Responding to international terrorism: the securitisation of the United Kingdom's ports.

Introduction

It was less than a week after the 11 September 2001 terrorist attacks that the then Secretary-General of the International Maritime Organization (IMO), William O'Neil, noted that 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"* (O'Neil, 2001).[i][1] A little under three years later, on 1 July 2004, this re-examination and re-assessment was most clearly illustrated when the International Ship and Port Facility Security (ISPS) Code came in to force. Developed within the IMO and introducedinternationally for added consistency, the ISPS Code encapsulated a new maritime security regime. To name just two examples, it required the appointment of Port Facility Security Officers (PFSO) tasked, amongst other things, with co-ordinating port security surveys and developing port security plans; while it also required the introduction of restricted zones within ports.

The ISPS Code was the international community's most prominent regulatory response to concerns that terrorists might attack ships and ports and/or exploit them

to facilitate attacks elsewhere.[ii][2] Today it sits alongside various other mechanisms designed to secure the maritime domain against a series of presented security threats;[iii][3] threats such as piracy, terrorism and drugs trafficking. These threats have increasingly been laid out in formal maritime security strategies such as that of the African Union (AU) in January 2014, the United Kingdom (UK) in May 2014, and the European Union (EU) in June 2014.[iv][4]

As maritime security considerations rise up both the political and security agendas with prominent challenges such as piracy increasingly capturing attention, this article sheds further light on how we might think about resultant security practice. It does this through an elaboration of how one part of the maritime domain – ports - and in one major island state and global maritime power - the United Kingdom - was securitised in the specific context of responses to international terrorism, the 'war on terror'. This process results in the development of a typology of counter-terrorism practice, a typology which offers a mechanism for examining port security. Ports are an important case study as they have a multi-faceted role representing nodes in the global supply chain, hubs in the transport network and as border management locations. As such what happens in and around them in terms of security practice has a significant bearing on economic development and has the potential to spark varied political debate.

Taking the date onwhich the ISPS Code came in to force internationally, 1 July 2004, and drawing upon developments in the years immediately thereafter, the article

demonstrates the way in which activities associated with UK ports were influenced by wider concerns about the threat that international terrorism posed to what a number of leading western political leaders would refer to as the 'civilised way of life'[v][5]. Examples of counter-terrorism practice associated with UK ports are discussed, with the totality of this practice understood to encapsulate three broad constituent parts – 'legislation and regulations', 'institutional developments and infrastructure changes' and 'working practices'.[vi][6]

Structurally the article starts by contextualising the environment in which counter-terrorism practice in UK ports was implemented drawing upon the Copenhagen School's work on securitisation. It argues that the securitisation of UK ports in the context of responses to international terrorism was wrapped up in a mutually reinforcing relationship with the macrosecuritisation of the 'civilised way of life', captured in the 'war on terror' discourse. It was in this context that a particular set of narratives emerged about the threat posed by international terrorism to UK ports, narratives that ultimately underpinned the case for, and created the space in which, the counter-terrorism security response in relation to ports was implemented. Despite the reference to narratives however, the article does not seek to offer an additional discourse analysis of the 'war on terror', of which there are many (see Silberstein 2004, Jackson 2005, Croft 2006). Rather the discussion of narratives is included to illustrate the backdrop against which counter-terrorism practice was implemented in UK ports.

With this process complete the article moves to its core task of laying out its typology by discussing examples of legislation and regulations, institutional developments and infrastructure changes, alongside working practices witnessed in the years after the ISPS Code's introduction. Three overarching objectives underpinning counter-terrorism practice are noted: (1) ensuring security readiness by *preparing* for all eventualities, (2) *protecting* the port from the terrorist threat, and (3) putting in place mechanisms to *verify* security compliance and standards. While the focus of the article is on counter-terrorism practice in UK ports, the multi-levelled governance associated with UK port security is evident as the involvement of actors at the international (IMO), regional (European Union) and national (UK) levels is discussed, and the influence of the United States noted. This multi-levelledgovernance is perhaps unsurprising when we consider the global nature of the maritime industry, the existence of the European single market, and the relative openness of UK ports to private ownership, each where regulatory harmonisation is deemed to aid business. Nevertheless, it illustrates the way in which ports serve as an example of the blurring of state sovereignty as varied non-state actors exercise influence over activities within a state's territorial boundaries.

