transit transport system such as the rail network, a case noted in the previous chapter. He explicitly emphasised the need, highlighted as one of the main characteristics of the counter-terrorism security response, to focus on “a ‘layered approach’ to security – because no single security measure is either foolproof or capable of mitigating every threat. You need a range of measures”.  

Similarly when asked how much attention was being placed on the maritime environment the Director of TRANSEC Nikki Tompkinson responded by arguing:

I think we have a good regime in place. I think it is proportionate to the level of threat and, I think, as will be obvious, if you look at what has happened around the world, aviation and rail tend to feature more than maritime; maritime is there but it is, I would judge, of a slightly different order.

Moreover, in terms of the security response level set in relation to UK maritime infrastructure, after both the London 2005 attacks and the foiled trans-Atlantic bomb plot in August 2006 the level remained unchanged even as the level for aviation was increased.

---

60 Alastair Darling, ‘Anti-terrorism in Public Transport’. As it was elaborated in the previous chapter, TRANSEC embraced this layered approach in its activities in the maritime environment.


62 This was a point emphasised in relation to the London 2005 attacks in one interview conducted by the author. Also see Terry Sutton and Hugh O’Mahony, ‘UK ports keep security at ‘moderate’ level as terrorist threat brings air travel to halt’, *Lloyd’s List*, 11 August 2006, p. 1, accessed IMO Knowledge Centre 19-21 October 2009.
This awareness of nuance was just as visible on the ground, if not more so, than in the public pronouncements and actions of those in UK central government be that political leaders or regulators. Accepting the distinction between maritime infrastructure as ‘target’ and ‘vulnerable node’ advanced in the line of questioning, one port security manager explained that while he could not rule out a terrorist attack in his port, there had not been a major terror alert. Instead it was far more likely that something related to international terrorism could transit through the port.\(^{63}\) Another interviewee shared this view arguing “my concern would have to be the port as a soft underbelly and backdoor for a wider range of subversive and terrorist assets coming in to the country”.\(^{64}\) His personal assessment was that approximately 75% of his work was concentrated on the port being a ‘backdoor’, as opposed to 25% on the port as a target itself.\(^{65}\) A third interviewee also noted that while maritime infrastructure may have had a ‘moderate’ threat level as a target of terrorism, this did not take in to account the threat level associated with its role as a facilitator of terrorism.\(^{66}\)

A further illustration of nuance came when discussions turned to determining the extent to which maritime infrastructure could in some ways be regarded as a ‘poor relation’, always playing catch-up in security terms in comparison to aviation infrastructure. Here there was some disagreement between those security professionals interviewed. One SB ports officer noted how the maritime environment

\(^{63}\) Author’s interview with number 7, 18 March 2009.

\(^{64}\) Author’s interview with number 4, 1 April 2009.

\(^{65}\) Idem.

\(^{66}\) Author’s interview with number 1, 19 March 2009.
definitely did not get the attention it deserved commenting, “the airport side has always been the more glamorous side”. Yet for one port manager a comparison between aviation and maritime infrastructure security was regarded as unhelpful. Utilising the example of the failed attempt by Umar Farouk Abdulmutallab to blow himself up during a flight to Detroit in late 2009, he explained:

I don’t think that the security requirements for the aviation industry should necessarily be overlaid and then measured in the maritime industry. The whole thing is so very, very different. The aviation industry is young; the maritime industry is old. The size and scale of it is very different, the consequences are very different. [...] The best thing he [the Detroit bomber] would have done if he tried that on a ship is blown his knackers off. You know he wouldn’t have really have made much of a spectacular. Yes it would be very interesting, yes we would get very excited about it, yes we would need to do a lot about it, but it wouldn’t [...] sink a ship. Whereas it would bring an aeroplane down, so the consequences of that sort of threat are very different. So we actually really need to be thinking of different ways of what we are doing.

(4.4) UK maritime infrastructure – the post-securitised environment:

What the previous section illustrated was that a greater complexity was evident in relation to both the reproduction of the two main narratives relating to UK maritime infrastructure and the accompanying reflection and resistance. To continue the focus on how the counter-terrorism security response was reflected upon and in what form resistance was evident in this period, the transition from discourse to practice as the focal point of examination again needs to take place. As it has been noted, it was

67 Author’s interview with number 2, 28 July 2009.
69 Author’s interview with number 11, 3 March 2010.
clear that reflection and indeed resistance continued to be largely directed at particular elements of the counter-terrorism security response.

The ISPS code remained the subject of considerable reflection particularly as ports internationally began to face up to assessing the results of their first year audits of security practice.\(^\text{70}\) Here it was particularly noticeable how there were disagreements over where security standards were highest. Although it was suggested that the US could be distinguished from the rest of the world in terms of the high quality of its security practices, the Chief Executive of International Maritime Security Geoff Greaves argued that within Europe the UK stood above its neighbours.\(^\text{71}\) Greaves suggested that the UK remained the only European country to apply the code “to the letter” and that many other governments treated security certificates simply as “handing out bits of paper”. This further illustrates the efforts made and noted in the previous chapter on distinguishing between different levels of compliance.\(^\text{72}\)

Concern over the level of implementation of ISPS procedures in European ports had been long-standing. The previous year an anonymous letter to journal Fairplay reported a series of lapses in ports in the Netherlands, Belgium and France. The author ended his letter with stinging criticism writing:


\(^{72}\) ‘Europe makes ‘mockery’ of ISPS Code, says Greaves’, \textit{Lloyd’s List}. 
I have one question: where is ISPS in Europe? We Europeans are just playing with our security. Sooner or later, we will have the same problems as the US. Europe, wake up. It is time to take your responsibilities seriously. It is already too late, but better late than never.\(^73\)

The letter’s message was satirically encapsulated in this accompanying cartoon.

*Image 6 – Big Mac:*\(^74\)

Beyond this, reflection and occasionally resistance in relation to the ISPS code continued to largely coalesce around maintaining the three balances – a balance between security and commercial activities, between security and liberty encapsulated in calls for fair treatment of seafarers, and over who had what


\(^74\) Image 6 – ‘Big Mac’, reproduced with the kind permission of cartoonist Steve Burke and Fairplay. This cartoon was originally published in ‘Europe’s open-door Port Policy’, Fairplay.
responsibilities in relation to the implementation of the response. However a host of additional issues were also discussed. One journal raised the issue of boredom created by associated paperwork suggesting the emphasis on compliance could come at the detriment of security. Another highlighted concern that smaller companies had struggled with the burdens imposed by the ISPS code. There was also focus on the extent to which security practices impinged on safety. Collectively this contributed towards those responsible for maritime infrastructure security outside of the UK still emphasising the need to institutionalise further the existing counter-terrorism security response, including the ISPS code. This emphasis was shared within the UK, but it was relatively less significant as there was little evidence of any major problems relating to the code.


With the code firmly embedded in the UK, coupled with the impact of events like the 2005 terrorist attacks in London, the balance of developments in this period fell on adding to the response beyond the code. This situation emerged out of associated developments particularly relating to the security of the wider supply chain, transport network and UK border, of which maritime infrastructure was part. This was not unique to this period, as has been acknowledged on a number of occasions already in this case study, yet ultimately it was the continued implementation of the response that demonstrated UK maritime infrastructure was a ‘site of securitisation’. Breaking down the totality of counter-terrorism practice in to its three constituent parts again these developments can be elaborated, while both the features and main characteristics of the response are further illustrated. Due to the multi-levelled governance of the maritime industry, developments outside of the UK are again also discussed to fully contextualise trends.

(4.4.1) Legislation and regulations:

With regards to the ISPS code, those efforts noted in the previous chapter to implement a similar security regime beyond the ship/port interface formally materialised in October 2005 when the European Council and Parliament adopted a new directive (EC 2005/65).\(^{81}\) It was a clear sign of the increasingly expansive scope of the counter-terrorism security response, not simply in the way in which it represented a further measure added to it, but in the way in which security focus fell over a wider geographic area. A spatial dimension then to this expanding scope was

---

evident. Equally, the emphasis on harmonising and improving security standards was again illustrated as the directive’s objective was to establish a framework for the EU as a whole. Member states were directed to designate a port security authority for every major port that was to be responsible for identifying and taking the necessary port security measures in line with port security assessments and plans. With regards to those port security assessments, the directive noted that “areas will be judged not only upon their direct profile as a potential target, but also upon their potential role of passage when neighbouring areas are targeted”, representing a direct example of the reproduction of the two main narratives in official regulatory documents. Member States had to comply with the directive by 15 June 2007.

In the UK, this process was by no means smooth as a view was held by both regulators and the industry that the requirements set out in the directive had already largely been met. For example, the demands that security assessments and plans were reviewed at least once every five years, and that annual basic training covered “communication, coordination, resource availability and response”, were already in place and on occasion had already been exceeded. This meant that in this period, and by the end of June 2009, the directive actually led to very few infrastructure developments, nor had a significant impact on working practices in the UK. Ultimately it was the need to create port security authorities over which disagreements between the EU and UK became most apparent. UK authorities

82 Ibid, Paragraph 10.
83 Ibid., Annex I. Italics added by author for emphasis.
84 Ibid., Article 18, 1.
85 Ibid., Article 10, I and Annex III.
argued that the existence of port security committees represented compliance as their activities were what the directive envisaged for port security authorities. Yet the EU disagreed seeking to ensure such institutional structures were established and governed on a statutory basis. At one point the UK was even threatened with legal action for non-compliance.\textsuperscript{86} Interestingly the differences of opinion were about whether requirements had been met and were not over whether an extension was itself necessary, where there was agreement. Eventually the UK did introduce secondary legislation transposing the directive’s requirements in to UK law and set about creating port authorities, but this did not take place until the second half of 2009 after the case study period.\textsuperscript{87}

Beyond the ISPS code, other legislative and regulatory developments were pursued in this period. The IMO, for example, concentrated on updating the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA) treaties that helped govern behaviour at sea. At a diplomatic conference held in London in October 2005, new protocols were agreed. These included broadening the list of offences deemed unlawful to more explicitly cover efforts to utilise shipping to transport chemical, biological, radiological and nuclear (CBRN) materials and/or be utilised as a weapon itself, and new provisions to enable states to board ships under suspicion


of being associated with unlawful acts. Although the SUA changes did not directly influence day-to-day activities within UK maritime infrastructure, they did further illustrate the belief held within the IMO in the value of ensuring its regulatory frameworks evolved in order to defeat what the organisation’s Secretary-General had described as the “scourge of terrorism worldwide”. They also demonstrated the IMO’s emphasis on enhancing co-ordination at the international level to meet that presented threat. More pertinently still, the changes showed how IMO member states were sufficiently concerned over the potential for vessels to be utilised as weapons and/or mechanisms to transport dangerous materials ashore, that they sought greater powers to intervene against a vessel before it got to land.

This was representative of an emphasis from members of the policy network right along the policy chain and at all levels of governance to seek to tackle the threat presented as being posed by international terrorism further away from a state’s territory. It was further evidence of the expansion in scope of the response not simply from the ship-port interface to the whole port, but beyond that. To

---


91 On similar grounds in May 2006 the IMO adopted a resolution to formally introduce a ‘Long-Range Identification and Tracking’ (LRIT) system internationally. Here passenger ships, cargo ships of 300 gross tonnage and above, and mobile offshore drilling units would, amongst other things, have to report their location with the country with which they were registered (the flag state) at least four times a day. See ‘Resolution MSC.202(81) Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974
understand this expansion it is necessary to shift focus on to developments relating to wider supply chain security, and specifically legislative moves by the US Congress to mandate that 100% of in-bound containers to the US were scanned for CBRN materials prior to their departure. Despite being a foreign initiative, it was relevant to UK infrastructure because of the international and inter-connected nature of the maritime industry. The US’ prominent position in trading terms forced those outside to look up, take note and have an opinion on the issue if only out of commercial necessity. Congressional desire to prevent ‘dirty bombs’ arriving in the US was understood to require greater oversight by the state over activities within maritime infrastructure. For 100% scanning to be effective more information had to be collected on containers and their carriers, and enhanced co-ordination across different levels of governance and between different states was regarded not simply as desirable, but as a necessity.

The scanning proposal built on previous US efforts such as the Container Security Initiative (CSI).

In a leaflet explaining the initiative it was explicitly noted that, “in post-9/11 America the Container Security Initiative (CSI) is based on an idea that makes sense: extend the zone of security outward so appropriate enforcement actions...”


can be taken earlier in the supply chain”. 93 The language of extending the zone of security outward effectively captures the spatial dimension to the increasingly expansive scope of the counter-terrorism security response relating to UK maritime infrastructure. Ultimately the 100% scanning proposal was widely resisted both within and outside the maritime industry and within and outside the US, demonstrating further the inter-connected nature of the industry. The resistance coalesced around concerns that the proposal would disrupt trade, was overly bureaucratic, highly impractical, especially in financial terms, and represented an expansion of US sovereignty in to other states. 94

It was directed predominantly at the content and perceived negative impact of this specific proposal and not particularly at either the idea of extending the zone of security, or that there was a terrorist threat relating to the wider supply chain and by association maritime infrastructure as one part of it. During spring 2006 the legislative ping-pong within Congress was considerable, with Democrats pushing the 100% scanning proposal, and the Bush administration largely critiquing it. One prominent supporter of 100% scanning was Democratic Congressman Jerrold Nadler who, in a press release in April 2006, lambasted the Bush administration on the issue commenting, “it’s common knowledge that Al Qaeda wants to sneak a nuclear


94 The resistance to the idea of 100% scanning, prompted by and directed at a variety of different draft Congressional bills, was captured by the maritime media over the course of the period. For example see Janet Porter, ‘US ports Bill to cause chaos, warns Koch’, Lloyd’s List, 5 April 2006, p. 1; Janet Porter, ‘Hutchison boss joins US ports security debate’, Lloyd’s List, 19 April 2006, p. 3; ‘Impending US box inspection laws ‘could shut ports and disrupt trade’, Lloyd’s List, 10 January 2007, p. 3; Opinion, ‘Through a box, clearly: seeing the sense behind seemingly dumb proposals’, Fairplay, 18 January 2007, pp.1-2 and Justin Stares, ‘Screening ‘will disrupt trade ‘’, Lloyd’s List, 26 January 2007, p. 3. All accessed IMO Knowledge Centre 8-10 February 2010.
weapon into this country – yet this Administration has been content to let 95 percent of the shipping containers we receive go uninspected”. Eventually a compromise solution seemingly emerged in the form of the Security and Accountability for Every (SAFE) Port Act, which encapsulated the concept of 100% scanning but sought to limit it to a selection of ports on a trial basis.

This represented a small victory for those who sought a less prescriptive, more intelligence and goal-based counter-terrorism security response, although the trajectory towards further expansion had been set. In early 2007, after Democratic victory in the 2006 mid-term elections, the demands for making 100% scanning universal once again grew. This reflection, even resistance also illustrates how opinions on the specific mechanics of delivery diverged along the policy chain.


96 ‘Security and Accountability for Every Port Act’, signed in to law 13 October 2006, accessed 27 February 2010, http://www.gpo.gov/fdsys/pkg/PLAW-109publ347/content-detail.html. The act was the result of two separate bills merging. The first was the ‘GreenLane Maritime Cargo Security Act’ which was introduced in the Senate in January 2006 and passed on 14 September 2006 by 98-0. The second was the ‘Security and Accountability for Every Port Act’ which was introduced in the House of Representatives in March 2006 and was passed by 421-2 on 4 May 2006. On 29 September 2006 a joint committee of Congress met to merge the two bills which took the SAFE Ports Act name and was passed on 30 September 2006 unanimously in the Senate and by 409-2 in the House. The final bill included the 100% scanning mandate but without a deadline for its implementation and called for a trial in three foreign ports. It also, amongst other things, set a funding allocation for elements of port security, and placed in law the Container Security Initiative and the Customs-Trade Partnership Against Terrorism (C-TPAT). For further information on the Act see Kenneth Christopher, Port Security Management, p. 105. See the same source for information on C-TPAT, p. 212.

97 The Democrats took control of both the Senate and House of Representative in the 2007 mid-term elections. As part of their first 100 days in control they introduced in the House the ‘Implementing Recommendations of the 9/11 Commission Act’. It included a provision to ban containers bound for the US from countries that shipped more than 75,000 containers to the US in 2005, which had not been scanned at their port of origin with US-installed equipment and US-mandated electronic seals within three years from the bill becoming law. The provision would extend to all countries within five years of the bill’s passage. The bill passed the House by 299-128-8 on 9 January 2007. The bill would become law in some form in August 2007, which will be elaborated in greater depth in the next chapter. For more information on this stage of proceedings see Rajesh Joshi, ‘US to impose box screening at foreign ports’, Lloyd’s List, 9 January 2007, p. 1, accessed IMO Knowledge Centre, 8-10 February 2010 and Rajesh Joshi, ‘Capitol Hill shows first ominous signs of “shipping by politics”’, Lloyd’s List, 8 February 2007, p. 10, accessed IMO Knowledge Centre 8-10 February 2010.
between political leaders and those members of the policy network charged with
developing legislation, and between legislators and those within the industry itself.
This reminds us both of the continual reflection which takes place as the counter-
terrorism security response is being implemented, and how that implementation is a
multi-staged process. There may be agreement that an emergency measure is
necessary, but disagreement over its content, over how it is delivered and
subsequently maintained.

The UK, like the rest of the EU, did not embrace 100% scanning, but rather
continued to place greatest emphasis on an intelligence-led approach to container
security. Despite this, there was a push to extend the zone of security outward in
different ways, which also required the collection of additional information on the
movement of both people and cargo and enhanced co-ordination between members
of the policy network. The EU began to implement various new customs regulations
based on the ‘SAFE standards’ for supply-chain security guidelines raised in the
previous chapter. One was its own ‘24-hr manifest rule’ to collect data on containers
bound for an EU port at least a day before loading commenced in the non-EU port,
although it did not seek to replicate the US practice of placing its own customs
officials in overseas ports.\(^{98}\) Another proposal was to introduce a voluntary
accreditation scheme by January 2008 to allow Member States to award companies
involved in the supply chain Authorised Economic Operator (AEO) status. This
status was to be awarded for a three year period once a set of minimum security

\(^{98}\) The 24-hr rule proposal was critiqued from within the maritime industry both on the grounds of adding
bureaucracy and for omitting certain members of the wider supply chain. See Justin Stares, ‘Industry alarm over
Brussels changes to customs code’, Lloyd’s List, 25 July 2006, p. 3, accessed IMO Knowledge Centre 8-10
February 2010 and Rajesh Joshi, ‘Brussels’ 24-hour box rule ‘fatally flawed’’, Lloyd’s List, 21 September 2006,
p. 1, accessed IMO Knowledge Centre 8-10 February 2010.
requirements had been met, enabling operators to gain fast-track treatment both within the Union and at its external borders.\textsuperscript{99} The UK also, for example, continued the process of ‘exporting’ its borders through juxtaposed controls (immigration and customs points outside of the UK) and the stationing of Airline Liaison Officers in different countries, checking passenger documents, to manage the flow of people to the UK increasingly at the point of origin.\textsuperscript{100}

\textbf{(4.4.2) Institutional changes and infrastructure developments:}

Demonstrating further the relative decline in prominence of developments relating to the ISPS code in this period, many of the developments in institutional and infrastructure terms were predominantly unrelated to the code. Internationally, in terms of institutional changes, the IMO formally established a new maritime security sub-division within its Secretariat in January 2007, further demonstrating the high priority it gave security.\textsuperscript{101} In the UK, changes in domestic counter-terrorism practice more generally had an impact on day-to-day security operations in relation to


maritime infrastructure. Despite the government’s plans for police force mergers failing in this period, emphasis was placed by political leaders on the need for ‘Active Enhancement’, where the police collaborated more closely with different members of the policy network both in the public and private sectors. This was closely associated with the previously discussed launch of the Metropolitan Police’s Counter-terrorism Command and the emphasis on developing regional counter-terrorism structures, two changes that had introduced new units’ security professionals, specifically SB ports officers, worked with.

Beyond these changes the launch of the Police National Maritime Security Strategy (PNMSS) introduced additional structures designed to enhance co-ordination not just between the police but between a number of members of the policy network responsible for the security of UK maritime infrastructure. Emerging out of the PROTECT strand of the UK government’s counter-terrorism strategy (CONTEST), the PNMSS recommended “a systematic approach to portal security” ensuring “the

consistent protection of portal regions across the UK”, by encouraging a “joined-up partnership approach making effective use of current enforcement agency and partner resources”. Each region was required to develop its own management structures in order to discuss and co-ordinate the delivery of the strategy. The most common format was for senior representatives from SB, home office police forces, immigration, customs and the coastguard in particular to meet face-to-face on a periodic basis. Others, including representatives from the national association of British ports and port managers attended dependent on the meeting agenda and/or the security level of those topics under discussion.

The borders of each region were the subject of considerable debate both during and after this time period and continued to evolve. These debates were fuelled by a series of factors including historical alliances between various police forces, considerations of police force size and threat perception. Concerns for example were expressed over the initial separation of Norfolk and Suffolk in to different portal regions, a situation that was later rectified when the former was brought in to the Thames and Dover portal region with the latter. There was also a view advanced that the Metropolitan Police was so large and had to deal with threats of a sufficiently different nature and magnitude in comparison to neighbouring forces that it made efforts to enhance co-ordination here inherently more complex.


104 Author’s interview with number 1, 23 April 2010 and informal discussion with number 16, 24 March 2009.
The PNMSS also emphasised the need to identify vulnerable sites and installations in a region for protection, recommended the creation of Regional Maritime Information and Intelligence Teams (ReMIIT) and the launch of Regional Maritime Response Teams (ReMRT) to name just three examples.\(^ {105}\) It further illustrated the ‘centralised framing and localised delivery’ approach to implementation that had already been very evident both in UK counter-terrorism efforts as a whole, and in the way in which the ISPS code had itself had been implemented with an international regulatory framework setting the environment in which policy network members in the UK operated, with the EU having an element of oversight in inspections. The PNMSS was written and subsequently maintained by the National Coordinator Ports Policing (NCPP), an office funded by the Home Office through the Association of Chief Police Officers Council Committee on Terrorism and Allied Matters (ACPO(TAM)). Amongst others things the NCPP organised national, quarterly seaport commander meetings bringing together representatives from most coastal police forces in the UK in order to ensure the strategy was effectively delivered and continued to evolve.\(^ {106}\) The NCPP had expanded its role in 2003 from co-ordinating SB activity in UK ports to include the ACPO(Ports) portfolio that encapsulated those protective services in ports provided by uniformed officers.\(^ {107}\)

---

\(^ {105}\) James Douglass, ‘Police National Maritime Security Strategy’. In author’s interview with number 4, 23 March 2010, the interviewee did not feel that the guidelines for the work of the Portal Groups were particularly prescriptive. In author’s interview with number 1, 19 March 2009, the interviewee explained that certain parts of the PNMSS were not relevant for every region as they may not have particular maritime capabilities or specific issues did not arise.

\(^ {106}\) Information ascertained during interview conducted by author. Seaport Commander Meetings were themed with one being on intelligence and another on small ports and harbours.

Moving on to infrastructure developments there continued to be investment in and use of new technology in this period as one mechanism to secure maritime infrastructure.\textsuperscript{108} Providing the means by which the information necessary to extend the zone of security outward could be collected and analysed, the government continued in partnership with the private sector to develop the necessary technology, including biometrics, to create what they described as “an integrated secure border for the 21\textsuperscript{st} century”.\textsuperscript{109} Known as the e-Borders programme, emphasis was placed on monitoring on a wider basis the travel patterns of those entering and leaving the UK and encapsulated the objective that full embarkation controls (counting everyone in and out of the country) would be reinstated by 2014.\textsuperscript{110} In short both Passenger Name Record (PNR) data and Advanced Passenger Information (API) data provided by carriers and/or collected at border points were fed in to databases enabling names to be automatically checked against watch lists and travel movements to be analysed.\textsuperscript{111} An initial trial known as Project Semaphore was the centrepiece of the programme in this period having been launched in late 2004 to run for three years.

The tasks undertaken in Project Semaphore had previously been conducted on a


smaller scale and more locally but with the use of technology and through a Joint Borders Operational Centre (JBOC) staffed with customs and police officers, the scale was increased.  

To some extent then e-Borders actually challenged the ‘centralised framing and localised delivery’ approach to implementation seen elsewhere. On a smaller scale the Department of Transport Security and Contingencies Directorate (TRANSEC) also introduced a new information management system to help better facilitate an assessment of port compliance levels with security regulations.

Overall however it continued to be port operators themselves who predominantly invested and utilised new technology. Here the technology required for port identity cards provoked significant discussions. The requirement for some form of identification for those working in and around UK maritime infrastructure was not itself new, yet the widespread introduction of secure zones through the ISPS code had led port owners, primarily through their management teams, to re-focus their energies on ensuring their identification processes evolved. The role of biometrics, something not required by regulators, was in particular the subject of debate with concerns held by port workers specifically. One of the most significant concerns highlighted by trade union representatives centred on the extent to which biometric identification cards required widespread criminal records checks on staff, and if so, to what extent any past criminal records could be utilised to question that

---

112 Ibid., p. 7. Also see Home Office, ‘Securing the Border’, p. 16.

individual’s trustworthiness. As one trade union representative noted, past offences did not necessarily have anything to do with security.\textsuperscript{114}

Despite these concerns, a sense of inevitability was expressed by those representatives that the issue of biometrics would stay on the agenda as the need for increased checks in ports, because of the presented terrorist threat, remained. While those whose job it was to represent port workers were uncomfortable about possible elements of the response, it remained the case that the presented threat was both acknowledged and accepted. This situation was further alluded to by another trade union representative who acknowledged how in the aftermath of the London 2005 terrorist attacks it had been easier to resist the need for biometric ID cards on practical (they won’t work) rather than security grounds, illustrating again the way in which securitisation shapes and squeezes the space for reflection and resistance.\textsuperscript{115}

As in preceding years, it was the Port of Felixstowe that utilised technology most visibly in its operations. In 2006 they introduced an identification system for those road hauliers using the port called the Road Haulier IDEntification System (RHIDES) which utilised an ID card with biometrics. The system was outlined on its accompanying website:

On arrival at the Port, the driver places the card into a reader and their hand on a biometric scanner. If a valid card is presented, the Port's gate control system

\textsuperscript{114} Author’s interview with number 4, 1 April 2009.

\textsuperscript{115} Author’s interview with number 13, 23 April 2010.
records the number against the container/s and allows the driver to enter the 'Restricted Area' of the Terminal.\textsuperscript{116}

The utilisation of biometrics, even though this was not a national requirement, was defended on the grounds of pursuing a greater level of security. The port introduced a ‘no card; no container’ policy from 1 March 2007 and in following years further increased its demands on hauliers. One example was its decision not to allow ‘orphan’ hauliers (those not linked to a recognised company) to utilise the port.\textsuperscript{117} This particular change illustrates how the move towards encouraging accredited status within the supply-chain more widely was replicated and implemented in an individual port, sold as speeding up operations and enhancing security.\textsuperscript{118}

The implementation of the RHIDES system with its ability to grant or deny access to particular areas of maritime infrastructure, coupled with the way in which increasing amounts of traveller data was collected and put through databases with certain individuals highlighted for further investigation in e-Borders, demonstrated the prominence of the use of technology. Yet these examples also illustrated a shift in which technology was utilised by members of the policy network away from simply facilitating implementation, aiding their day-to-day operations by say, allowing them to maintain a list of ISPS code compliant port facilities, and more towards a situation

\textsuperscript{116} Information taken from the Road Haulier Identification System (RHIDES) website, accessed 22 November 2010, \url{http://www.rhides.com}.

\textsuperscript{117} RHIDES website.

\textsuperscript{118} There was also a Vehicle Booking System (VBS) in the port, which required hauliers to book a delivery slot in advance. See Vehicle Booking System website, accessed 21 November 2010, \url{http://www.portoffelixstowe.co.uk/vbs/}. 
where technology occupied an ever more central place in the response, even leading
counter-terrorism efforts with human engagement actually reduced.\textsuperscript{119}

The introduction of technology as advanced as RHIDES also served as a reminder
that the security practices undertaken in and around UK maritime infrastructure did
in part depend on the scale of operations in a port and the ability and willingness of
port operators to meet costs. As one interviewee acknowledged, while other ports
took security seriously “there is a limit to what they can actually do, whilst trying to
maintain a business”. Beyond this the importance to a port operator of its ports
reputation was also raised as partial justification for their use of technology to
enhance security. “There is obviously going to be an element of ‘we don’t want it
happening on our patch’”.\textsuperscript{120} Both these points remind us that while security
remained of the highest priority, members of the policy network continued to
recognise and emphasise a desire to strike a balance between security and
commercial operations. One port manager emphasised that “the two things are not
incompatible” noting:

You can always create new risks but it goes back to why we do it and what we
are doing here. The risks and the operational requirements have to be together –
so security and trade facilitation in my mind is the same thing; just two ends of
the same see-saw. If you can make your supply chain more secure, it improves
operations. If you can make your operations better then generally it will improve
security. If the operation is slicker there is less chance anyone doing anything
bad to it.\textsuperscript{121}

\textsuperscript{119} For a further discussion of the role information technology systems play in relation to security see Michael

\textsuperscript{120} Author’s interviews with number 1, 19 March 2009 and number 7, 18 March 2009.

\textsuperscript{121} Author’s interviews with number 11, 3 March 2010.
In relation to spending on security in this period there continued to be a process of review over the level of costs incurred in maintaining the existing counter-terrorism security response. For example, the European Commission published a report in 2006 on transport security and its financing that provided a run-down of average security costs within the EU. It found that average investment costs for port facilities were 464,000 Euros, with average annual running costs at 234,000 Euros. It also acknowledged a substantial difference between an average investment of 798,000 Euros for multi-purpose facilities and 79,000 Euros for container facilities. The report explained that most costs were met directly or indirectly by the ports themselves within the EU, yet the Commission expressed its concern that outside the EU substantial state subsidies to port operators risked undermining competition, thus distorting the market. Similar concerns were also raised by some within the UK, particularly during the review process after the London 2005 terrorist attacks. The long-standing ‘user pays’ principle remained firmly in place however.

(4.4.3) Working practices:

With regards to working practices within UK maritime infrastructure in this period, it was more a case of evolution on, rather than any significant reversal away from,

---


previous developments. The emphasis continued to be placed by members of the policy network right along the policy chain on ensuring universal compliance with emergency measures, and an improvement in security by building additional security awareness and enhancing training. For example, a number of additional guidelines and training manuals for those working in maritime infrastructure security were published. Embracing different forms of communication, TRANSEC produced the first of two training DVDs in 2007 to outline its core advice on port security. These were provided to the author during the course of conducting research. The DVD’s intended audience went beyond those with direct security responsibilities and included all types of staff who worked within UK maritime infrastructure. ‘Safe Harbours: Port Security and You’ talked viewers through the ISPS code security levels, advised them to report damage to infrastructure, suspicious behaviour and offered a range of similar practical advice.\textsuperscript{125}

The messages reproduced in the DVD were very familiar. In its introductory section the narrator describes the size of the UK maritime industry noting how British ports deal with over 600 million tonnes of freight and 67 million passengers per year. In doing this the DVD emphasises the economic significance of the industry, a point made more explicitly when the narrator notes that “in the years ahead UK ports will play a vital role in both the economy and security of our nation. And it is up to all of us to help ensure that every British port continues to be a safe harbour.”\textsuperscript{126} The DVD then moves on to discuss, using imagery as it does so, a series of examples of

\textsuperscript{125} Department for Transport, ‘Safe Harbours: Port Security and You’, produced by Vision Productions, 2007. Many thanks to the interviewee who provided me with both DVDs.

\textsuperscript{126} Department for Transport, ‘Safe Harbours: Port Security and You’, at approximately 1 minute, 45 seconds.
terrorist attacks on shipping such as the attacks on the USS Cole and French tanker Limburg. To widen out this sense of threat the terrorist attacks in the US, Madrid and London are all also highlighted. The DVD then both reproduces the target narrative, whilst illustrating the way in which the presented threat relating to maritime infrastructure was in a mutually reinforcing relationship with the macrosecuritisation, when the narrator notes that “the attacks in Madrid and London prove that all types of transport, including the maritime sector, are potential terrorist targets”. 127

The overall result, as the DVD continually emphasises, is the need to maintain constant vigilance and no complacency with regards to this presented threat. The DVD’s accompanying ‘notes for trainers’ document emphasises “the more vigilant all staff are, the less opportunity there will be for terrorists to find a loophole in security.” 128 An actor playing a PFSO tells the viewer, “I need your help because security awareness is everyone’s responsibility”, 129 demonstrating the way in which the continued institutionalisation of the counter-terrorism security response was sought through greater security awareness. Towards the conclusion of the DVD the PFSO gives a warning about complacency commenting, “do you know my biggest worry about security? Complacency. This port can operate for months, even years

127 Ibid., at approximately 3 minutes, 10 seconds.

128 Department for Transport, ‘Safe Harbours: Port Security and You (Note for Trainers)’, paragraph 3.

129 Department for Transport, ‘Safe Harbours: Port Security and You’, at approximately 5 minutes, 8 seconds.
with no security incidents and what happens? We can start losing out edge.”

The DVD then provided a further mechanism for the presented threat to be reiterated.

Alongside TRANSEC publications, in 2006 MI5 also published public guidance for those with some interaction with critical national infrastructure entitled ‘Protecting Against Terrorism’.

It included advice on how best to assess threats and build a security culture within organisations. This publication was directed at a slightly wider pool of individuals than the TRANSEC DVD, particularly as it was more widely available. The need to increase the security awareness of those individuals who entered the maritime environment on a more sporadic basis was also acknowledged. The International Maritime Contractors Association published their own pamphlet outlining the core components of the ISPS code and the requirements it placed on its members.

A trend emerged where increasing numbers of individuals who did not have the maintenance of security as their primary responsibility, as security professionals did, were nevertheless deemed to require some form of security awareness to help secure maritime infrastructure. This was a trend that was increasingly prominent in later years.

---

130 Ibid., at approximately 11 minutes, 40 seconds.


The publications also illustrated a move towards actively sharing best practice within the industry, a further mechanism utilised to improve security standards. The Nautical Institute, for example, published a book entitled ‘Maritime Security’, which amongst other things provided guidance on how to most effectively design security systems within the maritime environment. Here it included such advice as placing the “strongest barrier closest to target” and the “earliest warning furthest from target”. In the UK specifically, best practice tended to be shared both within and between agencies through discussion forums born out of strategies such as the PNMSS. Hutchison Port Holdings which owned and operated Felixstowe also actively shared best practice within the company itself. This transfer of security knowledge also rested on members of the policy network building relationships with each other over time.

This emphasis on agency was widely acknowledged during site visits and interviews as playing an important role in the counter-terrorism security response. Enhancing co-ordination between SB ports officers and customs officials for example was a regular occurrence in UK maritime infrastructure, yet in one case it became more than about attendance at joint meetings and instead involved the embedding, long-term, of ports officers inside a customs building. The objective was to ensure lines of communication were far more direct and that each could share more specific information with the other. For one of those involved in this initiative success was described as being the point at which “we attend each other’s social functions”, in so


134 Information ascertained during an interview.
far as this would prove that different organisational cultural barriers had broken down. In this case it was an objective met. Despite the embedding of SB officers in customs buildings, however, the situation noted in the previous chapter, that strategic security decision-making within UK maritime infrastructure rested with a relatively small pool of individuals, did not fundamentally change.

On similar lines, a clear hierarchy in terms of who led on security decision-making was apparent across the three UK cases studied. At one port, a private security manager acknowledged that while his team provided information they thought might be useful to SB ports officers, he had no expectation that they would then get back to him and provide any form of update on that information’s value. Here the information sharing process was both informal and unidirectional. It was a situation largely explained by the varied responsibilities held by different security professionals alongside the amount of information to which they had access. The sense of being something of an outsider in terms of security knowledge was implicitly noted by one trade union representative. Although he felt the terrorist threat did occasionally get blown out of proportion, he added a disclaimer to his comments noting “that perhaps is something coming from an uneducated view. The Security Services may say we are being overrun or are quite good at keeping them under wraps”.

135 Author’s interview with number 2, 28 July 2009.

136 Author’s interview with number 10, 24 March 2010.

137 Author’s interview with number 14, 9 December 2009.
(4.5) Conclusion:

The developments witnessed in this period demonstrate an underlying complexity to securitisation that on initial examination is not always readily apparent. Both the macrosecuritisation of the ‘civilised way of life’ and the securitisation of UK maritime infrastructure remained stable, yet a number of additional insights about the process become clearer with two further years of discourse and practice having been examined. In terms of how UK maritime infrastructure was specifically securitised in the context of responses to international terrorism, the chapter has further illustrated the way in which the stability of securitisation cannot be assessed by examining the specific terminology deployed in isolation. Political leaders, parliamentarians and security professionals in the UK were more willing to publicly demonstrate their dislike for the terminology of ‘war’ and the appropriateness of a militaristic response, but the idea that international terrorism threatened the civilised way of life, which most crucially underpinned the ‘war on terror’ discourse, continued to be emphasised and facilitate policy.

For those interested in the securitisation of UK maritime infrastructure this is particularly relevant because it helps to explain the stability of the securitisation despite the focus of the policy network increasingly turning towards the security of the wider supply chain, transport network and UK border in this period. In emphasising the reiteration of specific ideas over the specific terminology deployed, it becomes possible to recognise the way in which the presentation of UK maritime infrastructure as both a potential target and vulnerable node in relation to
international terrorism endured. The presentation of the ideas may have been repackaged, but the ideas were reiterated nevertheless.

The way in which the security of UK maritime infrastructure was discussed within the context of these wider debates, launched in the aftermath of the London 2005 terrorist attacks, also illustrates once more the ability of particular events to shape the way in which the securitisation evolved. The Lloyd’s List editorial calling for continued vigilance and chastising those sceptics of the counter-terrorism security response, illustrated the way in which events could be utilised to reiterate the presentation of threats. It also became evident that many of the counter-terrorism practices witnessed in this period could be described as associative in the sense that they impacted on UK maritime infrastructure but were not necessarily designed with it as their focal point. The UK government’s e-Borders programme and the proposed introduction of an EU-wide 24-hr manifest are just two examples.

Additional insights in to reflection and resistance in relation to the securitisation can also be garnered. The previous chapter noted how reflection about the counter-terrorism security response was both natural and continual, that resistance emerged out of and subsequently shaped the direction of this reflection, that specific events influenced proceedings, and that ultimately resistance took different forms. In these two years the policy network continued to highlight new dimensions to the presented threat, specifically to small ports and harbours, yet there was also more explicit acknowledgement of nuance relating to that threat. The view expressed by members of the policy network that not all forms of transport could or should be treated in the
same way with regards to security, suggests that whilst there remained acceptance that international terrorism posed a threat, members of the policy network were perfectly willing to recognise a hierarchy in terms of likelihood of an attack. There was then a form of ordering taking place, where the presented threat as a whole was dissected. This was effectively captured by the SB ports officer who acknowledged 75% of his working time was spent preventing terrorists from exploiting his port, with 25% focused on ensuring the port was not attacked itself.

The added complexity to the securitisation of UK maritime infrastructure was also evident in the way in which certain acts of resistance did bring about change. The developments in this two year period illustrate how resistance can at times be successful, even if this success should be regarded as limited. More specifically resistance was seen in the way in which particular elements of the counter-terrorism security response could be challenged, bringing about change in practice. Securitisation does restrict the parameters of debate, a situation acutely illustrated in the TU representative’s acknowledgement that biometric ID cards could only be successfully resisted in his port on the grounds of practicalities (they wouldn’t work) rather than on the grounds of security (there was no threat). Yet securitisation did not eradicate all the space for discussion, for contestation and negotiation over the content and delivery of emergency measures took place and could be heated. The ultimately successful resistance to the UK proposal to extend pre-charge detention to 90 days and to US Congressional plans to require all containers bound for the US to be scanned for CBRN materials illustrates this. These examples provide evidence to show how the implementation of emergency measures is by no means smooth.
Despite this, it would be unwise to overplay the significance of these successful acts of resistance. Resisting individual emergency measures may ultimately prove to be a successful strategy for those interested in desecuritisation – by hoping that a tipping point is reached whereby it becomes widely accepted that the problem is not so much the measures initiated but the ideas that facilitate them – but there is no evidence to suggest this had taken place here. As it has already been noted in this conclusion, the idea that international terrorism posed a threat to UK maritime infrastructure, wrapped up in the macrosecuritisation of the ‘civilised way of life’, remained both salient and understood, two central facilitating conditions for securitisation according to the Copenhagen School. When one considers that the UK pre-charge detention period was still extended to 28 days and that a trial of 100% container scanning was initiated, it is clear what was regarded as accepted practice had again shifted. As a result, at most it seems accurate to suggest that developments in this period do little more than confirm that while securitisation has a general result, the politics of emergency, the specific nature of that emergency may vary.

Shifting focus to the impact of continued securitisation on the management of UK maritime infrastructure a number of points are worthy of elaboration. Further enhancing co-ordination between members of the policy network remained a priority, most clearly demonstrated in the development and launch of the PNMSS. This strategy illustrated again the ‘central framing and localised delivery’ model pursued in relation to counter-terrorism and the desire from the policy network to institutionalise further the existing counter-terrorism response particularly by creating mechanisms to share best practice. There remained difficulties which suggested that securitisation did not completely remove long-standing problems
associated with co-ordination between different parties. The hierarchy within the policy network, captured in the way in which particular actors had access to wider pools of information, was further demonstrated in the largely unidirectional nature of the way in which information was felt to flow between private security personnel and SB ports officers in one port. There was also acknowledgement of the limitations of enhancing co-ordination through structural means alone, with an emphasis on building relationships displayed. Collectively these two examples show once again the diverse means utilised to secure UK maritime infrastructure.

One of those means was the use of technology, a feature of the counter-terrorism security response which was first highlighted in the previous chapter, and which was particularly evident in this period. Through initiatives such as e-Borders and RHIDES, it was clear that technology was understood to have a substantial role in enhancing security by members of the policy network. One commonality between RHIDES, established on the ground in Felixstowe, and e-Borders, established more widely across the UK, was that each served as a mechanism through which information on the movement of both people and goods could be collected and analysed. This represented an effort to accumulate knowledge about UK maritime infrastructure and was an additional way in which increased power relating to that infrastructure could be gained. In short, learning more about the activities taking place within UK maritime infrastructure was a way in which both the British state and port owners in particular could gain control. This accumulation of knowledge then sat alongside an investment in material capabilities – in other infrastructure such as fencing and in security personnel – also pursued in to order increase power relating to maritime infrastructure, which is how a number of developments
witnessed in the previous chapter can now be understood. Here the use of fencing to
demarcate restricted zones and specially trained staff meant that behaviour within
maritime infrastructure could, to an increasing extent, be managed and desirable
actions emphasised. Technology of course could be utilised to serve this purpose too.

The main characteristics of the counter-terrorism security response then were very
much as had been suggested at the end of the previous chapter. The focus on
updating the SUA convention, the initiation of 100% scanning trials, the proposed
introduction of an EU 24-hr manifest rule and the launch of Regional Portal Groups
through the PNMSS, were just a few of the ways in which the policy network
displayed a willingness to add to the counter-terrorism security response. This of
course sat alongside efforts to further institutionalise existing emergency measures
such as the ISPS code through say, TRANSEC’s launch of new awareness DVDs.
The response then continued to evolve, while the new emergency measures
represented additional layers to it. It was however the increasingly expansive scope
of the counter-terrorism security response which was most clearly demonstrated.
Although the additional measures noted here meant that as before a growing range of
day-to-day activities within UK maritime infrastructure were framed by counter-
terrorism considerations, a spatial to dimension to the expansive scope was also
evident.

The introduction of the EU directive on port security in October 2005 was a concrete
sign of the way in which the policy network turned their attentions from focusing on
the security of the ship/port interface to the port as a whole. This had been the desire
of a number of members of the policy network in the early stages of the development of the ISPS code of course, captured in the 2004 IMO/ILO code of practice on port security. With the UK government’s emphasis on exporting borders, the space which was to be secured in relation to UK maritime infrastructure continued to grow. It was a trend fuelled by securitisation and the view that securing UK maritime infrastructure was a necessity in order to secure the ‘civilised way of life’. In presenting the threat posed by international terrorism as an existential one, weaknesses and gaps in security were understood to have potential consequences whereby life as it was known could end. As a result there was a desire to expand the space which was secured. This would make it more difficult for UK maritime infrastructure to be attacked or exploited by terrorists as threats could be intercepted earlier, the presented threat then was to be pushed further away.

The next chapter continues to shed light on the securitisation of UK maritime infrastructure as developments between 27 June 2007 and 30 June 2009 are examined. Representing the final part of the detailed case study, the chapter argues how, despite a change in political leadership in the UK, there remained no fundamental departure away from the pursuit of a ‘war on terror’ or the belief that UK maritime infrastructure itself was threatened by international terrorism. As attention turns to the impact of continued securitisation on the management of UK maritime infrastructure, the prominent features and main characteristics of the counter-terrorism security response set out thus far continue to be fleshed out. In particular the chapter illustrates further the spatial dimension to securitisation as it charts the implementation of counter-terrorism initiatives designed to secure harbours, indeed the British coastline as a whole. In doing this the trend for a
growing number of non-security professionals, including members of the general public, to gain some responsibilities relating to, and awareness of UK maritime infrastructure security is also highlighted. The chapter concludes by highlighting how the pursuit of increased power by both the British state and port owners in particular in relation to UK maritime infrastructure, represents the thread which runs through the counter-terrorism security response. Security and power here were intertwined.
Chapter Five

Staying the course: securing UK maritime infrastructure after Blair

As the threats we face are changing rapidly, we can never assume that the established way of doing things will be enough. We will always make the necessary changes, whether through greater investment, changes to our laws or reforms to the way we do things, to ensure that Britain is protected.\(^\text{138}\)

(Gordon Brown, Prime Minister United Kingdom, 22 March 2009.)

(5.1) Introduction:

The previous chapter demonstrated how the 2005 terrorist attacks in London helped to renew the macrosecuritisation of the ‘civilised way of life’ ensuring once again that the wider environment in which UK maritime infrastructure had itself been securitised remained stable. In the following two years the focus of the counter-terrorism security response relating to that infrastructure had, in relative terms, moved away from the emphasis on further institutionalising the existing response, specifically the ISPS code, and on to adding to the response where it was deemed appropriate. This strategic focus emerged in part because the existing response was deemed to be well institutionalised in the UK. Yet it also occurred because the London 2005 attacks had initiated a series of discussions relating to the security of

the UK border and transport network, alongside discussions internationally about the security of the wider supply chain, all of which maritime infrastructure could said to be part. Despite this shift in focus, the broad trajectory of the response demonstrated considerable continuity with previous time periods. Its features, the discussions accompanying implementation and the main characteristics of the response remained consistent. More specifically the use of technology to enhance security continued to grow, the role of agency in enhancing co-ordination was highlighted and the desire to extend the zone of security outwards noted.

This chapter examines developments in the period between 27 June 2007 and 30 June 2009. It argues that despite a change in political leadership at the very top of government in the UK as Gordon Brown became Prime Minister, there was very little change in the reiteration and subsequent acceptance of the macrosecuritisation. Whilst the terminology of the ‘war on terror’ continued to be jettisoned, a combination of personal political history, the collective impact of previous trends in both discourse and practice, combined with terrorist attacks in the UK within days of Brown coming in to office, ensured the policy environment was not conducive to wholesale change. This stability ensured UK maritime infrastructure remained securitised. The idea then that there was a terrorist threat relating to UK maritime infrastructure, bound up in the presentation of an existential threat to the ‘civilised way of life’, which in turn meant counter-terrorism practices were deemed to be a necessity, continued to be reiterated and accepted. In terms of the counter-terrorism security response itself, implementing those elements of the response that had been initiated in previous years was given the greatest prominence.
To elaborate this situation the way in which the macrosecuritisation was reiterated in this period is first elaborated. Here attention falls on demonstrating how the terrorist attacks in London and Glasgow during the summer of 2007 created the space in which the presented threat could be reiterated. Evidence of resistance to the macrosecuritisation is once again acknowledged, as with previous periods the chapter argues it remained largely directed at particular counter-terrorism practices rather than the idea of an existential terrorist threat. The resistance still brought about changes in terms of individual policies, but ultimately the prominent position counter-terrorism efforts held remained unchanged. In terms of the securitisation of UK maritime infrastructure specifically, the reproduction of the ‘target’ and ‘vulnerable node’ narratives still largely took place during wider reflection over the security of the wider supply chain, transport network and UK border. Here again the perceived weaknesses and gaps in the existing counter-terrorism security response were highlighted to be addressed, whilst locating new dimensions to the presented threat continued. The terrorist attacks in Mumbai in late 2008 had a particular impact as their maritime dimension was emphasised as evidence of the vulnerabilities of small ports, harbours, the coastline as a whole.

By sub-dividing the totality of counter-terrorism practice in to three constituent parts and utilising activities in and around the ports of Felixstowe, Holyhead and Tilbury once more, the chapter continues to reorient emphasis towards the ‘post-securitised environment’ illustrating the substantial impact of securitisation on the management of UK maritime infrastructure. The chapter highlights how whilst there was no evidence of significant budget cuts in relation to counter-terrorism in this period, international financial problems and recession in the UK began to place the issue of
funding firmly on the agenda. The result was that the attentions of members of the policy network increasingly fell on preparing for a potentially tighter financial settlement ahead. Alongside this, a growth in the number of individuals in the maritime environment with some responsibilities relating to, and awareness of UK maritime infrastructure security became increasingly evident. The chapter explains how members of the general public increasingly found themselves encouraged to take a more proactive role in helping to secure UK maritime infrastructure by, say, looking out for and reporting possible hostile reconnaissance by terrorists in their locality. These initiatives also further demonstrated the spatial dimension to securitisation as the extension of the zone of security outwards sought to encapsulate harbours and the coastline as a whole. Taken alongside those efforts at securing the wider supply chain and UK border, the chapter concludes by suggesting that thread which ran through the counter-terrorism security response was the pursuit of increased power by both the British state and port owners in particular in relation to UK maritime infrastructure.

(5.2) New Prime Minister, little change – Gordon Brown and the ‘war on terror’:

In his opening address as Prime Minister, Gordon Brown sought to more broadly position himself as an agent of change. Outlining his intention to lead a government with “new priorities”, he moved to draw a line under the administration of his
predecessor Tony Blair who had left office with dismal poll ratings.\(^\text{139}\) Despite this emphasis, it quickly became clear that the change did not extend to include any fundamental departure at a governmental level in the UK, from the belief that international terrorism posed an existential threat to the ‘civilised way of life’ and that a Manichean battle between good and evil was ongoing. This macrosecuritisation captured in the ‘war on terror’ discourse continued to be reiterated by political leaders and reproduced more widely. Nevertheless the jettisoning of the terminology of ‘war’ highlighted in the previous chapter continued, Brown’s Foreign Secretary David Miliband argued in one newspaper column that the notion of a ‘war’ had been both “misleading and mistaken” as it gave, amongst other things, “the impression of a unified, transnational enemy”.\(^\text{140}\) Such a rejection of terminology was far from universal however with Brown himself penning a column entitled ‘We are about to take the war against terror to a new level’ in March 2009.\(^\text{141}\)


\(^{141}\) Gordon Brown, ‘We are about to take the War against Terror to a new level’.
This stability of the macrosecuritisation was not altogether surprising taking in to account Brown’s personal political history. As with a large proportion of his first cabinet, Brown had been ever present in the governments’ of Tony Blair and had supported military operations in Afghanistan, in Iraq and domestic counter-terrorism efforts as a whole. In short then while the individual in the top job had changed, it was still a Labour government and it remained wedded to the thinking associated with the macrosecuritisation. Within Brown’s opening address there was a reference to a need for “change to protect and extend the British way of life”, suggesting he had some concerns that British identity and values were being threatened. Alongside this, the cumulative impact of the years of previous reiteration of the macrosecuritisation through the ‘war on terror’ discourse, and the resulting implementation of a range of emergency measures - some of which have been outlined in the course of this case study thus far - cannot be discounted. The idea that international terrorism posed an existential threat had been firmly institutionalised through a range of practices, demonstrating once more the intertwined relationship between discourse and practice. Moving away from this construction of reality then was unlikely to be straightforward.

Alongside Brown’s personal political history and the implementation of counter-terrorism practices over previous years, the third reason which can help understand this stability is the consistently acknowledged role particular events play in creating the space in which further reiteration of the presented threat can take place. More

---


143 ‘In Full: Brown’s Speech’, BBC News Online.
specifically on 29 June 2007, within days of Brown taking office, two car bombs designed to be detonated remotely by mobile phone were left in central London. One was left outside a ‘Tiger Tiger’ nightclub and the other on a nearby street although neither detonated. The police were alerted to the car outside the club by a passing ambulance crew who had spotted fumes leaving the vehicle. The second car was noticed by local council parking staff who had reported a strong smell of petrol coming from the vehicle as they had towed it away for being illegally parked. The following day two men drove a Jeep Cherokee laden with petrol and gas canisters into the main terminal building at Glasgow Airport. This attack resulted in the death of the Jeep’s driver, a broken leg for one passerby who had stopped to help police tackle the attackers, and structural damage to the terminal building itself.144 On 1 August the government responded by temporarily raising the terrorist threat level to ‘critical’ meaning further attacks were regarded as imminent.145

Neither attack had the same impact in terms of deaths, injuries and physical destruction as the London 2005 terrorist attacks, nor had the same deeply emotional impact on the wider population, yet political leaders remained quick to revert to the familiar discourse. This reiteration, as has been argued previously in this case study, represented an acknowledgement on behalf of political leaders that the presented threat remained both salient and understood to an audience made up of those charged with counter-terrorism responsibilities in the UK and the general public. In a


statement to Parliament for example, a couple of days after the attacks, Home Secretary Jacqui Smith argued that “terrorism is a serious threat to us all. We must ensure that our resources, capability and legislation support our common endeavour to defend the shared values of this country from terror.”  

Brown himself declared that there was a need to engage in a campaign to win ‘hearts and minds’ stating:

it is about how we persuade people that our values, about the dignity of human life, about liberty, about our belief in fairness for all, that these are values that define Britain and those people that try to present Britain in another light, we have got to take them on.

There was solidarity within Europe too with the President of the European Parliament Hans-Gert Pöttering drawing attention to, amongst others, the UK attacks telling colleagues “terrorism is a direct assault on freedom, human rights and democracy. Terrorism is an attempt to destroy our values by blind force, values which unite us in the European Union and in our Member States.” The characteristics of the macrosecuritisation then were present. The threat was presented as particularly serious, while the response had to be suitably robust and engage everyone against the ‘other’, the ‘enemy’. As Brown told the BBC’s Andrew Marr,

---


“we are dealing with a terrorist threat, we know it is serious, we know it is long-term, such attacks as this can happen at any time.”

The result was that emphasis continued to fall on the need to ensure constant vigilance and no complacency with regards to the presented threat. Such calls were further energised because the attack in Glasgow had represented a departure from the prominent terrorist focus on London. The Welsh Secretary Peter Hain for example commented that, “people in Wales should not be complacent that attacks only happen in London.”

Beyond political leaders wider reiteration was evident. A South Wales Constabulary spokesman argued it was important not to “allow Wales to become a soft target”.

The Scotland on Sunday newspaper declared “our airports will never be the same again”, concluding “it is to be hoped that yesterday's attack is an isolated incident, but the reality is that we will have to deal with more in the future.”

Security ‘experts’ waded in discussing through the media how the airport attack were security chief’s “nightmare scenario”, how Scotland had been seen as an “easier target”, and considering “how will Al-Qaeda strike next?”

Such reiteration was not confined to June and July 2007. In March 2009 for example, the


151 Idem.


Home Secretary introduced the publication of an updated UK Counter-terrorism Strategy (CONTEST II) telling the House of Commons:


Counter-terrorism remained of the utmost priority, with further policy developments remaining the clearest sign of continued macrosecuritisation. Many of these developments built on previous practice as perceived gaps and weaknesses in the existing counter-terrorism security response were highlighted to be addressed. Specifically, the June 2007 terrorist attacks led to a review of the protective security arrangements for crowded places, transport infrastructure and critical national infrastructure as a whole.\footnote{The review was led by the Security and Counter-terrorism Minister Lord West. Gordon Brown, ‘National Security’, House of Commons, 25 July 2007, Hansard starting column 841, accessed 4 January 2011, \url{http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070725/debtext/70725-0004.htm}. The Home Secretary briefly summarised the findings in another statement a few months later, but emphasised that the full review could not be published for security reasons. See Jacqui Smith, ‘Statement on Protective Security’, House of Commons, 14 November 2007, Hansard Written Statement, accessed 4 January 2011, \url{http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm071114/wmstext/71114m0001.htm#07111429000008}.} The working background of the two men who attacked Glasgow Airport in the National Health Service (NHS) ignited a discussion over the level of security vetting carried out on staff in roles deemed to be of particular...
Returning to those prominent features of the response discussed previously in the case study, the government announced a further growth in spending on counter-terrorism in the pre-budget report in autumn 2007. Referencing previous terrorist attacks to help justify the increase, the Chancellor Alastair Darling noted how “the terrorist attacks in July 2005 and attacks since, remind us all of the constant threat to our security here in Britain and of the critical importance of our police and security services.”

Darling also announced the creation of a single budget for counter-terrorism to finance the work of the intelligence services, police and all government departments in the area. It would rise by £1 billion over three years to £3.5 billion by the financial year 2010/11. This figure remained unchanged despite global financial problems becoming increasingly prominent in 2008 and the subsequent recession in the UK between 2008 and 2009. This recession did result in growing discussions, particularly towards the end of the case study period in mid-2009, over the extent to which budgets would have to be cut when the existing financial settlement

---


concluded. Yet despite emerging references to a global financial ‘crisis’ in this period the single security budget was protected until the end of the 2010/11 financial year. Other policy developments further proved the stability of the macrosecuritisation. In terms of enhancing co-ordination between those responsible for counter-terrorism, further institutional changes were undertaken. In March 2007 for example the Office for Security and Counter-terrorism (OSCT) was created within the Home Office. It was designed to provide additional focus to counter-terrorism activities across government. The Centre for the Protection of Critical National Infrastructure (CPNI) was also established to “provide protective security advice to businesses and organisations across the national infrastructure.”

The government also announced in the autumn of 2007 its intention to launch a new United Kingdom Border Agency (UKBA), merging the Border and Immigration Agency (BIA), those sections of Her Majesty’s Revenues and Customs (HMRC) that dealt with port of entry functions and UK Visas.

---


The proliferation of legislation with some counter-terrorism implications also continued. The UK Borders Act, 2007, Criminal Justice and Immigration Act, 2008, and the Borders, Citizenship and Immigration Act, 2009 were introduced.\textsuperscript{163} It was the Counter-Terrorism Act, 2008 which was the government’s lead legislative response in the period. Amongst other things it returned to the controversial issue of pre-charge detention, as the government again sought to extend the period in which terrorist suspects could be detained.\textsuperscript{164} Preparing the ground for the move, the Home Office Minister Tony McNulty invoked the memory of previous terrorist attacks to make his case telling the Mirror newspaper:

As an extreme example, imagine two or three 9/11s. Imagine two 7/7s. Given the evidence we've got and the nature of plots so far disrupted, such scenarios aren't fanciful [...] We hope never to utilise this power [...] But given all we know, we need to take it for extreme circumstances.\textsuperscript{165}

This example further illustrates the way in which events created the space in which further reiteration of the presented threat took place. Despite prefacing his comments with an acknowledgement they were “an extreme example”, McNulty’s request that readers consider what not just another 9/11 or 7/7 would look like, but two or three of them, was designed to illustrate the sense of scale to the presented threat. The


reference to “the evidence we’ve got” without providing further details also maintained a veil of secrecy over proceedings and implied significant threat.\textsuperscript{166}

Unsurprisingly based on previous experience, the bill was the subject of resistance. In the House of Commons Shadow Home Secretary David Davis declared, “let me be crystal clear: there is not one shred of evidence for an extension beyond 28 days—full stop.”\textsuperscript{167} In June 2008, after the House of Commons had voted to allow pre-charge detention to be extended to 42 days in certain circumstances, Davis resigned as a MP.\textsuperscript{168} His expressed intention was to fight a by-election to shed greater light on the issue of civil liberties.\textsuperscript{169} The House of Lords ultimately rejected the 42 day proposal and the government decided not to take the issue any further. Instead they signalled an intention to prepare a draft bill that could be introduced at speed to introduce the provision in the future should the need arise.\textsuperscript{170} The bill as a whole became law in November 2008, eleven months after it had first been

\textsuperscript{166} The Home Secretary opened the second reading of the bill by reminding Parliament and thus indirectly the British people of the threat posed by those who “wish to kill and maim and to undermine the values that we all share in this country”, describing the threat as “serious and urgent”. Jacqui Smith, ‘Counter-Terrorism Bill: Second Reading’, House of Commons, 1 April 2008, Hansard starting column 647, accessed 6 January 2011, \url{http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080401/debtext/80401-0007.htm#08040156000001}.

\textsuperscript{167} David Davis, ‘Counter-Terrorism bill: Second Reading’, Hansard column 659.

\textsuperscript{168} The government’s victory in the House of Commons was regarded as somewhat controversial because it was won with the last minute support of the Democratic Unionist Party’s MPs, whom it was alleged had managed to extract a variety of additional, but unrelated commitments from the government. See Andrew Porter, ‘Gordon Brown wins crucial 42 day vote thanks to Ulster MPs’, \textit{The Telegraph Online}, 11 June 2008, accessed 6 January 2011, \url{http://www.telegraph.co.uk/news/newstopics/politics/labour/2112553/Gordon-Brown-wins-crucial-42-day-vote-thanks-to-Ulster-MPs.html} and ‘Brown wins 42 day vote by a whisker’, \textit{The Sun Online}, 11 June 2008, accessed 6 January 2011, \url{http://www.thesun.co.uk/sol/homepage/news/article1280597.ece}.

\textsuperscript{169} David Davis resigned on 12 June 2008. See ‘David Davis resignation speech in full’, \textit{inthenews.co.uk}, 12 June 2008, accessed 6 January 2011, \url{http://www.inthenews.co.uk/infocus/features/in-focus/david-davis-resignation-speech-in-full-81227044.htm}. He was re-elected the following month with 72% of the vote but without facing either a Labour or Liberal Democrat candidate, see ‘Davis re-elected on reduced vote’, \textit{epolitix.com}, 10 July 2008, accessed 6 January 2011, \url{http://www.epolitix.com/latestnews/article-detail/newsarticle/davis-re-elected-on-reduced-vote/}.

published. This suggested that the government had not fully convinced parliamentarians that greater urgency was required on this occasion. This was not the only development against which resistance was witnessed. To name just two examples, parliamentarians argued that some of the airport security checks introduced in August 2006 were problematic, whilst wider anger continued to be expressed in Parliament over accusations that the UK government had been complicit in the process of extraordinary rendition.

As had been evident in previous years the resistance remained largely directed at particular counter-terrorism practices rather than at the idea that international terrorism posed an existential threat to the ‘civilised way of life’. This distinction was again made more explicitly in a contribution in the House of Commons, just as it had been by Mark Oaten in 2005. While opposition leader David Cameron outlined his concerns over pre-charge detention and other measures including the

---


ongoing ID cards scheme amongst others, he opened his remarks by asking the Prime Minister whether he agreed “that the threat we face from terrorism today is of a different order from the threats we faced in the past?” The debate over pre-charge detention was a passionate one, but in large part it rested on a divergence of opinion over the most appropriate means of preparing for a future terrorist attack not whether an attack would happen. For the government and its supporters legislating reserve powers offered the most prudent option, while for its opponents the use of existing emergency legislation like the Civil Contingencies Act was sufficient.

It was also questionable how successful the resistance was, David Davis’ resignation illustrated the way in which resistance against particular practices maintained an ability to seize attention, but it could also be seen as an acknowledgement of the overall failure of previous resistance to bring about fundamental change in policy trajectory. Moreover despite government concessions, the Counter-terrorism Act, 2008 still became law and in doing so it did, amongst other things, remove the prohibition on post-charge questioning in certain circumstances, introduced longer jail sentences for those convicted of terrorism-related acts and allowed some use of intercept evidence in criminal proceedings. The pace with which legislation was implemented may have slowed relative to that witnessed in previous years, yet seen

---


alongside legislation previously implemented the parameters of accepted practice had substantially changed. Such changes are difficult to imagine as have being possible without macrosecuritisation and the sense of necessity in terms of a response which comes with it.

(5.3) UK maritime infrastructure as a ‘site of securitisation’:

With the mutually reinforcing relationship between the macrosecuritisation and the securitisation of UK maritime infrastructure firmly established in this case study so far, the reproduction of the ‘target’ and ‘vulnerable node’ narratives in this wider context was not surprising. Both political leaders with some responsibility for the counter-terrorism security response relating to UK maritime infrastructure, and members of the policy network as a whole, continued to emphasise the serious nature of the threat posed by international terrorism and in doing so ensured the calls for constant vigilance and no complacency in relation to it were maintained.

Recognising once more the multi-levelled governance of UK maritime infrastructure, the public pronouncements of actors outside of the UK contributed towards framing the policy environment. Internationally the Secretary-General of the IMO continued to focus on the terrorist threat. At one conference for example he talked of the “iconic nature of the September 11 attacks” and reminded his audience that none were “left untouched by the causes or effects of terrorism in all its manifestations and definitions”. This continued memorialisation of past terrorist attacks anchored the Secretary-General’s subsequent discussion over the threat posed by piracy and the associated “potential for a seized ship to be used as a weapon against other
vessels or in port”, with previous moments of violence.\textsuperscript{176} Another senior IMO official embraced a similar discursive trajectory in a speech to a UN conference on effective border security. Reiterating the importance of safety and security at sea for social development and economic growth, he opened his speech by making reference to past attacks and describing the period as “the uncertain times which were inaugurated on 11 September 2001”.\textsuperscript{177} The Chief Executive of Shipping Australia Ltd Llew Russell reminded the transport and logistics industry that security had to be taken into account “at all levels and at all times”. Reiterating the notion of the terrorist threat being all-encompassing and timeless, Russell warned the industry of potential domestic dangers ahead stating:

I think they are forgetting [the threat] is potentially here in our own back yard. That’s what terrorists groups wait for. They’ve got plenty of time. It’s their timing and their agenda and they will wait for people to lose interest and that’s when they will start to become more active.\textsuperscript{178}

Representing further continuity with previous time periods the narratives continued to be reproduced as part of wider associated discussions on the security of the wider supply chain, transport network and UK border of which maritime infrastructure was regarded as part. One subtle difference however was that slightly less emphasis in relative terms was placed on maritime infrastructure’s role as part of the transport network and slightly more on the other two roles in this period. Undoubtedly this


was influenced by the terrorist attacks in the UK in June 2007. In particular there was the previously noted review in to protective security arrangements for critical national infrastructure led by Lord West. Yet there was also a Department of Transport review in to transport personnel security arrangements to help tackle any ‘insider threat’, and discussions over enhancing border security both before and after the creation of the UKBA.\textsuperscript{179} This reproduction was also clearly witnessed in the new CONTEST strategy where various strategic objectives and initiatives had links to maritime infrastructure.\textsuperscript{180} The idea of maritime infrastructure being a ‘target’ of terrorism, was most directly captured at the beginning of the ‘Protect’ section of the strategy which noted that:

\begin{quote}
The critical national infrastructure delivers essential services to the public. Damage to that infrastructure can have severe economic impact or cause large scale loss of life. Intelligence shows that terrorists are interested in attacking national infrastructure targets and recognise the potential impact those attacks can have.\textsuperscript{181}
\end{quote}

By emphasising that terrorists were interested in such attacks and highlighting the negative consequences a possible terrorist attack on critical national infrastructure could have on the wider way of life, the way the narratives drew upon the macrosecuritisation was again evident.

\begin{footnotes}


\textsuperscript{181} Ibid., p. 104.
\end{footnotes}
A second continuity was the way in which, through continual policy reflection, focus fell on discussing new dimensions to the presented terrorist threat and highlighting gaps and weaknesses in the existing counter-terrorism security response to be addressed. Internationally there was a growing emphasis in this period on drawing links between piracy and terrorism which served to further reinforce the sense that the backdrop in which policy was being implemented was particularly dangerous.\(^{182}\) Attention also fell on the threat terrorists could pose to energy terminals and vessels, or whether terrorists could pose as shipping agents to exploit accredited operator status initiatives. Linking back to previous discussions, whilst also demonstrating the way in which securitisation led members of the policy network to seemingly seek out threats around every corner, concern that the proposals for 100% scanning of containers would not prevent terrorists utilising other bulk carriers to transport people and weapons were also evident.\(^{183}\) On top of all this in the UK specifically concerns were also expressed over the security problems that may stem from inadequately completed ship manifests, as security professionals sought to undertake routine checks on who was travelling in and out of the UK.\(^{184}\)


\(^{184}\) Author’s interview with number 5, 31 March 2009 and associated site visits.
Ultimately it was concerns over the security of small vessels and those facilities which served them that remained dominant at all levels of governance. The IMO continued to research the issue, with reports and policy submissions emerging that reiterated the potential threats posed to pleasure craft, fishing vessels and others.\textsuperscript{185} In the US, one report by the Homeland Security Institute noted rather directly that:

Terrorists have demonstrated their interest in and ability to use transportation assets, including small vessels, to achieve their destructive aims. In the aftermath of the 9/11 attacks, the earlier attack on the USS COLE, and other maritime attacks around the world, the threat has clearly been demonstrated.\textsuperscript{186}

Terrorist attacks in Mumbai in November 2008 where the attackers entered the city by inflatable speedboats, placed further focus on small vessels and the security of the coastline as a whole.\textsuperscript{187} This demonstrated again the spatial dimension to securitisation, highlighted in the previous chapter, as threat perception and

\textsuperscript{185} For example, submission by the United Kingdom, ‘Correspondence group on security aspects of the operation of ships which do not fall within the scope of SOLAS chapter XI-2 and the ISPS Code (MSC83/4/2)’, Maritime Safety Committee, International Maritime Organization, 25 July 2007; Submission by Australia, ‘Security arrangements for ships which do not fall within the scope of SOLAS chapter XI-2 and the ISPS Code (MSC 83/4/4)’, Maritime Safety Committee, International Maritime Organization, 14 August 2007 and Submission by Japan, the United Kingdom and the United States, ‘Report of the Correspondence Group on security arrangements for vessels which do not fall within the scope of SOLAS chapter XI-2 and the ISPS Code (MSC 85/4/1)’, Maritime Safety Committee, International Maritime Organization, 22 August 2008. All accessed IMO Knowledge Centre 23-25 February 2010. In author’s interview with number 1, 19 March 2009, the interviewee noted that one of the UK’s quarterly police ‘Seaport Commanders Meetings’ was organised around the theme of small ports and harbours.


management was increasingly determined by efforts to extend the zone of security outwards.

The US Under-Secretary for Intelligence and Analysis at the Department of Homeland Security, Charles E. Allen told a US Senate Hearing in January 2009, “they [the terrorists] entered by water where security was the weakest. They thought they could greatly increase the likelihood of their success if they came by sea”.188 A Lloyd’s List editorial the following week struck a despondent note regarding maritime security generally concluding “as the events in Mumbai – saddening and sickening in equal measure – underline, the price of liberty really is eternal vigilance. Unfortunately at sea, even eternal vigilance just might not be enough”.189 In the UK the Mumbai attacks were utilised to highlight the evolving threat terrorist more generally by emphasising the way terrorists could deploy a “mixture of tactics combining ‘hit and run’ attacks with ‘seize and hold’ hostage taking.”190

Overall there continued to be limited resistance evident to the idea that there was a terrorist threat relating to maritime infrastructure which was bound up with the presented existential threat to the ‘civilised way of life’. Internationally the US proposal for 100% container scanning provoked some accusations that dimensions of the presented threat were being exaggerated. One newspaper columnist for example critiqued what he regarded as the short supply of common-sense displayed by US

---


legislators and noted how attendees at a World Customs Organization (WCO) conference had mocked the “notion that terrorists would have some kind of bomb in a box and then send it thousands of miles in the hope it would explode at the right time and in the right place”. The columnist questioned whether 100% scanning would be rolled out to land borders too, and quoted one delegate as having joked, “If I was a terrorist I would simply become Canadian or Mexican”. Yet most resistance to 100% scanning, as before, focused on the logistics of the plans and concern for trade competitiveness, serving as a reminder of the three balances that had also invoked much discussion in previous years.

Despite the lack of direct resistance there was further evidence of awareness of nuance amongst the policy network regarding the presented threat relating to UK maritime infrastructure, particularly in relation to those distinctions between threat perceptions around the aviation and maritime industry noted in the previous chapter. For example, after the June 2007 terrorist attacks, while some British ports were reported to have increased security checks, officially they remained at the lowest level one security status. This represented an acknowledgement from the regulator TRANSEC and those charged with setting threat levels in the UK that despite an


192 Idem.


attack on an airport, the threat posed in the maritime environment was not thought to have substantially increased.

(5.4) UK maritime infrastructure – the post-securitised environment:

With the discursive trends noted and the overall stability highlighted, emphasis once against shifts to examining practice in order to facilitate the process of shedding further light on the ‘post-securitised environment’. These sustained counter-terrorism developments remained the clearest sign of the securitisation of UK maritime infrastructure as a ‘site of securitisation’ as efforts to ‘secure’ the infrastructure from the presented threat continued. As in previous periods members of the policy network responsible for UK maritime infrastructure security reflected on the existing counter-terrorism security response, asking themselves what worked and what could come next. This led to discussions which, amongst others, focused on how prescriptive the response should be and the need to maintain the three balances between security and commercial activities, between security and liberty, and over who had what responsibilities in relation to the implementation of the response.

In terms of strategic focus, the trajectory located in the previous chapter whereby the policy network continued to focus on further institutionalising the existing response including the ISPS code remained in place. Yet as before the ISPS code continued to diminish in prominence, especially in the UK, relative to other changes.

---

195 In terms of further institutionalising the ISPS code, the IMO continued to review activities at the international level of governance. For example the IMO published ‘Revised Guidance to Masters, Companies and Duly Authorized Officers on the requirements relating to the submission of security-related information prior to the entry of a ship into port (MSC.1/Circ.1305)’, Maritime Safety Committee, International Maritime Organization, 9 June 2009, accessed IMO Knowledge Centre 23-25 February 2010. The purpose of these guidelines was to share best practice and push for greater uniformity between member states. A Lloyd’s List editorial in August 2008 also highlighted the concern of shipmasters internationally over security failures in ports, questioning whether the time had arrived for the code to be “properly audited, with a stronger emphasis on the shoreside component”. Insight and Opinion, ‘Not feeling more secure’, Lloyd’s List, 29 August 2008, p. 8, accessed IMO Knowledge Centre 23-25 February 2010.
Internationally then an IMO report for example suggested that there was a “gap in knowledge and understanding” within the maritime industry of the relationship between the code and other measures that had been implemented across the industry including the World Customs Organization’s (WCO) ‘SAFE Framework of Standards’. Concerns for seafarer rights remained evident, particularly as a rise in the incidents of piracy led to growing concerns over the hostile environment in which they had to work. Efforts to seek universal compliance and the harmonisation and improvement of security standards, were also pursued.

Yet the focus largely fell on fully implementing and then institutionalising elements of the response that had been initiated previously but had not necessarily come into force. There were also additions and adaptations made to the response where it was deemed appropriate. These developments, mirroring the discourse, still tended to emerge out of associated developments relating to the security of the wider supply chain, transport network and UK border. Overall then there was no significant reversal in terms of the broad trajectory of the response, although resistance against

---


198 During the course of this period the IMO discussed developing model legislation that could include amongst other things a framework for a “national inspection regime to ensure continued compliance by companies, ships, port facilities and RSO’s with national implementation requirements”. See submission by Austria et al., ‘Measures to enhance Maritime Security: Development of Model Legislation on Maritime Security (MSC 84/4/4)’, *Maritime Safety Committee, International Maritime Organization*, 5 March 2008, p. 3, accessed IMO Knowledge Centre 23-25 February 2010.
particular proposals such as 100% scanning was noticeable and continued to have some impact. In terms of the prominent features and main characteristics of the counter-terrorism security response, these remained as previously outlined. However, once again additional insights are located and discussed.

(5.4.1) Legislation and regulations:

In terms of legislation and regulations in relation to the ISPS code the EU introduced a new regulation ‘(EC) No. 324/2008’ setting out “revised procedures for conducting Commission inspections in the field of maritime security”\textsuperscript{199} The central objective of the regulation remained to ensure inspections were conducted in a “transparent, effective, harmonised and consistent manner”\textsuperscript{200} Attention also fell on ensuring that the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA) protocols agreed by the IMO in 2005 were ratified by contracting states. In late 2008 the UK government put forward tentative plans to do just that in the form of a Transport Security Bill, yet it ultimately failed to make it on to the parliamentary schedule\textsuperscript{201} The process of ratification was relatively slow as it was not until 28 July 2010 that the protocols formally came in to force, 90 days after the Republic of Nauru had become the 12\textsuperscript{th} state to ratify them\textsuperscript{202} This lapse in time between the


\textsuperscript{200} Idem.


protocols being agreed by IMO members, ratification and the date they formally came into force reminds us how the implementation of emergency measures is a continual and multi-staged process which although imbued with greater urgently, is not immune to problems, delays and on rare occasions the substantial adaptation, and even reversal of particular measures.

This complexity can be illustrated further by returning to those developments relating to the US proposal for 100% scanning of inbound containers. As the previous chapter elaborated, the 100% scanning proposal had provoked considerable resistance from both inside and outside the US after its emergence during the controversy over the DP World takeover. This resistance had highlighted again the international, inter-connected nature of the maritime industry and wider supply chain as the measures pursued by one, albeit greatly powerful state, required others to take note and consider their own practices. The legislative ping-pong that followed had resulted in the introduction of the Security and Accountability for Every (SAFE) Port Act, an act that had recognised the concept of 100% scanning but only introduced it on a limited and trial basis through the Secure Freight Initiative (SFI). In October 2007 the Port of Southampton was announced as one of the first members of this initiative.203 Yet after victory in the 2006 mid-terms, Congressional democrats placed the proposal back on the agenda and with greater success. In the summer of 2007 a requirement that 100% of inbound containers were scanned by 2012 was included in H.R 1 - Implementing Recommendations of the 9/11 Commission Act of

---

There was however some flexibility in that Section 1701, Chapter Four empowered the Homeland Security Secretary to delay implementation if a series of conditions were not met. A first 100 days initiative by Democrats, the bill was passed 371 votes to 40 in the House and 85 votes to 8 in the Senate in July 2007 and was signed into law by President Bush on 3 August 2007.

Unsurprisingly considering the resistance provoked in previous years, there continued to be concerns expressed in this period even as the SFI began and attention turned to preparing for 2012. In the UK the 100% scanning proposal was highlighted as an issue port managers had to be aware of, yet one manager expressed the feeling that the proposal may never fully materialise. Certainly the previous noted chapter of the Act to delay implementation gave some legitimate grounds for optimism on this front. It was also a position that was fuelled by an expectation that resistance was so widespread that it was going to be difficult to continue as was planned, and clear and ongoing concerns expressed by senior members of the Bush administration over the proposal. The US Homeland Security Secretary Michael Chertoff, for example, argued that the proposal represented a “20th century command-and-control”

204 ‘An Act To provide for the implementation of the Recommendations of the National Commission on Terrorist Attacks Upon the United States (H.R.1)’, 110th Congress of the United States, signed into law 3 August 2007, accessed 14 January 2011, http://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/. Specifically see ‘Title XVII Maritime Cargo’, Sec. 1701, paragraph 4 which states that the Secretary of Homeland Security may delay implementation of 100% scanning for two year, renewable periods beyond 1 July 2012 if, (4a) there is not suitable scanning equipment, (4b) if the equipment does not have a sufficiently low false alarm rate, (4c) if the equipment cannot be placed in a port due to physical restrictions, (4d) if equipment cannot be integrated with existing systems, (4e) if equipment will significantly impact trade capacity and flow of cargo, and (4f) if equipment does not adequately provide a notification of questionable or high-risk cargo. Military cargo was also exempted, with the Secretary having to keep Congress regularly updated of progress/extension requests, pp. 489-490.

205 In the House there were 22 members who either were not present or did not vote for the Act in its final form, while there were 7 Senators who either were not present or did not vote. For full details of the bill’s passage see ‘Implementing Recommendations of the 9/11 Commission Act of 2007 (H.R.1)’, govtrack.us, accessed 14 January 2010, http://www.govtrack.us/congress/bill.xpd?bill=h110-1.

206 Author’s interview with number 11, 3 March 2010.
approach to supply chain security that was in essence “a version of old Soviet-style heavy regulation”. His preference was to pursue a “21st century partnership approach” to locate where “the true danger lies”.

This was also a further illustration of the ongoing discussions taking place during implementation over how prescriptive the counter-terrorism security response should be. These discussions were similar to those discussions over the extent to which universal guidelines were necessary say, for Port Facility Security Officers (PFSO’s), that arose in the year after the ISPS code came in to force. Despite all this however it was reported that the port of Rotterdam had been preparing for 100% scanning, while the WCO raised concerns that Europe had not woken up to the possibility of the proposal coming to fruition. The WCO Secretary-General summed up the situation effectively, arguing “there is a big game of call my bluff going on and there will be winners and losers”. Ultimately the combination of delays in the ratification of the SUA protocols and the resistance and indecision surrounding 100% scanning can be regarded, metaphorically speaking, as bumps along the road of implementation. The continued focus on 100% scanning however further demonstrated the trend that those responsible for maritime infrastructure security internationally were interested in extending the zone of security outward,

---


208 Ibid., p. 7.


210 WCO Secretary-General Michel Danet quoted by Justin Stares, ‘Europe has not woken up to 100% scanning’.
where presented threats could be tackled further away from territorial borders and the infrastructure which could be attacked or exploited.

On similar lines the EU’s own 24-hour manifest rule continued to be developed, although the date it would become mandatory was postponed from 1 July 2009 to 1 January 2011 because of delays in ensuring the appropriate institutional structures and infrastructure were in place across the union. Another measure relating to the wider supply chain which was initiated previously – the Authorised Economic Operator (AEO) scheme – formally came into force on 1 January 2008. The AEO scheme was co-ordinated in the UK by HM Revenue and Customs and remained as originally conceptualised a voluntary scheme. A company gained AEO status in return for proving financially solvency, compliance with customs requirements, an ability to demonstrate satisfactory management systems and being “compliant in respect of security and safety standards”, all of which were confirmed through an audit. The status allowed consignments to be fast-tracked at border points, be


prioritised if required for examination and demanded a reduced set of consignment data to be submitted to the relevant authorities.\textsuperscript{214}

The status was sold as both enhancing security and as giving the recipient a commercial edge, an approach that directly played on the ongoing discussions over the need to maintain such a balance in the counter-terrorism security response. Yet while the emphasis on co-operating with business, the scheme was ultimately developed, delivered and maintained by the state and provided a further opportunity for more information on the movement of goods to be more centrally collected and held. Moreover despite membership being voluntary it provided another mechanism, like with security training generally, to manage behaviour by raising-up and here reward desirable behaviour. In doing so the extent to which membership would subsequently become a necessity, in order for a business to thrive, was highlighted.

\textit{(5.4.2) Institutional changes and infrastructure developments:}

In terms of institutional changes the most significant development was the launch of the UKBA on 1 April 2008.\textsuperscript{215} This ensured there was a new agency with which both SB ports officers and port personnel as a whole had to work with in relation to the counter-terrorism security response. As noted earlier in this chapter the UKBA was made up out of a merger between three existing organisations.\textsuperscript{216} Although its creation had been announced by Gordon Brown in the aftermath of the June 2007

\textsuperscript{214} Idem.


\textsuperscript{216} The new organisation had approximately 25,000 staff and an annual budget of £2 billion budget and was initially set up as a shadow agency under Home Office control. See Lord West of Spithead, ‘UK Border Agency’, House of Lords, 3 April 2008, Hansard Written Statement, accessed 14 January 2011, http://www.publications.parliament.uk/pa/ld200708/ldhansrd/text/80403-08040371000286.htm#08040371000286.
terrorist attacks, the idea of setting up a new unified border force in some form had been one long discussed in political circles. More specifically the new agency would be responsible “for securing the UK border and controlling migration in the UK”, managing “border control for the UK, enforcing immigration and customs regulations,” and considering “applications for permission to enter or stay in the UK, and for citizenship and asylum”. Its operations did then have a counter-terrorism function by monitoring the flow of both people and goods. Its officer’s powers remained as they were prior to the merger, although in the case of immigration officers these had already been increased through the ‘UK Borders Act, 2007’ to widen their ability, amongst other things, to detain individuals. There were however discussions as to whether they should increase further.

The justification for creating the new agency was most clearly elaborated in a Cabinet Office paper entitled ‘Security in a Global Hub: Establishing the UK’s new border arrangements’. Here references linked to the two main narratives that drew on the macrosecuritisation were evident. The paper noted how the UK’s “economic and social well being depends to a great extent on the effectiveness and smooth operation of our international links” and listed a series of threats being faced including “from organised crime and terrorism”. These threats were described as being “of an

---


unprecedented level of virulence, sophistication and variety”. \(^{221}\) Later the paper highlighted the all-encompassing, timeless nature of the presented threat acknowledging how “improvements in the UK’s ability to tackle terrorist plots, including through better border controls, will inevitably cause the terrorist threat to mutate”. \(^{222}\) Launching the UKBA then was by no means regarded as enough as a response on its own, the paper ruled out the immediate inclusion of SB ports police officers and ports police in to the new agency due to concerns over “accountability, tasking and independence” and because of a risk that “too large an organisation […] would simply replicate old divisions under a new umbrella”. \(^{223}\) It was not ruled out for the longer term however, and there was certainly a feeling expressed amongst those SB ports officers interviewed that such a new unified force could emerge in the future, particularly after the Olympics and in the event of the election of a Conservative government. \(^{224}\)

It was the Border Force component of the new agency with which other security professionals most commonly had dealings. \(^{225}\) To a large extent the changes brought about by the creation of UKBA on day-to-day activities was actually limited in so far as the agency was made up of a merger between three existing organisations, two of whom - the BIA and HMRC - had a long-standing presence in and around UK

\(^{221}\) Idem.

\(^{222}\) Ibid., p. 22.

\(^{223}\) Ibid., p. 71 and p. 14 respectively.

\(^{224}\) The Conservative Party, *A Border Protection Service for the UK*. Also see author’s interviewee with number 2, 28 July 2009 and author’s interview with number 1, 19 March 2009. It was also a feeling expressed in general, informal conversations during site visits.

maritime infrastructure. The internal process of standardising operational structures and officer terms and conditions remained ongoing after April 2008, and as such there continued to be a degree of separation in operational terms between the different components of the agency during this period. Linking back to the possible mechanisms of collaboration discussed in the previous chapter, relationships with the UKBA were reframed in order to meet the new institutional context. The Association of Chief Police Officers (ACPO) for example signed a Memorandum of Understanding (MoU) with the new agency to provide:

A framework for deeper collaboration between the new agency and ACPO at the border. It establishes a clear set of principles to strengthen the UK’s border through closer working. Critically, it provides strategic direction for intelligence sharing and delivery of frontline operations and supports the aims of the National Security Strategy in providing a platform for addressing and managing security challenges and underlying drivers, both immediately and in the longer term.226

The focus then remained on further enhancing co-ordinating between different members of the policy network, a feature of the counter-terrorism security response regularly highlighted in this case study. The very creation of the UKBA and the subsequent formal elaboration of how collaboration was to work between it and the police represented the continued emphasis on developing formal structures to achieve this end. This co-ordination did not always progress smoothly, as one interviewee noted there continued to be occasional lapses in communication between the different organisations and a tendency for each to defend their own turf and seek

---

maximum credit for operational successes to further justify their own roles.227 Again the importance of building and maintaining personal relationships remained of crucial importance particularly as the structural changes were being implemented. This took the form of something as simple as being invited to sit in on the meetings of partner agencies, in order to keep up to date with their operations and offer up opinions.228

Beyond the UKBA, the most notable institutional change was the creation of a single Welsh unit for counter-terrorism in which SB ports officers in North Wales, responsible for the Port of Holyhead, played a part. The Welsh Extremism and Counter-terrorism Unit (WECTU) formally began operations on 1 April 2008 and represented another example of the emphasis on centralised planning and localised delivery in policing that had been encapsulated in the regionalisation of Special Branch and the creation of portal regions to deliver the Police National Maritime Security Strategy (PNMSS).229 In terms of the portal region, North Wales had originally been placed in with North West England due to historic linkages in crime patterns, yet the desire for a unified approach across the principality, linked to wider moves towards devolution, ensured that an all-Wales group was subsequently set up.230 The creation of WECTU also illustrated the way in which security professionals often had to wear a number of different hats during the course of their

227 Author’s interview with number 5, 31 March 2009. Similar comments were made in author’s interview with number 9, 12 May 2010 and with number 4, 23 March 2010.

228 Such a meeting was attended in a strictly viewing capacity only by the author during the course of one site visit.


230 Information ascertained during an interview.
work recognising the different responsibilities placed on them. A SB ports officer in North Wales for example found themselves with UK-wide security responsibilities with regards to the UK border, pan-Wales responsibilities to ensure a unified national response, and responsibilities to the particular force which employed them.\footnote{Information ascertained during an interview.}

In terms of infrastructure the focus remained on ensuring the necessary technology was in place within UK maritime infrastructure both to meet existing security requirements and to facilitate the further extension of the zone of security outwards. Here the need for greater, possibly even 100\% scanning of containers ensured considerable emphasis was placed on developing solutions that could either balance such possible future security demands with commercial operations and/or illustrate alternative solutions to render such scanning unnecessary. Outside of the UK attention most prominently fell on the idea of developing ‘smart containers’ that could be electronically sealed to ensure greater security.\footnote{For example Janet Porter, ‘Europe leads box security research’, \textit{Lloyd’s List}, 22 August 2007, p. 4; Roger Hailey, ‘US urged to think ‘inside’ the box on container rules’, \textit{Lloyd’s List, Logged In}, 23 June 2008, p. 6; Roger Hailey, ‘Secure seals could offer US an alternative to scanning’, \textit{Lloyd’s List, Logged In}, 28 July 2008, p. 7 and ‘SecTrain bolsters box security’, \textit{Lloyd’s List}, 17 February 2009, p. 11. All accessed IMO Knowledge Centre 8-10 February 2010.} Members of the policy network in the UK were certainly aware of such technology with one port security manager acknowledging smart containers had been the subject of discussion at one of his port’s regular security committee meetings.\footnote{Author’s interview with number 7, 18 March 2009.} Although still in the early stages of development at least two possible devices which could monitor a variety of different threats to containers were reported in the maritime industry press. One developed by French company, Thales Research Technology, was amongst other
things “able to generate warnings, if for example, container doors are opened unexpectedly, there is a break-in through the side walls or roof, a deviation from the planned route, cargo tampering, or if the box has been moved into an unauthorised areas”.

It was envisaged regular data updates would be sent back to relevant authorities and alarms triggered if something untoward was detected.

Beyond the focus on developing solutions for the future, the roll-out of the UK government’s e-Borders programme continued. In late 2007 the Project Semaphore trial was declared a success and the government announced the next stage in the programme. A consortium of private businesses, Trusted Borders, was awarded a contract to provide the necessary technology. The intention remained that progressively data on an increasing number of passenger journeys was to be collected and analysed, while by March 2014 it was envisaged that full embarkation controls would have been reintroduced. However, just as with the US 100% scanning proposal implementation was not altogether smooth. The programme was critiqued as an example of how the balance between security and liberty had once again been lost. The UK-wide campaign group No2ID for example argued that “e-borders could easily stand for ‘Everywhere Borders’”, since it can collect data

---

234 Janet Porter, ‘Europe leads box security research’.
235 Idem.
everywhere and pass it anywhere. It is no longer a one-off check. It means a ‘papers, please’ Britain of mass surveillance, where ordinary citizens are tracked automatically.” 238 Within the maritime community the Royal Yachting Association (RYA) expressed some unease at the extent to which recreational boating could be included in the programme. 239 By the end of 2009 the intention was that e-Borders would “collect details of 60% of all international passenger and crew details from a range of carriers and to check that 60% against lists of people who are of interest to authorities”. 240

In terms of maintaining the existing counter-terrorism security response it became clearer as this period progressed that the global financial problems and recession in the UK had had some impact on the maritime industry as a whole. 241 More specifically financial problems were highlighted as the cause of DP World’s postponement of plans to develop a new deep-sea port (Thames Port) in the Thames Estuary, while the Port of Felixstowe also brought forward its long-standing plans to


239 See Gabrielle Garton Grimwood, ‘E-borders and Operation Semaphore’, pp. 13-14. Outside of the case study period concerns were also raised as to whether e-Borders was compatible with EU law, see Melanie Gower, ‘The e-Borders programme’, pp. 9-11.

240 UKBA website [National Archive version as at 8 April 2010], “Managing our border/Technology/E-Borders When will the changes take place?” quoted by Melanie Gower, ‘The e-Borders programme’, p. 5.

241 To get a general feel of the impact internationally see ‘Security Compensation’, Lloyd’s List, 27 February 2008, p.12, where it discusses the Spanish government providing financial support to its maritime industry to finance security operations. Also see Insight and Opinion, ‘The Need for Non-Doms’, Lloyd’s List, 20 April 2009, p. 2. It discusses the potential pitfalls of the UK government’s plans to tax non-doms on the maritime industry. While the IMO Secretary-General also acknowledged how “the unprecedented financial and economic crisis the world has been going through since the middle of last year has hardly left any sector, including shipping, unscathed”. Efthimios Mitropoulos, ‘Address by the Secretary-General (MSC 86-INF.18)’, Maritime Safety Committee, International Maritime Organization, 27 May 2009, p. 2. All accessed IMO Knowledge Centre 8-10 February 2010.
close its Landguard Terminal due to a downturn in container traffic.\textsuperscript{242} Felixstowe did however continue to develop a new south terminal to open in 2014 increasing trading capacity in the medium to long term.\textsuperscript{243} In terms of financial investment in UK maritime infrastructure security there were few overt signs that the financial problems resulted in investment being significantly cut either in terms of public or private security provision in this period.\textsuperscript{244} Investment in the police and intelligence services for counter-terrorism activities as a whole did, as noted earlier in this chapter, actually reached new highs in the 2007-10 financial period. Both Felixstowe and Tilbury maintained the bulk of their port police force strength. This was particularly relevant because both relied on the private port owners for their funding.\textsuperscript{245}

Towards the end of this period however just as political leaders were beginning to emphasise the need for future spending restraint and discussing efficiencies across government, members of the policy network relating to UK maritime infrastructure security were also increasingly aware that financial pressures were on the horizon. One SB ports officer noted that the “days money slushed around for counter-


\textsuperscript{243} Information provided during a site visit to Felixstowe. Also see ‘Future Development’, Port of Felixstowe website, accessed 15 January 2011, \url{http://www.portoffelixstowe.co.uk/PUBLICATIONS/JOURNAL/frmfuturedevelopment.aspx}.

\textsuperscript{244} One interviewee noted how the recession had meant more surveillance being conducted around his port for any incidents of theft. Author’s interview with number 7, 18 March 2009.

\textsuperscript{245} Idem.
terrorism two years ago has gone”, 246 while another alluded to the power of events in energising securitisations and subsequently influencing the counter-terrorism security response when he acknowledged he expected staff cuts unless there was a “big bang somewhere”, an event that required a heightened response. 247 Within the police as a whole this realisation combined with the ongoing focus on ‘Active Enhancement’ and collaborative working to enhance operational effectiveness, led to a continued emphasis being placed on sharing assets and even merging some departments across force areas. 248

Norfolk and Suffolk constabularies moved to co-ordinate operations more fully in the area of protective services which included SB functions. 249 A process was also initiated so that by spring 2009 the allocation of Designated Security Post (DSP) funding for SB ports officers – a grant to fund a particular number of counter-terrorism positions in each constabulary that was originally allocated by the Home Office - would be co-ordinated by the National Co-ordinator Ports Policing (NCPP) utilising an updated series of Key Performance Indicators (KPI’s). 250 These KPI’s sought to frame investment even more closely with an assessment of threat in a particular area, representing evolving scrutiny on counter-terrorism policing and

246 Author’s interview with number 4, 23 March 2010.

247 Author’s interview with number 5, 31 March 2009.

248 Author’s interview with number 1, 23 April 2010 commented, “if things remain unchanged in the way they are, I don’t foresee there being any more money becoming available over the years, so it is very much on a smarter way of working, the continued work we have started to do over the year looking at other partner assets, developing working relationships, building those networks and collaborative working between force areas.”

249 Information gathered during site visit. The end result of this collaboration can now be seen in the form of a Joint Assistant Chief Constable responsible for Protective Services across the area ACC Gary Kitching who began work on 1 April 2011. See ‘Joint ACC Gary Kitching’, Norfolk Constabulary website, accessed 25 July 2011, http://www.norfolk.police.uk/aboutus/ourpeople/jointaccgarykitching.aspx.

250 Discussed in author’s interviews with number 1, 23 April 2010 and with number 4, 23 March 2010.
bringing as one SB ports officer described it “professionalised transparency” to the financial process.²⁵¹

(5.4.3) Working practice:

With regards to working practices it continued to be a case of evolution on previous developments. There remained a focus on increasing compliance and harmonising security standards through building security awareness, introducing new training mechanisms, undertaking security drills and sharing best practice.²⁵² Alongside these the introduction of the new KPI’s to assess and then allocate DSP funding provided an additional mechanism to deliver such compliance and harmonisation. On a regular basis from spring 2009 SB ports officers were required to submit information centrally and be in a position to have that information audited.²⁵³ Although a number of those officers interviewed accepted the need for such indicators, some concerns were expressed in this initial phase of implementation. First, concerns focused on the relevance of the KPI’s to their operations, with a view put forward that the KPI’s were written with major airports in mind. Second, there was also some unease over how the central office – here the NCPP – would utilise that information in future funding allocations. Overall then the concerns centred on the extent to which the KPI’s could adequately capture the nuance involved in responding to the presented terrorist threat. The diversity in the size and type of infrastructure, the diversity in the range of counter-terrorism activities undertaken in and around that infrastructure and the way in which there was not a constant pace of work, but rather a burst of activity

²⁵¹ Author’s interview with number 4, 23 March 2010.


²⁵³ Author’s interviews with number 1, 23 April 2010 and number 4, 23 March 2010.
was always possible had to be considered.\textsuperscript{254} Ultimately the KPI’s did though evolve as the result of feedback from SB ports officers on what did and did not work. This demonstrated an element of flexibility on the part of NCPP that SB ports officers appreciated.\textsuperscript{255}

The use of KPI’s was by no means unique to ports policing, being a common practice across the maritime industry as a whole to ensure compliance and standards were continually assessed. For example, one port manager explained how was required by his superiors to submit information on a weekly basis in relation to his security staff’s most recent operations.\textsuperscript{256} Beyond KPI’s best practice continued to be shared between members of the policy network through forums such as the regular port security meetings and the portal group meetings encapsulated in the PNMSS. Here an internal portal group to portal group review mechanism was also designed whereby representatives from neighbouring groups visited each other to share best practice and assess progress in implementing the PNMSS.\textsuperscript{257} Such developments represented further concrete signs of the acceptance by members of the policy network of the need to maintain constant vigilance and no complacency with regards to the presented terrorist threat.

The emphasis on security drills also evolved to a point at which in one of the cases port managers eventually invited local constabulary representatives to deliver a

\textsuperscript{254} Author’s interview with number 5, 31 March 2009. These concerns were also expressed in a series of other informal conversations during site visits.

\textsuperscript{255} Author’s interviews with number 4, 23 March 2010 and number 5, 31 March 2009.

\textsuperscript{256} Author’s interview with number 11, 3 March 2010.

\textsuperscript{257} Author’s interviews with number 4, 23 March, 2010 and number 1, 23 April 2010.
scenario-building event known as Area Reinforcement Gained Using Scenarios (ARGUS).\textsuperscript{258} Here selected port staff were challenged over the course of half a day to discuss possible responses to a simulated suicide attack on the port. ARGUS had been rolled-out nationally and represented a concerted effort from the UK government, through the National Counter-Terrorism Security Office (NaCTSO), to educate and engage with particular personnel working in various crowded places, advising them both how to recognise the signs of hostile reconnaissance and deal with the aftermath of a terrorist attack.\textsuperscript{259} The macrosecuritisation of the ‘civilised way of life’ and securitisation of UK maritime infrastructure had already led to counter-terrorism considerations gaining a higher profile, occupying greater amounts of working hours and grabbing attention. Here then an accompanying feature of the counter-terrorism security response was that an increasing number of non-security professionals, individuals who did not have security responsibilities as their core job, gained some responsibilities relating to, and awareness of UK maritime infrastructure security. In the previous chapter this was seen in the informal security advice provided to outside contractors working within UK maritime infrastructure.

The idea that non-security professionals, in short members of the general public had a role to play in counter-terrorism was not of course unique to this time period or even the period from September 2001.\textsuperscript{260} Yet there remained a sense it was important to remind people of their responsibilities. As one police officer argued “to some

\textsuperscript{258} Author’s interviews with number 1, 19 March, 2009 and number 7, 18 March 2009.


\textsuperscript{260} The public were of course asked to remain vigilant and help the police with regards to terrorism relating to Northern Ireland.
extent we have forgotten some of the lessons of the IRA’s campaign261 and as such the need for businesses to have search strategies in place, say for suspect packages was essential. The focus on the public’s role in counter-terrorism gained momentum around the launch of ‘CONTEST II’ and in the aftermath of the Mumbai terrorist attacks.262 In the maritime environment it was most clearly encapsulated in the development and launch of a project called ‘Kraken’ in Suffolk.263 It encouraged those who worked or enjoyed the maritime environment “to be extra vigilant to counter the threat of terrorism”, and to report activity or behaviour that was deemed to be “suspicious and which may be connected with acts (or preparatory acts) of terrorism or serious crime”.264 Kraken was a further illustration of the way in which the zone of security was extended outwards, in this case from small ports, to harbours and even coastal communities in general. It also represented a clear example of the way in which best practice was shared having been initially created by the Police Service of Northern Ireland (PSNI), subsequently developed by Hampshire Constabulary and then placed in to the PNMSS as an example of an initiative worth implementing at a local level.265 In Wales Kraken would be launched in 2010 under a different branding of ‘Coast Watch’ but with nevertheless similar objectives.266

261 Author’s interview with number 6, 21 April 2010.


263 It was formally launched on 7 April 2009 at Suffolk Constabulary Headquarters, an event the author was kindly invited to.


265 Information ascertained during author interview.

266 Coast Watch in Wales was launched on 17 March 2010. An official launch video for Coast Watch can be viewed at, accessed 8 November 2010, http://www.youtube.com/watch?v=UFbrnisCK4o.
As part of the project the wider maritime community – including volunteer coastguards, harbour masters, private yacht club representatives, pleasure craft owners, and even members of the public living in coastal areas - were provided with a telephone hotline and on occasion an electronic submission system for providing information on suspicious behaviour and even possible hostile reconnaissance to the authorities. In return the police provided regular updates on security issues in the specific area. Taken alongside the organisation of ARGUS events, the public were not simply expected then to be passive receivers of information learning but were also asked to take on an increasingly proactive role in relation to implementation. They were to act not simply as the last line of defence against terrorist attack, should the state and its security professionals be unable to respond, but also as a first line of defence - locating, and reporting issues themselves.

Although one police officer was keen to stress the limits to this more engaged and proactive role emphasising:

it is about identifying, observing and reporting and recording. It is not about identifying and engaging and actually if they are concerned about stuff they shouldn’t be putting themselves in a position where they are confronting people.\textsuperscript{267}

These members of the public nevertheless seemed to occupy a grey area further blurring the traditional separation between security professional and public. They had more information than those not involved in the project and had a security role to play, but did not have the same extent of legal powers to accompany this role.

\textsuperscript{267}Author’s interview with number 4, 23 March 2010.
They were brought, albeit only partially and in a heavily managed way, into the working environment occupied by the security professional.\textsuperscript{268}

A continued focus on Suffolk Constabulary’s Project Kraken and to a lesser extent the Welsh Coast Watch initiative, also offers further insights in to how the emphasis on improving security awareness was pursued and highlights some of the complexities associated with this process. As in those efforts to further institutionalise the ISPS code, the police utilised presentations, leaflets and newsletters to outline the presented terrorist threat, set out the objectives of Kraken and the associated demands on members of the public. At the project launch invited members of the local maritime community including those listed earlier were informed of the “severe” threat posed by international terrorism to the UK and reminded how an insecure coastline could facilitate terrorism.\textsuperscript{269} This was a clear example of the ‘vulnerable node’ narrative being reproduced. The objective of Kraken was outlined as creating a more hostile environment in which terrorists had to operate, while the attendees were told to expect the unexpected. In one newsletter entitled ‘Op Kraken Requirements’, project members were informed that:

Vessels using Suffolk’s waterways should be alert for persons filming, photographing, drawing or loitering in areas of critical infrastructure. [...] Terrorist surveillance and reconnaissance of critical infrastructure is an integral

\textsuperscript{268} The separation highlighted here refers to the position in which serving police officers hold in relation to members of the public. Once sworn in as constables, that individual has additional responsibilities yet is also legally empowered, on receipt of a warrant card, to carry out that job by say, having the ability to detain and arrest individuals. It is also worth noting that outside of the case study period Suffolk Constabulary in partnership with certain maritime organisations worked to vet key staff whilst also drawing up information sharing protocols, enabling information of a more sensitive nature to be shared. The constabulary also initiated the process of arranging a license agreement through the Cabinet Office to enable certain maritime users to have greater access to more the secure TETRA communications system utilised by the Police and other emergency services. Information ascertained during an interview. Also see Paul Cornish, ‘The United Kingdom’, pp. 163-167 in Karin von Hippel (ed.), \textit{Europe Confronts Terrorism} (Houndmills, Basingstoke, Hampshire: New York: Palgrave Macmillan, 2005) and Nick Vaughan-Williams, ‘Borderwork beyond Inside/Outside? Frontex, the Citizen-Detective and the War on Terror’, \textit{Space and Polity}, 12:1 (2008), specifically pp. 68-76.

\textsuperscript{269} Project Kraken launch event, Suffolk Constabulary, 7 April 2009.
part of attack planning. Reports of any suspicious behaviour are essential in identifying potential criminal activity.\textsuperscript{270}

The sub-section of the newsletter concluded with a reminder of the importance of reporting information which was framed in expressions of concern over what currently could be being missed, “at this time, there is no way of knowing how many suspicious incidents go unreported”.\textsuperscript{271} Here then the all-encompassing nature of the presented threat was alluded to subsequently heightening the sense of danger.

Beyond these efforts at building awareness, update meetings were also organised to report on project progress and to enhance name recognition further institutionalising it by seeking to build a greater sense of project identity. As the first photograph shows there were even Kraken pin badges and stress balls manufactured and distributed to members and interested parties.\textsuperscript{272} The second photograph illustrates the Welsh Coast Watch branding through the catchphrase ‘Flag it up’ and the use of beer mats to ensure people were reminded to remain constantly vigilant even when having a drink.


\textsuperscript{271} Idem.

\textsuperscript{272} In NW England they also utilised waterproof kits so that project information could be taken out to sea. Information ascertained during a meeting attended.
Image 7 – Project Kraken paraphernalia.

Image 8 – Coast Watch branding.

273 Image 7 – “Project Kraken Paraphernalia,” image taken by author.

274 Image 8 – “Coast Watch Branding,” image taken by author.
The extent which those members of the public involved in projects such as ARGUS and Kraken fully accepted the rationale behind their creation is hard to fully assess. That said with Kraken in Suffolk the high level of turnout at both the launch and update events, the actual receipt of information through the hotline, and the comments made in interviews conducted suggested support was strong. In a small survey designed and distributed during the course of research in partnership with Suffolk Constabulary, this strong level of support was illustrated.\textsuperscript{275} 95.5\% of respondents agreed that the project was a “valuable crime and counter-terrorism strategy”, with a similar percentage, 95.4\% of respondents, accepting more generally that the public have an “important role to play in the fight against terrorism” with most suggesting this should involve serving as an additional pair of eyes and ears on the ground.\textsuperscript{276}

Some complexities did emerge however, further demonstrating the wider acknowledgement of nuance in relation to the presented terrorist threat highlighted during the course of this case study. While 86.4\% of those who responded said they either ‘strongly agree’ or ‘agree’ with the statement “the threat of terrorism against the United Kingdom has increased significantly since September 11th 2001”, and 54.5\% agreed to some extent with the statement “terrorism poses a significant risk to the maritime community in particular”, only 45.4\% agreed that “the current threat of terrorism to Suffolk is significant.”\textsuperscript{277} There was a level of uncertainty then over the extent to which a terrorist threat they felt was significant both nationally and in the

\textsuperscript{275} See Appendix B – ‘Project Kraken Survey’. The survey was designed by the author, checked by representatives from Suffolk Constabulary and then sent to all Project Kraken members in Suffolk as of April 2010. It achieved a 30\% reply rate.

\textsuperscript{276} Appendix B – ‘Project Kraken Survey 2010’.

\textsuperscript{277} Appendix B – ‘Project Kraken Survey 2010’.
maritime environment generally was wholly relevant to them. The idea that Suffolk was a sleepy county where terrorism was not particularly likely was something which was raised in a number of interviews with Suffolk police officers as an issue that they had to be aware of and actually challenge. In itself it also suggested that certain members of the public deconstructed the presented terrorist threat in to dimensions they deemed to be more and less likely.

It was also clear during the implementation of Kraken in Suffolk and Coast Watch in Wales that both SB ports officers and Home Office police officers were aware of how the use of the word ‘terrorism’ had the potential to invoke fear amongst the public with whom they wanted to engage and co-operate with. One SB ports officer acknowledged how “the T word frightens the shit out of people” noting his biggest fear was “raising fear of terrorism”. The idea that the word ‘terrorism’ could act as a barrier to the public getting involved did in part explain the decision for Kraken in Suffolk to eventually be branded a “crime and counter-terrorism strategy”, rather than as it was initially planned a “counter-terrorism vigilance strategy”. Hampshire Constabulary’s use of an image of an attacked oil tanker was also jettisoned as having little connection to the local area, as shown in the following photograph of one poster published.

---

278 Information ascertained in a series of interviews.
279 Information ascertained during interview conducted by the author.
280 Information ascertained during author interview.
281 Idem.
Despite this however there was also acceptance from these same officers of the way in which references to terrorism caught public attention most effectively. One SB ports officer suggested it was about the visual impact of terrorism, “the obvious impact worldwide of a terrorist incident seems to be self-evident compared to the invisible side of serious organised crime”. There was an acknowledgment then of the need to maintain a balance in terms of the use of particular terminology, attracting interest but not creating unnecessary fear. There was also acceptance of the need for flexibility in the message utilised. Another police officer noted how a colleague had argued at one community event that the reason why certain areas may not have been targeted is actually because people are vigilant, that security is

---

282 Image (9) – “Project Kraken Poster,” image taken by author. One contact telephone number removed by author for the purposes of anonymity.

283 Author’s interview with number 4, 1 April 2009.
Counter-terrorism successes then were presented as no excuse to let the guard down representing a form of self-perpetuating cycle.

(5.5) Conclusion:

This chapter has continued the process, undertaken right across the case study, to progressively shed light on the securitisation of UK maritime infrastructure in the context of responses to international terrorism. In addressing how specifically UK maritime infrastructure was securitised, despite the continued overall stability discursively, insights can again be noted. With five years of discourse and practice examined, taken alongside those trends highlighted in chapter two, the cumulative effects of securitisation were arguably clearer than at any previous time. The ‘war on terror’ discourse, the ‘target’ and ‘vulnerable node’ narratives, and large parts of the counter-terrorism security response relating to UK maritime infrastructure, had been firmly institutionalised. A specific apparatus of counter-terrorism was in place, an apparatus that’s form, even existence, rested upon the continued acceptance that international terrorism posed an existential threat to the ‘civilised way of life’. It was very much the norm to look at international terrorism and the response to it in a particular way. As a result the stability of securitisation did not rest on a particular set of actors reiterating the presented threat, it had a more autonomous form of resilience.

---

284 Author’s interview with number 1, 23 April 2010.
As in previous years particular events had had a notable impact on the evolution of the securitisation of UK maritime infrastructure. Just as the terrorist attacks at Glasgow airport were utilised to call attention to the possibility of terrorist strikes outside of the capital city, the Mumbai attacks fuelled concerns about the threat posed by terrorism along an entire coastline. Once again then focus continued to fall on highlighting perceived gaps and weaknesses in the existing counter-terrorism security response to be addressed. The calls for constant vigilance and no complacency remained evident, wrapped up for example in the reminders about how the events of 11 September 2001 had “changed the world” encapsulated in the statements of senior IMO officials. The way in which those events associated with the stability of the international financial system led members of the policy network to acknowledge and begin to plan for possible future counter-terrorism budget cuts, also alluded to how events with a more indirect connection to counter-terrorism could impact securitisation. Yet while efforts to manage economic problems undoubtedly rose in prominence in this period both internationally and within the UK, it was too early to say with any certainty what the relationship between these and the ‘war on terror’ would be.

Thinking about resistance to securitisation, developments in this period served to further emphasise the message of caution relayed in the previous chapter over the likelihood that successes at resisting individual emergency measures may ultimately bring about desecuritisation. Despite previous success at preventing pre-charge detention being extended to 90 days in 2005, the UK government’s renewed attempt to extend detention in 2008 illustrated the continued resilience of the macrosecuritisation. This was only emphasised further by David Davis’ resignation,
which as the chapter argued, can be seen as a move made from a position of relative weakness. This resilience was seen in relation to the securitisation of maritime infrastructure in the return of the US 100% scanning proposal that became law in 2007, and where large parts of the maritime industry internationally rested their hopes for a delay in implementation on the US Secretary for Homeland Security.

With regards to the impact of securitisation on the management of UK maritime infrastructure, the continual and multi-stage nature of the implementation of emergency measures was demonstrated in the way in which the policy network divided their time between putting the necessary systems in place to bring in to force previously agreed measures, sought to institutionalise further existing measures and developed new measures where they saw fit. In terms of the first work stream, focus fell on launching the EU 24-hr manifest and AEO schemes. The delay in launch date for the former scheme by two years illustrated again that implementation is not always smooth. Efforts to reform the EU ISPS code inspection regime and the introduction of KPI’s and peer review mechanisms through the PNMSS demonstrated the focus on further institutionalising existing measures. UK enquiries in to protective security arrangements, an update to the ‘CONTEST’ strategy and the launch of the UKBA showed how securitisation continued to facilitate new practice. The constantly evolving and layered characteristics to the counter-terrorism security response then remained evident.

It was however in relation to the increasingly expansive scope of the response where many of the insights emerged. Chapter three noted how the response was
increasingly expansive in the way in which a growing range of day-to-day activities relating to UK maritime infrastructure had been framed by counter-terrorism considerations. Chapter four meanwhile highlighted the way in which efforts to extend the zone of security outwards from say, the ship/port interface to the entire port, demonstrated the way in which the response was increasingly expansive spatially. Each was further illustrated by developments in this two year period.

In the case of the former, by encouraging members of the public from coastal communities to assist counter-terrorism efforts, serving as what can be described as informal security professionals, the growth in the number of individuals with some responsibilities relating to, and awareness of, security with regards to UK maritime infrastructure continued to expand. This sat alongside the growth in the number of private security personnel, general port staff, and outside contractors who, as it has already been noted, were encouraged to play their part in securing maritime infrastructure. Besides representing further confirmation of the way in which security activities had a higher profile, it also demonstrated the widespread and continued accepted of the presented threat. This was further emphasised in the results of the survey of members of project Kraken in Suffolk where a substantial majority agreed that terrorist posed a significant threat and that the general public had a role to play in counter-terrorism.

In the case of the latter - the spatial dimension to securitisation - project Kraken again proves to be helpful. The way in which the focus of the policy network turned to securing harbours and the coastline as a whole, represented a further expansion of
the space relating to UK maritime infrastructure which was deemed to require securing. The previous chapter argued that this expansion rested on the idea that the presented threat had to be pushed further away from UK maritime infrastructure to make it more difficult for it to be attacked or exploited by terrorists. What became increasingly evident however was the way in which such expansion was to an extent self-perpetuating. Resting on the acceptance that the threat posed by international terrorism is existential and that as such any security gaps may have unimaginable negative consequences, an increase in security in one place could result in an increase in threat elsewhere. This in turn demanded that the space secured be further expanded and so forth. This general trend for some counter-terrorism practices to require the implementation of additional counter-terrorism practices is neatly captured in the discussed UK Cabinet Office paper on border security which stated that improvements in border security would inevitably cause the terrorist threat to mutate.

Overall developments in this period demonstrate the way in which the pursuit of increased power by both the British state and port owners in particular in relation to UK maritime infrastructure was the thread that ran through the counter-terrorism security response. This pursuit for the British state continued through the activities of institutions such as TRANSEC and Special Branch, while for port owners it was through the activities of their senior management teams. The use of two main, interlinked mechanisms - investing in material capabilities and accumulating knowledge about UK maritime infrastructure - was again witnessed. By expanding the pool of individuals with some security responsibilities and awareness, through Kraken and ARGUS, the ability to manage behaviour within maritime infrastructure,
emphasising desirable actions was increased. Although membership of Kraken was of course voluntary, this did not diminish this process. Through the AEO scheme, which was also voluntary, particular behaviour was incentivised. The extent to which being outside of such initiatives was in some ways a disadvantage would be worthy of further investigation. In acting as additional pairs of ‘eyes and ears’ for the police, members of Kraken also facilitated the accumulation of knowledge about small ports, harbours, and the coastline around UK maritime infrastructure. Beyond people, technology also continued to be utilised both to accumulate knowledge and manage behaviour, as was illustrated in the next phase of roll-out of e-Borders and efforts to develop smart containers.

Over the course of this case study a wide range of trends both in terms of discourse and practice have been elaborated. A greater understanding of the securitisation of UK maritime infrastructure, specifically the post-securitised environment, has been garnered as a result. While each chapter has sought to build upon the previous, there remains a requirement to pull together findings from across the five year period that has been examined. In the overall conclusion to the thesis which follows three tasks will be undertaken. First a summary of how the thesis’ line of argument developed will be provided and a general conclusion drawn. This will further demonstrate how the case study’s structure has helped to facilitate the examination of securitisation. The conclusion will be elaborated through a summary of the thesis’ main findings with answers to the two core research questions - ‘How has UK maritime infrastructure been securitised in the context of responses to international terrorism?’ and ‘What has been the impact of post-2004 language on day-to-day security operations in that infrastructure?’ - provided. Finally, an effort will be made to look
beyond the thesis with some brief comments on possible future research avenues which stem from it.
Conclusion

Continuity and change: the securitisation of UK maritime infrastructure during the ‘war on terror’

(C.I) The thesis’ argument:

Across the thesis, the line of argument advanced has been that the United Kingdom’s (UK) maritime infrastructure was securitised in the context of the macrosecuritisation of the ‘civilised way of life’, which were in a mutually reinforcing relationship. This macrosecuritisation was captured within the ‘war on terror’ discourse of counter-terrorism. The impact of this securitisation on the management of UK maritime infrastructure was substantial with a counter-terrorism security response evident which can be characterised as constantly evolving, layered and increasingly expansive in scope and that had a series of prominent, recurring features. The thread which ran through this response was the pursuit of increased power in relation to UK maritime infrastructure undertaken by the British state and port owners in particular. Security and power in this case then were very much intertwined.

This line of argument developed over the course of the thesis with each chapter, specifically within the case study, building upon the last, by engaging with and
shedding further light on previously highlighted insights. The thesis’ starting premise was that the UK’s maritime infrastructure had been securitised in the context of responses to international terrorism. In short this meant that it was widely accepted that maritime infrastructure required securing against a presented terrorist threat, facilitating the implementation of a series of emergency measures. The thesis’ primary objective was to examine the impact of this securitisation on the management of UK maritime infrastructure in the five years between 1 July 2004 and 30 June 2009. This situation, first elaborated in the thesis’ introduction, meant that the thesis was at its heart a study about security. It was this focus which justified the use of the Copenhagen School’s securitisation theory as the analytical framework for the case study.

More specifically the use of securitisation theory rested on two assumptions. The first was that the theory’s conceptualisation of security as being socially constructed effectively captured the way in which particular and dominant understandings of the threat posed by international terrorism emerged after 11 September 2001. The second was that securitisation theory specifically offered a valuable set of insights, its emphasis on discursive construction and the politics of emergency in particular, that more fully captured developments relating to UK maritime infrastructure. These assumptions were defended in the first chapter by contextualising the theory within the wider security studies literature, elaborating its core components and evolution and through an engagement with a number of its critics. With the thesis’ primary objective in mind, the first chapter also made the case for reorienting research emphasis towards the ‘post-securitised environment’ and on to the implementation of emergency measures. In short greater focus was to be placed on what
securitisations ‘do’ in practice. An explanation of the specific parameters of the case study, the methods that were to be used and the sources utilised illustrated how this reorientation would take place.

In setting out the analytical framework through which the securitisation of UK maritime infrastructure was to be examined, the first chapter represented one half of a process of preparing for the case study. The second half of this process required the case study to be placed in its immediate historic context, providing a base point in terms of both discourse and practice from which later trends could be compared. It was in the second chapter that this task was undertaken. More specifically the chapter illustrated how in the context of a ‘war on terror’, the UK’s maritime infrastructure had been securitised. The threat presented as being posed by international terrorism to UK maritime infrastructure was captured in two main narratives, one where the infrastructure was a potential target and another where that infrastructure could be exploited by terrorists. Both drew upon the macrosecuritisation of the ‘civilised way of life’ captured in the ‘war on terror’ discourse, and in their reproduction, alongside through the implementation of subsequent emergency measures, the macrosecuritisation was reinforced.

By the end of chapter two then the close, indeed mutually reinforcing relationship, between the macrosecuritisation of the ‘civilised way of life’ and the securitisation of UK maritime infrastructure had emerged. An early insight in to the substantial impact of securitisation on the management of UK maritime infrastructure was also gained as the chapter elaborated the early stages of the implementation of the
International Ship and Port Facility Security (ISPS) code. The code was the central tenet of the counter-terrorism security response implemented in the immediate aftermath of terrorist attacks in the United States (US) on 11 September 2001.\footnote{International Maritime Organization, \textit{International Ship and Port Facility Security Code and SOLAS Amendments} (London: International Maritime Organization, 2003).} A point was reached whereby a number of the prominent features of the counter-terrorism security response could be noted. More specifically legislation and regulations were clearly utilised, increasing the power of many actors in relation to UK maritime infrastructure. There was a focus on enhancing the co-ordination between different members of the policy network. Security spending within UK maritime infrastructure grew, as did the profile of security activities, while a notable sense of urgency underpinned implementation. These features provided additional direction to the examination of counter-terrorism practice in the case study itself.

Over the course of the three chapters that made up the case study, the contours of the argument became clearer. With regards to the way in which UK maritime infrastructure was securitised, the macrosecuritisation of the ‘civilised way of life’ remained markedly stable over the course of the case study period. Particular events, most notably the terrorist attacks in London in July 2005, sparked considerable reflection about the ‘war on terror’, yet ultimately, and despite the terminology of ‘war’ being increasingly jettisoned, the idea that the ‘civilised way of life’ was existentially threatened by international terrorism remained resilient. This stable wider context ensured that the backdrop in which UK maritime infrastructure had been securitised in the aftermath of 11 September 2001 remained largely unchanged.
No wider structural changes then became apparent that would deprive the two main narratives relating to UK maritime infrastructure of their salience. They continued to be widely reproduced by a range of different members of the policy network between 2004 and 2009, creating the space and providing the rationale for the continued implementation of emergency measures. This in turn ensured that the broader threat presented as being posed by international terrorism remained in the wider consciousness. The mutually reinforcing relationship then between the macrosecuritisation of the ‘civilised way of life’ and the securitisation of UK maritime infrastructure was evident across the thesis.

Beneath this overall stability however, additional details about how specifically UK maritime infrastructure was securitised became apparent. The element of process to the securitisation was particularly notable. Chapter three highlighted the way in which constant reflection over the counter-terrorism security response - whether it worked and what, if anything, should come next - was apparent. This reflection was underpinned by the emphasis on maintaining constant vigilance and no complacency with regards to the presented threat. It was out of this reflection that resistance was witnessed. This resistance was directed most commonly at particular elements of the counter-terrorism security response rather than against the rationale for emergency measures themselves. In the 12 months after the ISPS code came in to force, where there were glimpses of resistance levelled at the presented terrorist threat, there was little evidence to suggest it had undermined the securitisation in any way. Nevertheless this situation demonstrated that resistance to the securitisation came in different forms. As the case study shifted to focus on the two years after the terrorist attacks in London on 7 July 2005 and the early years of the Premiership of Gordon
Brown respectively, these intricacies in relation to the securitisation of UK maritime infrastructure became clearer. To name just two examples, the target and vulnerable node narratives were increasingly reproduced as part of wider discussions over the security of the wider supply chain, transport network and UK border, while particular acts of resistance were able to bring about some change in counter-terrorism practice.

With regards to the impact of continued securitisation on the management of UK maritime infrastructure, the way in which the ISPS code led to the creation of restricted zones, the introduction of a three-tiered security level system and required the appointment of a Port Facility Security Officer (PFSO), gave an early impression of the considerable impact witnessed. Further light was shed on the prominent features of the counter-terrorism security response throughout the case study. The consistent use of legislation and regulations in the response remained evident. Security budgets continued to grow, with finance only prominently occupying the thoughts of the policy network towards the end of the case study, as recession hit the UK. The higher profile of security activities within UK maritime infrastructure was maintained as efforts to enhance security awareness expanded. Beyond these the focus on further enhancing co-ordination between members of the policy network was the subject of particular discussion, with the third chapter highlighting the importance of trust in building relationships. The fourth chapter built upon this by highlighting the emphasis placed on agency over structure to enhance co-ordination and by arguing that there was a hierarchy within the policy network, evident in committee membership and access to security information. Finally an additional feature of the response – the growing use of technology to enhance security – was
raised. The third chapter acknowledged this in its discussion of Felixstowe’s use of technology, and the substantial role technology was deemed to play was further demonstrated in the subsequent chapters as the Road Haulier IDENTification System (RHIDES) and the e-Borders programme were discussed.

In examining counter-terrorism practice and shedding further light on what were regarded as the prominent features of the counter-terrorism security response the thesis was able, over the course of the case study, to set out the response’s main characteristics too. After examining developments in the 12 months after the ISPS code had come in to force, an initial attempt at discussing these characteristics was made. Three in particular were noted, with the counter-terrorism security response described as constantly evolving, layered and increasingly expansive in scope. In the case of the latter characteristic this expansion was evident in the way in which counter-terrorism considerations shaped a growing range of day-to-day activities. Collectively these characteristics mirrored those of the presented threat itself. Aided with insights from two additional years of practice, the fourth chapter confirmed these characteristics. The chapter drew to a close by recognising a spatial dimension to the way in which the response was increasingly expansive in scope, as the idea of extending the zone of security outwards was highlighted. This idea had materialised in the extension of an ISPS-style security regime from the ship/port interface to the entire port, and the way in which the UK sought to ‘export’ its borders. The fifth chapter illustrated the spatial dimension to securitisation more explicitly through an examination of Project Kraken, a police initiative rolled out across the UK that sought to enhance security awareness around harbours and the coastline as a whole.
It was not until the fifth chapter and its conclusion most prominently, that the pursuit of increased power in relation to UK maritime infrastructure by the British state and port owners in particular was described as the thread which ran through the counter-terrorism security response. Despite this, the way in which security and power were intertwined in this case was evident across the thesis as a whole. ‘Power’ was defined broadly as the possession of influence over increasing areas of life in the second chapter. Here it was noted how the ISPS code had, for example, empowered state’s through their respective designated authorities with oversight over Port Facility Security Plans. In chapter four it was noted how the use of technology enabled both the British state and port owners to increase its pool of information over the movement of both people and goods. The accumulation of knowledge about UK maritime infrastructure represented one mechanism to increase power. This conclusion enabled previous practices to be reassessed. Specifically the increased use of fencing through the ISPS code and the growth in the number of private security personnel employed within UK maritime infrastructure were categorised as examples of investment in material capabilities. This investment enabled behaviour within UK maritime infrastructure to be more effectively managed with desired behaviour highlighted. This was a further mechanism to increase power and was illustrated in the final chapter in the growth in the number of members of the public involved in the security of UK maritime infrastructure. It was through these individuals behaviour could be managed, while they also served as additional pairs of eyes and ears on the ground.

Overall the main conclusion which can be drawn from this thesis is that the securitisation of UK maritime infrastructure was more complex than it first seemed.
Although its mutually reinforcing relationship with the macrosecuritisation of the ‘civilised way of life’ remained constant and the two main narratives widely and consistently reproduced, the case study was able to shed light on intricacies in relation to the role particular events play, the forms of resistance and their likelihood of success to name just three examples. This complexity was further demonstrated in the way in which the prominent features and main characteristics of the counter-terrorism security response did, in an overarching sense remain consistent, yet additional dynamics continued to emerge as the case study progressed. Overall then it was a picture of continuity and change. This conclusion will be defended by returning to address the two core research questions around which this thesis has been organised, noting the key research findings.

(C.2) Key findings:

Core Research Question (1) - ‘How has the United Kingdom’s maritime infrastructure been securitised in the context of responses to international terrorism?’

The first core research question served as an acknowledgement of the need to fully contextualise those counter-terrorism practices examined within the thesis. The starting premise was that UK maritime infrastructure had been securitised. This position was supported by the introduction of the ISPS code and a range of additional emergency measures thereafter. The creation of a Police National Maritime Security Strategy (PNMSS) and associated institutional structures, the launch of Project Kraken within coastal communities, and the introduction of a European wide 24-hour manifest declaration scheme, were just three examples.
The securitisation of UK maritime infrastructure took place in the wider context of the macrosecuritisation of the ‘civilised way of life’. The UK’s maritime infrastructure was a ‘site of securitisation’ in the sense that everyone, everything, and all activities associated with it were presented as requiring ‘securing’ from international terrorism. This facilitated the implementation of emergency measures. Returning to Figure 1, which outlined the securitisation process, can help to elaborate this situation further.

*Figure 1 - The securitisation process:*

In the aftermath of the terrorist attacks in the US on 11 September 2001, western political leaders internationally, most prominently from the US and UK, presented the ‘civilised way of life’ as being existentially threatened by international terrorism. The ‘civilised way of life’ was broadly understood as encapsulating democracy, economic prosperity and individual liberty. The political leaders then represented the
securitising actors, while the presentation of existential threat represented the securitising moves. Two audiences were appealed to, the national policy networks responsible for counter-terrorism and the general public. This macrosecuritisation was captured in the ‘war on terror’ discourse of counter-terrorism, where responding to international terrorism was understood as a Manichean battle between good and evil. The acceptance of the presented existential threat and the subsequent necessity for emergency action was evident in the combination of continual reiteration of the ‘war on terror’ discourse, its wider reproduction say, by parliamentarians, and in the way in which large swathes of both foreign and domestic policy were framed by counter-terrorism considerations.

The ‘macro’ within the macrosecuritisation rested on the way in which the referent object was an entire way of life and the presented threat international terrorism as a whole. This was significant because of its all-encompassing implications. The response then had to be equally wide-ranging, meaning that more areas of life were themselves deemed to require securing in order to ensure the survival of the ‘civilised way of life’. Illustrating the way in which a new policy trajectory had emerged then, within the UK specifically counter-terrorism very much took centre-stage. It became involved in the conflicts in Afghanistan and Iraq, and introduced a range of domestic counter-terrorism measures including the extension of pre-charge detention. This was the backdrop that saw UK maritime infrastructure securitised.

The presented terrorist threat relating to that infrastructure was captured in two main narratives. The ‘target’ narrative presented UK maritime infrastructure as being at
threat of attack from terrorists. Such an attack could undermine the operability of the infrastructure which in turn would have wider negative implications for say, the economy. The ‘vulnerable node’ narrative presented UK maritime infrastructure as a space that could be exploited by terrorists to do harm elsewhere, again with wider negative implications. Both narratives then drew upon the macrosecuritisation, the wider concerns about the security of the ‘civilised way of life’. They were reproduced by the policy network responsible for the security of UK maritime infrastructure. This included political leaders with some responsibility for policy relating to UK maritime infrastructure, alongside parliamentarians, civil servants, security professionals both state and privately funded, and the maritime industry as a whole, especially port owners and their senior management teams. These narratives created the space, provided the rationale even for the implementation of emergency measures relating to UK maritime infrastructure. In Figure 1 then they were located in the box entitled ‘emergency measures’.

The description of the relationship between the macrosecuritisation of the ‘civilised way of life’ and the securitisation of UK maritime infrastructure as mutually reinforcing stemmed from the recognition that both narratives drew upon the macrosecuritisation. Although concerns about the threat posed by terrorism, specifically in relation to Northern Ireland, meant that efforts were made to secure UK maritime infrastructure prior to 11 September 2001, undoubtedly in this period it was international terrorism that largely drove counter-terrorism efforts. Moreover without the macrosecuritisation is it very difficult to imagine the pace and scale of the changes witnessed in the case study occurring either. The reiteration of the two narratives served to further embed in wider consciousness the idea that international
terrorism was something that had to be addressed. This process only continued as emergency measures designed to secure UK maritime infrastructure were implemented.

Thinking in terms of continuity and change, the former was evident in a couple of main ways. First, the macrosecuritisation had its own genealogy, a point noted in chapter one. The idea that good and evil are pitted against each other, specifically in relation to international terrorism was by no means new. Second, the overall stability of the macrosecuritisation and the securitisation of UK maritime infrastructure was evident. Both the ‘war on terror’ discourse and the two narratives were widely reproduced, resilient to resistance and remained largely unchanged in form throughout the case study period. The Copenhagen School have suggested that macrosecuritisations are more prone to break down than securitisations, but in this case study no break down was evident. The terminology of ‘war’ was increasingly jettisoned, yet the idea that an existential threat was posed to the ‘civilised way of life’ remained accepted. This emphasises the Copenhagen School’s point that securitisation is ultimately about the grammatical structure of “existential threat, point of no return, and a possible way out”.

With regards to change, this stemmed from the element of process to the securitisation. This was evident in the mutually reinforcing relationship outlined

---


previously but was also seen in the way in which particular dimensions of the presented threat relating to UK maritime infrastructure were emphasised at different times. While there was a continual acceptance that there was a terrorist threat which could be broadly sub-divided in to concerns around the infrastructure being a target or a vulnerable node, it was further distilled. For example, as the case study period progressed it was clear how the attention of the policy network did, in relative terms, shift from the security of the ship/port interface to the security of smaller ports and harbours. To a large extent this fluidity was only extenuated by the international, inter-connected nature of the maritime industry which meant that policy developments in one state could have an impact on security practice in another. Here the US Congressional plan to demand the scanning of 100% of inbound containers for chemical, biological, radiological and nuclear (CBRN) materials was the clearest example.

Although different dimensions to the presented threat were highlighted, there was also acknowledgement of some of its nuance amongst members of the policy network, particularly over the likelihood of particular incidents actually materialising. Stopping the exploitation of a port by terrorists, rather than protecting it from attack was regarded by one Special Branch (SB) ports officer as the primary burden on his time. In the aftermath of terrorist attacks in London on 7 July 2005 and again in London and Glasgow in June 2007, the security level in UK maritime infrastructure remained lower than that in relation to its airports. Amongst the Project Kraken members of Suffolk the sense of terrorist threat facing their county was felt to be substantially less than that facing the UK as a whole.
Both these trends rested upon the tendency of the policy network to continually reflect about the security of UK maritime infrastructure in the context of the ‘war on terror’, also included in Figure 1. Illustrating the link between discourse and practice, the continued securitisation of UK maritime infrastructure ensured that calls for constant vigilance and no complacency with regards to the presented threat were made. This in turn led members of the policy network to locate perceived gaps and weaknesses in the existing counter-terrorism security response which required addressing. It was in this process that the new dimensions to the threat were raised and the nuance acknowledged. The process of reflection can ultimately be captured in two broad, recurring questions: ‘Is the existing counter-terrorism security response working?’ and ‘What, if anything, should come next?’ These questions provoke a series of ongoing discussions, which in this case study centred on how prescriptive the counter-terrorism security response should be and the need to maintain three balances. These were between security and commercial operations, between security and liberty, and over who had what responsibilities in relation to the response.

It is out of this reflection that acts of resistance to securitisation emerged. Most commonly resistance was directed at particular elements of the counter-terrorism security response, their perceived negative impact and future proposals relating to them. Occasionally it was directed at the rationale behind emergency measures, the idea of a terrorist threat, but with little sign of any substantial impact. This demonstrated that resistance came in different forms. It also serves as a reminder that securitisation did not eradicate all debate. The parameters of discussion were clearly restricted. This was demonstrated both by the relative absence of particular forms of resistance, and in the example of the Trade Union representative who admitted to
feeling able to resist biometric ID cards only on practical rather than security grounds. Yet there was widespread and at times heated discussion over particular measures. The US scanning proposal again was the clearest example across the case study.

That such a proposal was first delayed and then limited to a series of trials also illustrated that resistance could be successful in changing practice. But in the context of the securitisation of UK maritime infrastructure as a whole the success of acts of resistance can still only be described as limited. What was regarded as accepted practice did over the course of the case study change markedly. For example, the need for CBRN scanning equipment, an increased private security presence, and the growing use of ID cards all became widely accepted. Acts of resistance also created the opportunity for the reiteration of the presented threat as discussion followed. Particular events also had a similar effect. The terrorist attacks in Madrid in 2004 were seized upon by the IMO to encourage compliance with the ISPS code. The terrorist attacks in London in 2005 led to the presented terrorist threat being highlighted as part of wider discussions over the security of the transport network. The terrorist attacks in Mumbai in 2008 further enhanced the focus on the need to secure the wider coastline. This situation was captured very effectively by one SB ports officer who described the threat level as a “bit like a hospital monitor, it blips along with a couple of blips, continual things, then woof you get 9/11 and 7/7”.

While securitisation took place in the context of the macrosecuritisation of the ‘civilised way of life’, particular intricacies did then emerge.

---

4 Author’s interview with number 5, 31 March 2009.
Core Research Question (2) – ‘What has been the impact of securitisation on the management of UK maritime infrastructure?’

The second core research question captured the desired reorientation of research emphasis towards the post-securitised environment and on to the implementation of emergency measures. It recognised that in relative terms the Copenhagen School say very little about what securitisations ‘do’ in practice beyond suggesting that emergency measures may result in the revocation, suspension and/or circumnavigation of normal rules of engagement. Those studies that utilise securitisation theory also tend to focus more on how securitisation occurs and whether it is positive or negative over what impact it has. The reorientation then focused on examining the content of emergency measures, how they were delivered and what impact they had on day-to-day activities. Collectively this was described as the counter-terrorism security response.

Before moving on to discuss the prominent features and main characteristics of the counter-terrorism security response two additional, overarching points need to be noted. First, counter-terrorism was an important dimension to life within UK maritime infrastructure well before either 1 July 2004 or 11 September 2001. Demonstrating continuity with the past, UK experience in relation to Northern Ireland ensured counter-terrorism’s place on the policy agenda, with legislation such as the Aviation and Maritime Security Act, 1990 (AMSA) representing a concrete measure taken to help secure UK maritime infrastructure prior to 2001. Despite this,

---


the pace and scale of change undoubtedly were of a greater magnitude in the context of the ‘war on terror’.

Second, the ‘emergency’ in emergency measures did stem as much from the context in which policies emerged and the grounds on which they were subsequently justified and defended, than it did from their content. Although there was an underpinning of urgency to implementation, particularly the ISPS code, and efforts to require 100% scanning can be described as extraordinary, this cannot be said to the same extent with regards to the erection of a fence or the organisation of a meeting between port managers and SB ports officers. This may remind us of how the boundaries of accepted practice have changed, but it certainly does illustrate the value of aggregating findings in order to highlight trends.

Three main characteristics and six prominent features of the counter-terrorism security response were highlighted over the course of the thesis. They remained consistent throughout the case study, but new dynamics relating to each emerged as greater light was shed on counter-terrorism practice.

(1) The counter-terrorism security response constantly evolved:

The calls to maintain constant vigilance and no complacency with regards to the presented terrorist threat and the subsequent process of reflection discussed earlier, ensured counter-terrorism practice evolved as members of the policy network sought to stay ahead of their ‘enemy’. The implementation of emergency measures was a
continual and multi-stage process, but one not immune to the difficulties associated with the implementation of policy. Alterations to the membership of regional portal groups created to deliver the PNMSS, was just one small illustration of how different actor interests led to concrete change. The evolution of the counter-terrorism security response was captured most clearly in those efforts to ensure the response was further institutionalised. Defined as the process of embedding particular activities, roles, even ideas in day-to-day operations so as they become like second nature, institutionalisation was pursued prominently via efforts to ensure universal compliance with emergency measures and the harmonisation and improvement of security standards. This had placed attention on enhancing security awareness and expanding security training seen with regards to the ISPS code after 1 July 2004, and the attempt at building a greater sense of project identity with Kraken in Suffolk through the production and distribution of paraphernalia, to name just two examples.

(2) The counter-terrorism security response was layered:

The layered characteristic of the counter-terrorism security response primarily emerged out a desire to ensure that if one element of the response failed to secure UK maritime infrastructure, another would be in place to tackle the presented terrorist threat. For example, while restricted zones around the port/ship interface were seen amongst other things as being able to help prevent an attack on a ship while docked or prevent terrorists from gaining access to the entire port, other measures were taken here too. The EU 24-hr manifest scheme would enable shore authorities to gain information on prospective vessels and cargos in advance of departure, allowing them to deny access to those around which there were concerns.
The introduction of CBRN scanners through Project Cyclamen provided another means of ensuring dangerous cargos did not gain further accessed into the country. The response was also layered in a more generic sense. As the security level in relation to UK maritime infrastructure varied so the security practices undertaken varied. Practice was shaped by a mixture of measures, some of which were developed with maritime infrastructure firmly as their focal point, some of which were more associative in that they focused on the wider supply chain, transport network and UK border, while general counter-terrorism and civil contingency legislation could also have an impact. Finally the response was layered in the way in which emergency measures were initiated at different levels of governance.

(3) *The counter-terrorism security response was increasingly expansive in scope:*

The third characteristic of the counter-terrorism security response, its increasingly expansive scope, was evident in two main ways. On the one hand this expansive scope was captured in the way in which counter-terrorism considerations influenced a growing range of day-to-day activities relating to UK maritime infrastructure. To illustrate, a senior port manager in the UK today could realistically find themselves acting as their port’s PFSO, being responsible for the writing and delivery of a programme of security training for staff, organising regular port security drills in liaison with private security personnel, attending regular port security committee meetings, helping to manage new biometric identification systems, even engaging with local community groups in a counter-terrorism project designed to secure harbours and coastline around their port. In short, counter-terrorism considerations
would shape an increasingly large part of that individual’s working life and in a variety of different ways.

There was also a spatial dimension to this increasingly expansive scope. EU ‘Directive 2005/65/EC’ on enhancing port security ensured that an ISPS-style regime was introduced to the entire port. Project Kraken illustrated a desire to secure harbours and the coastline as a whole, and e-Borders and the associated focus on exporting the UK border sought to extend the zone of security further still. This spatial dimension is captured in the following figure, whilst also showing the layered characteristic of the response quite effectively.

---

Figure 3 – The spatial dimension to the securitisation:

The expanding circles represent the way in which the space that was deemed to require securing in relation to UK maritime infrastructure expanded. The arrows illustrate the broad direction of travel in this case study specifically as focus was initially placed on securing the port/ship interface through the ISPS code. For members of the policy network the objective was to push the presented threat further away from UK maritime infrastructure thus making it more difficult for that infrastructure to be attacked or exploited by terrorists. There was a self-perpetuating dynamic to this process however as an increase in security in one zone was understood to increase the threat elsewhere. This in turn demanded that the space
secured be further expanded and so forth. This emerged out of a fear that rested on the belief that the threat posed by international terrorism to the ‘civilised way of life’ was existential and as such any security gaps could have unimaginable negative consequences.

i) The central role of legislation/regulations:

The first prominent feature of the counter-terrorism security response was the central role played by legislation and regulations with counter-terrorism implications. These measures put in place the framework around which many of the institutional developments and working practices witnessed formed. Two insights in particular were evident here. The legislation/regulations often served to increase the power of particular actors in relation to UK maritime infrastructure. They also regularly were initiated outside of the UK, demonstrating the multi-levelled governance structure in relation to UK maritime infrastructure. One example capturing this was ‘European Commission regulation 884/2005’. It laid down EU inspection procedures for the ISPS code, and in doing so indirectly empowered the British state through the Transport Security and Contingencies Directorate (TRANSEC) to facilitate Commission inspections.

---

ii) Enhancing co-ordination between members of the policy network:

The second feature of the response was the focus on enhancing co-ordination between members of the policy network. This was widely evident in the creation of port security committees, regional portal groups, and the United Kingdom Border Agency (UKBA) to name just three examples. Beyond the launch of new structures however, it was widely accepted by those members of the policy network interviewed that it was through agency, the building of working relationships, that most significant progress was made. Here trust emerged as an important commodity and rested on understandings of competency. In relation to security, competency was tied to experience, with particular value placed on that gained within the military. The regularity and quality of training and even the level of incentive were also highlighted. Despite the focus on enhancing co-ordination, the group within the policy network involved in decision-making of a more strategic nature remained small. TRANSEC officials, SB ports officers, Home Office police representatives and senior port managers were four prominent groups here. A hierarchy existed within the policy network, indeed with access to certain security information limited to state representatives, a hierarchy within a hierarchy could also be said to have existed. This also demonstrated the secrecy associated with security activities.

iii) The growth in security spending:

The third feature of the counter-terrorism security response was the growth in spending on activities relating to the security of UK maritime infrastructure. In the run-up to the ISPS code coming in to force, ports invested heavily in sufficient
fencing, CCTV and security personnel to monitor restricted zones. The costs of new fencing in one port were put at £1 million for example. Gaining wider access to specific spending figures on security was difficult, yet the more than doubling of private security personnel at the Port of Tilbury and the shift towards ports levying a security surcharge to meet costs demonstrated the direction of travel. This latter example also illustrated the ‘user pays’ principle that was in place within the UK, where the costs were deemed to lie where they fell. Of all the features of the response highlighted in this thesis, it was this one which was most prone to change. Towards the end of the case study period and amidst the backdrop of recession in the UK, members of the policy network were preparing for the potential of budget cuts.

iv) The growing use of technology to enhance security:

The fourth feature was the growth in the use of technology to enhance security. The use of technology was heavily dependent on the ability to make the necessary financial investment, a position not every UK port found itself in. The Port of Felixstowe was however able to invest introducing a new IDentification and Access Control System (IDACS), a Road Haulier IDentification System utilising biometrics (RHIDES) and a Vehicle Booking System (VBS). Beyond the private sector the British government launched their own multi-million pound e-Borders scheme, trialled through Project Semaphore, designed to analyse the travel patterns of particular individuals and facilitate the reintroduction of full border embarkation controls. The central commonality across the different systems was the way in which technology served as a mechanism through which information about the movement of both people and goods could be collected. They did in short aid the
accumulation of greater knowledge about the maritime environment. In doing so the extent to which technology was beginning to lead counter-terrorism efforts, becoming increasingly separated from human engagement, was also highlighted.

v) Urgency:

The fifth feature of the counter-terrorism security response and the one which underpinned it was a notable sense of urgency. This emerged directly as a result of the wider context in which UK maritime infrastructure was securitised as efforts to secure maritime infrastructure were bound up in the need to secure the ‘civilised way of life’. With survival at stake security was the main priority and necessary measures had to be implemented as quickly as possible. The speed of action was illustrated in the ISPS code itself which was conceived, developed, passed by the International Maritime Organization(IMO), and came in to force internationally in just over 33 months. It was also captured in demands that 100% container scanning be undertaken within five years of the US H.R 1 - Implementing Recommendations of the 9/11 Commission Act of 2007 becoming law.9 In isolation these time periods did not look particularly short. Yet in comparison with previous efforts to introduce new international regulations and by recognising the scale of change demanded, they represented considerable speed and an ambitious schedule respectively. This serves as a reminder of the need to judge cases in their own context. This is not to say there were not delays in implementation. The EU 24-hr manifest scheme was delayed, the ratification of the new protocols of the Suppression of Unlawful Act Against the

Safety of Maritime Navigation (SUA) treaties was a drawn out process, while the roll out of project Kraken nationally occurred in stages. Yet the prominence of counter-terrorism considerations ensured security remained the issue presented as being of utmost importance in relation to UK maritime infrastructure.

*vi) A higher profile for security activities:*

Following on from this the sixth feature, did to a considerable extent, emerge as consequence of the other features. Security had always had a place in day-to-day activities in relation to UK maritime infrastructure, but its overall profile undoubtedly rose as a result of a range of new practice. Aesthetically this higher profile was captured in the introduction of restricted zones with accompanying access gates, fencing, CCTV and search procedures. It ensured that many UK ports more closely looked like military bases. In terms of working practices the emphasis on ensuring compliance with emergency measures and an improvement in security standards resulted in a range of efforts to enhance security awareness and expand security training. Posters, newsletters, security signs and DVD’s were utilised alongside electronic ISPS code training programmes and regular port security drills. These efforts were not directed simply at those who had security as their main role, but increasingly to anyone who had some relationship with UK maritime infrastructure. They also demonstrated the visual element to securitisation, noted in chapter one, as the presented threat was reiterated beyond discourse.
The pursuit of power:

The central thread running through the counter-terrorism security response was the pursuit of increased power in relation to UK maritime infrastructure, particularly by the British state and port owners. For the state this took place through institutions such as TRANSEC and SB ports officers, while for port owners it was through senior management teams and their work. More specifically two main, interlinked mechanisms of increasing power were witnessed. The use of fencing and the growth in the number of individuals with some responsibilities for, and awareness of security did, for example, represent an investment in material capabilities. These practices were understood as providing the means through which behaviour within UK maritime infrastructure was more effectively managed, with movement determined by physical boundaries and desirable behaviour emphasised through a cohort of ‘enlightened’ individuals.

If investing in material capabilities represented one mechanism to increase power, the second was the accumulation of knowledge about the marine environment. By learning more about the movement of people and goods within and around UK maritime infrastructure behaviour could once more be managed. The accumulation of knowledge was facilitated primarily by technology systems which were able to collect and analyse vast pools of information, and through that group of security aware individuals who provided additional pairs of eyes and ears. The desire to secure UK maritime infrastructure then was intertwined with the pursuit of increased power in relation to it. This situation occurred as a direct result of the way in which UK maritime infrastructure had been securitised. An attack on, or the exploitation of
UK maritime infrastructure was understood to have potentially catastrophic implications for the ‘civilised way of life’. The pursuit of increased power was driven by a fear of the consequences of failure.

(C.3) Future research avenues:

With the key findings elaborated attention can now turn to considering future research avenues. A useful starting point here is to consider the parameters of the existing case study itself. Although there always remains scope to collect additional material in relation to those developments witnessed in the three cases studied here – Felixstowe, Holyhead and Tilbury - the opportunities afforded to visit each case and the access granted to key members of the policy network enabled a depth of understanding to emerge. Gaining an insight in the views of those within the UK intelligence services on their work in relation to UK maritime infrastructure would be an interesting addition to the study. Yet the opportunity to engage with those SB ports officers who play a crucial intelligence gathering function day-to-day within UK maritime infrastructure, enabled some light to be shed on the more secretive side to counter-terrorism practice nevertheless. Additional insights would also emerge if the opportunity to become embedded within UK maritime infrastructure became available. Being able to witness day-to-day activities first hand over a longer period of time would, for example, provide great insight in to the dynamics of those working relationships between different members of the policy network, enabling more light to be shed on the hierarchy illustrated in this thesis.
While the three specific cases utilised captured the primary functions of UK ports, the addition of further cases and the extension of the study to cover a longer period of time would also provide additional material to analyse, allowing the trends highlighted in this case study to be fleshed out in even greater depth. There remains the issue of research practicalities to consider here, but a closer understanding of counter-terrorism practice in relation to the River Thames would add an interesting further dimension to the case study. It would facilitate greater understanding of security in an urbanised maritime environment and enable a more detailed assessment of the extent to which the Metropolitan Police’s (MET) considerable difference in size of force helps or hinders national co-ordination in the marine environment. Reference to the distinctiveness of the MET was noted in the case study and was captured in a brief research trip to the force, but there is scope for more work here.10 In terms of timing, developments after June 2009 and beyond the General Election in 2010 would enable both the full impact of the recession on security spending to be considered and an assessment of the extent to which, if at all, a change of government has influence the securitisation.

Focusing on the key findings themselves, at the outset of this thesis it was suggested that reorienting emphasis towards the post-securitised environment and on to the implementation of emergency measures would facilitate a more complete examination of the wider implications of securitisation on, say, civil liberties. This is because a wider pool of evidence is gained by examining developments in practice

---

10 A two day research trip to the Metropolitan Police Service’s Marine Policing Unit (MPU) was undertaken while researching this case study. For further details on the MPU see their website, accessed 14 October 2008, http://www.met.police.uk/marine/.
over a sustained period of time allowing more detailed trends to be drawn. Certainly
the way in which port authorities internationally were accused of restricting seafarer
rights, the unease of hauliers specifically over the intrusion associated with
additional vehicle searches, and the tension over the use of biometric identification
cards within UK maritime infrastructure, illustrates that a range of examples were
highlighted in this case study which those interested in examining the relationship
between security and liberty more generally could utilise. For those interested in UK
maritime infrastructure specifically there is scope for a more sustained examination
of the security/liberty balance. Undertaking a series of interviews and organising
focus groups with ordinary port workers and hauliers to examine in greater detail the
extent to which they have felt that their freedoms had been eroded in the pursuit of
security would certainly be an interesting future research avenue. Such work would
also have wider benefits in facilitating greater understanding of what was deemed
acceptable practice, would further increase our knowledge of the way in which the
security message is communicated on the ground, and enable any acts of resistance
to the securitisation to be examined in more depth.

Beyond this, three additional avenues of research offer particularly interesting
opportunities. The growing use of technology to enhance security highlights a post-
anthropological dimension to security where the role of humans on a day-to-day
basis changes. The growing use of technology and its effects has been the subject of
discussions in relation to war and border control.11 There is potential from this case

---

11 In terms of war Michael Ignatieff’s book Virtual War offers an excellent overview of the trend towards
military conflicts being fought remotely utilising technology. See Michael Ignatieff, Virtual War: Kosovo and
Beyond (London: Vintage, 2001). Also see Christopher Coker, Humane Warfare (London: Routledge, 2001) and
Tyler Wall and Torin Monahan, ‘Surveillance and violence from afar: The politics of drones and luminal
study to examine in greater detail the mechanics of technology systems such as RHIDES and e-Borders, focusing specifically on the role of human engagement on a day-to-day basis, the level of oversight held over that data which is collected and the processes of accountability in place for when errors occur. The second research avenue focuses on the spatial dimension to securitisation which emerged over the course of the case study period. Engaging with the work of those interested in the way in which different spaces have been ‘secured’ and with what effects on day-to-day activities, it would be interesting to gain a firmer understanding from members of the policy network as to their justifications for the extension of the zone of security.  

A useful starting point would be to determine to what extent there was clear recognition from the policy network both that this process was taking place and of its self-perpetuating nature.

Finally, there is significant scope to study further the way in which a growing number of individuals have gained some responsibility for, and awareness of, security in relation to UK maritime infrastructure, particularly members of the general public. To what extent does this trend represent a ‘back to the future’ moment in comparison to say, the role played by the Home Guard during World War


Two? What expectations do both the public and the state place on each other? What are the consequences for the relationship between those brought in to the security world and those remaining on the outside? Here such research would benefit from engagement with literature on the privatisation of security more generally.¹³

Appendix A – Interview Strategy

The interviews undertaken during the course of research were semi-structured in the sense that a brief list of topics were utilised to structure discussion. Prior to each interview commencing, either via email or in person at the beginning of the interview, each interviewee was asked whether they were (a) happy to be recorded on a digital voice recorder and (b) in which way they would they like their interview material to be utilised (see categories below).

In the vast majority of cases the interviewee preferred not to be recorded. Here notes were taken during the interview which were subsequently written up in additional detail after the interview had concluded. Where an interviewee did agree to be recorded, detailed summaries of the interview were typed up after the interview. These were not verbatim transcripts, but rather time stamped summaries of the order in which points were raised, with selected quotations of interest listed. The interviewee’s full name was also removed from these summaries. Interview notes and some copies of the written summaries were stored in a safe for added security. Written summaries and interview recordings were also saved on a USB memory stick which was also stored in a safe. All those quotations utilised in the thesis are semi-verbatim as all umms, ahh’s, stuttering and false starts have been removed.

Each interviewee was offered the opportunity to have their interview material utilised in three main ways. Every interviewee except one agreed to speak ‘off record’, with the other individual agreeing to speak on a ‘background’ basis only.

Category A – ‘On Record’

- Interview material may be reproduced in full, including, but not limited to the use of direct quotations.
- Interview material is fully attributable to source.

Category B – ‘Off Record’

- Interview material may be reproduced in full, including, but not limited to the use of direct quotations.
- The interviewee’s name is not included in the thesis. The interviewee’s role is often referred to in more general terms such as a ‘Port Security Manager’ or ‘a Trade Union representative’. The interviewee is randomly allocated a number for the purposes of referencing.
- On a number of occasions and for additional anonymity an interviewee’s specific working location is also removed.
- Where the content of the material discussed may indirectly contribute towards identifying the specific working location of an interviewee, that material is referenced as ‘ascertained during an interview’ or words to that effect, with the interviewee’s reference number removed.

**Category C – ‘Background only’**

- Interview material may not be reproduced whatsoever and no record of interview is noted in the thesis.

- Interview material may be utilised for background purposes. These include, but are not limited to:

  - Clarifying, confirming and/or contextualising existing points/arguments made in the thesis.

  - Directing future research efforts.

  - Raising general trends e.g. ‘During the course of research one emerging trend was…’
Below is a wider dataset from the survey which was undertaken in collaboration with Suffolk Constabulary. The data is set out with the raw number of individuals who selected each box written first and the percentage of the total responses for that statement it represents in brackets afterwards. The total number of responses is written in brackets at the end of each statement/question. Please note that as each percentage is round up to one decimal place, the total across each box will not necessarily equal 100%.

**B: The Terrorist Threat -**

Please place a cross ‘x’ in the most appropriate response to the following statements:

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neither agree nor disagree</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. ‘The threat of terrorism against the United Kingdom has increased significantly since September 11th 2001.’ (22)</td>
<td>10 (45.5%)</td>
<td>9 (40.9%)</td>
<td>3 (13.6%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>5. ‘The current threat of terrorism to Suffolk is significant.’ (22)</td>
<td>1 (4.5%)</td>
<td>9 (40.9%)</td>
<td>12 (54.5%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>6. ‘Terrorism poses a significant risk to the maritime community in particular.’ (22)</td>
<td>2 (9.1%)</td>
<td>10 (45.5%)</td>
<td>8 (36.4%)</td>
<td>2 (9.1%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>7. ‘The United Kingdom’s coastline/border is very well protected against the threats posed by terrorism.’ (22)</td>
<td>0 (0%)</td>
<td>1 (4.5%)</td>
<td>5 (22.7%)</td>
<td>12 (54.5%)</td>
<td>4 (18.2%)</td>
</tr>
<tr>
<td>8. ‘The nature of the terrorist threat is well explained by the Government.’ (21)</td>
<td>0 (0%)</td>
<td>4 (19.0%)</td>
<td>9 (42.9%)</td>
<td>6 (28.6%)</td>
<td>2 (9.5%)</td>
</tr>
</tbody>
</table>
9. ‘The nature of the terrorist threat is well explained by Local Authorities (County/District Council).’ (21)  

<table>
<thead>
<tr>
<th></th>
<th>Very Likely</th>
<th>Likely</th>
<th>Not Sure</th>
<th>Unlikely</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0 (0%)</td>
<td>5 (23.8%)</td>
<td>12 (57.1%)</td>
<td>4 (19.0%)</td>
</tr>
</tbody>
</table>

10. ‘The nature of the terrorist threat is well explained by Suffolk Constabulary.’ (22)  

|                  | 3 (13.6%) | 9 (40.9%) | 6 (27.3%) | 4 (18.2%) | 0 (0%) |

11. ‘The threat posed by terrorism is exaggerated by the Government.’ (22)  

|                  | 0 (0%)      | 6 (27.3%) | 12 (54.5%) | 4 (18.2%) |

12. ‘The threat posed by terrorism is exaggerated by Local Authorities (County/District Council).’ (22)  

|                  | 0 (0%)      | 7 (31.8%) | 12 (54.5%) | 3 (13.6%) |

13. ‘The threat posed by terrorism is exaggerated by Suffolk Constabulary.’ (22)  

|                  | 0 (0%)      | 5 (22.7%) | 13 (59.1%) | 4 (18.2%) |

What is the likelihood of the following taking place in the next five years?

<table>
<thead>
<tr>
<th></th>
<th>Very Likely</th>
<th>Likely</th>
<th>Not Sure</th>
<th>Unlikely</th>
</tr>
</thead>
<tbody>
<tr>
<td>14. ‘A terrorist attack on a major Suffolk Port (e.g. Felixstowe, Ipswich).’ (21)</td>
<td>2 (9.5%)</td>
<td>11 (52.4%)</td>
<td>6 (28.6%)</td>
<td>2 (9.5%)</td>
</tr>
<tr>
<td>15. ‘A terrorist attack on a small Suffolk marina/harbour.’ (21)</td>
<td>0 (0%)</td>
<td>2 (9.5%)</td>
<td>7 (33.3%)</td>
<td>12 (57.1%)</td>
</tr>
<tr>
<td>16. ‘A terrorist attack on a Suffolk seaside resort (e.g. Lowestoft).’ (21)</td>
<td>0 (0%)</td>
<td>6 (28.6%)</td>
<td>11 (52.4%)</td>
<td>4 (19.0%)</td>
</tr>
<tr>
<td>17. ‘Weapons smuggling through a major Suffolk port.’ (20)</td>
<td>10 (50.0%)</td>
<td>7 (35.0%)</td>
<td>3 (15.0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>18. ‘Weapons smuggling via a smaller waterway/harbour.’ (21)</td>
<td>11 (52.4%)</td>
<td>7 (33.3%)</td>
<td>3 (14.3%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>19. ‘Terrorists entering the United Kingdom through a major Suffolk port.’</td>
<td>5</td>
<td>9</td>
<td>6</td>
<td>1 (4.8%)</td>
</tr>
</tbody>
</table>
20. ‘Terrorists entering the United Kingdom via a smaller waterway/harbour.’ (21)

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neither agree nor disagree</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(23.8%)</td>
<td>(42.9%)</td>
<td>(28.6%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(47.6%)</td>
<td>(38.1%)</td>
<td>(9.5%)</td>
<td>(4.8%)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

C: Counter-terrorist activities (in general) -

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neither agree nor disagree</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21. ‘The United Kingdom’s counter-terrorism activities are well explained by the Government.’ (22)</td>
<td>0 (0%)</td>
<td>4 (18.2%)</td>
<td>9 (40.9%)</td>
<td>9 (40.9%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>22. ‘Suffolk’s counter-terrorism activities are well explained by Suffolk Constabulary.’ (22)</td>
<td>1 (4.5%)</td>
<td>11 (50.0%)</td>
<td>7 (31.8%)</td>
<td>3 (13.6%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>23. ‘The United Kingdom’s counter-terrorism activities represent a proportionate response to the threats posed.’ (22)</td>
<td>1 (4.5%)</td>
<td>11 (50.0%)</td>
<td>9 (40.9%)</td>
<td>1 (4.5%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>24. ‘Suffolk Constabulary’s counter-terrorism activities represent a proportionate response to the threats posed to the county.’ (22)</td>
<td>2 (9.1%)</td>
<td>13 (59.1%)</td>
<td>7 (31.8%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>25. ‘The United Kingdom’s counter-terrorism activities are effective.’ (21)</td>
<td>1 (4.8%)</td>
<td>5 (23.8%)</td>
<td>15 (71.4%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>26. ‘Suffolk Constabulary’s counter-terrorism activities are effective.’ (22)</td>
<td>0 (0%)</td>
<td>7 (31.8%)</td>
<td>14 (63.6%)</td>
<td>1 (4.5%)</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>
27. ‘The general public have an important role to play in the fight against terrorism.’ (22)

<table>
<thead>
<tr>
<th></th>
<th>Yes (%)</th>
<th>No (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14 (63.6%)</td>
<td>7 (31.8%)</td>
</tr>
</tbody>
</table>

D: Project Kraken –

<table>
<thead>
<tr>
<th>Question</th>
<th>Strongly Agree (%)</th>
<th>Agree (%)</th>
<th>Neither agree nor disagree (%)</th>
<th>Disagree (%)</th>
<th>Strongly Disagree (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>30. Did you attend the Project Kraken Launch Event in April 2009? (22)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31. Are you a member of Project Kraken individually or as an organisation? (Please write in one of the boxes provided)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32. ‘I have a clear understanding of the objectives of Project Kraken.’ (22)</td>
<td>8 (36.4%)</td>
<td>14 (63.6%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>33. ‘The Project Kraken website is informative.’ (22)</td>
<td>1 (4.5%)</td>
<td>15 (68.2%)</td>
<td>6 (27.3%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>34. ‘The Project Kraken website is easy to use.’ (21)</td>
<td>1 (4.8%)</td>
<td>15 (71.4%)</td>
<td>5 (23.8%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>35. ‘The Project Kraken newsletter is informative.’ (22)</td>
<td>1 (4.5%)</td>
<td>14 (63.6%)</td>
<td>7 (31.8%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>36. ‘I would prefer more regular Project Kraken updates.’ (22)</td>
<td>1 (4.5%)</td>
<td>9 (40.9%)</td>
<td>12 (54.5%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>37. ‘I feel as though I/my organisation play an active role in Project Kraken.’ (22)</td>
<td>5 (22.7%)</td>
<td>13 (59.1%)</td>
<td>3 (13.6%)</td>
<td>1 (4.5%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>38. ‘If I had some information to share I would know how to do so.’ (22)</td>
<td>9 (40.9%)</td>
<td>13 (59.1%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>39. ‘If I had some information to share I would feel</td>
<td>10 (45.5%)</td>
<td>12 (54.5%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>
comfortable doing so.’ (22)

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>40. ‘I am confident the appropriate authorities will deal with my information professionally.’ (22)</td>
<td>7 (31.8%)</td>
<td>12 (54.5%)</td>
<td>3 (13.6%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>41. ‘I would like updates on those outcomes, where possible, resulting out of my information submission.’ (22)</td>
<td>4 (18.2%)</td>
<td>14 (63.6%)</td>
<td>3 (13.6%)</td>
<td>1 (4.5%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>42. ‘Project Kraken is a valuable crime &amp; counter-terrorism strategy.’ (22)</td>
<td>8 (36.4%)</td>
<td>13 (59.1%)</td>
<td>1 (4.5%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>43. Have you ever shared any information with the Police and partner agencies via Project Kraken? (22)</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7 (31.8%)</td>
<td>15 (68.2%)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Bibliography

Books & Book Chapters:


**Journal Articles & Research Papers:**


Balbaa, Alsnosy, ‘Protecting seafarer’s rights – the need to review the implementation of the ISPS code’, *Maritime Security and MET*, (2005), pp. 245-252.


**Media Sources:**


Stares, Justin, ‘Europe has not woken up to 100% scanning’, *Lloyd’s List*, 12 June 2008, p. 2, accessed IMO Knowledge Centre 8-10 February 2010.


Stares, Justin, ‘Screening ‘will disrupt trade’’, *Lloyd’s List*, 26 January 2007, p. 3, accessed IMO Knowledge Centre 8-10 February 2010.


**Documents:**

**Legislation & Regulations:**


**Speeches & Statements:**


Official Reports, Strategy Documents & Publications:


Commission of the European Communities, ‘Report from the Commission to the Council and European Parliament on transport security and its financing (COM


*Parliamentary Debates & Committee Work:*


Submission by Japan, the United Kingdom and the United States, ‘Report of the Correspondence Group on security arrangements for vessels which do not fall within


**Internet Resources:**