The article concludes by utilising the typology to elaborate how, in the case of the UK at least, the counter-terrorism security response in relation to ports could be described as constantly evolving, layered and increasingly expansive in scope. A spatial dimension to the securitisation of UK ports in this particular context is thus noted as being present alongside a temporal dimension, as authority figures sought ever greater knowledge about, and as such control over, activities associated with

these sites. The end result is that alongside providing a mechanism through which counter-terrorism practice associated with ports can be organised and examined, the article also illustrates how an emphasis on the management of space is a core consideration when conceptualising port security. While more generally the article also contributes towards efforts to more clearly map and conceptualise maritime security (Bueger 2015) by illustrating the way in which security practice within the shore component of the maritime domain – ports – was justified and practices institutionalised.

The macrosecuritisation of the 'civilised way of life'

Before laying out a typology of counter-terrorism practice in UK ports in the context of responses to international terrorism, it is first necessary to better understand the backdrop against which such practice became possible, and was implemented; in short the policy environment. This approach rests on a starting assumption that discourses have practical policy implications (Campbell 1998, Jackson 2005, Croft 2006, Hansen 2006). More specifically, to do this the work of the Copenhagen School, specifically its securitisation theory, is particularly useful. 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?" (Buzan, Waever and de Wilde 1998, 27). 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" (Buzan, Waever and de Wilde 1998, 24) so that emergency measures can be pursued.

This 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 (Buzan, Waever and de Wilde 1998, 26).[vii][7] 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" (Buzan, Waever and de Wilde 1998, 24). 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.

In 2009 Buzan and Waever introduced the concept of 'macrosecuritisation' to their work. They examined 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 (Buzan and Waever 2009, 253). They also acknowledged how "one over-arching conflict" can result in a "higher order of securitisation" becoming embedded with other "more parochial securitisations beneath it" (Buzan and Waever 2009, 253). Moreover, in examining the relationship between securitisations, Buzan and Waever (2009, 254) also highlighted the concept of 'security constellations'

which they acknowledged had been originally under-developed. A security constellation encapsulates "the totality of possible security interrelationships at all levels" (Buzan, Waever and de Wilde 1998, 201) and the focus on them is designed to serve as an acknowledgement that securitisations are not isolated (Buzan and Waever 2009, 257).

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 securitisations 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. This emphasis on meta-narratives 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.[viii][8]

Ultimately the 'war on terror' counter-terrorism discourse captured a macrosecuritisation. Here a macro-level referent object, the 'civilised way of life' (encapsulating liberal-democracy, individual liberty and economic prosperity) was presented as being existentially threatened by a macro-level threat, 'international terrorism'.[ix][9] 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 the responsibility for the counter-terrorism security response, and the general public to whom governments must appeal for support for their decisions.[x][10]

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'.[xi][11] 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'.[xii][12] This is the backdrop against which counter-terrorism developments in UK ports can beseen.

The port as potential target and vulnerable space

With the policy environment set out, attention can now return to the port, which this article argues, can be understood as a 'site of securitisation'.[xiii][13] This description stems from an acknowledgement that ports are ultimately geographic spaces in which buildings and equipment (assets) can be located and a series of activities take place. 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" (Bormann and Sheehan 2009, 2).

The emphasis on the inevitability and necessity of security practice is important to reiterate as it reminds us that such practice emerges from, and ultimately feeds, securitisation. From the aftermath of the 11 September 2001 terrorist attacks, through to the date the ISPS Code came in to force on 1 July 2004, and across subsequent years, two main threat narratives, not always easily differentiated from each other, were evident in relation to ports. The first narrative presented the port as possible 'target' of international terrorism. International terrorism threatened the operability of the infrastructure which in turn had wider negative ramifications. The second presented the port as a 'vulnerable node', a space that could be exploited by terrorists to do harm elsewhere. These narratives created the space in which, the rationale even, for the development and implementation of the counter-terrorism security response associated with UK ports.

To illustrate further, the contours of these two narratives can be seen in speeches made by two different Secretary-General's of the IMO, a specialised agency of the

United Nations responsible for developing and maintaining a comprehensive regulatory framework for shipping, and out of which the ISPS Code emerged. At a speech to the IMO in December 2002, IMO Secretary-General William O'Neil connectedthe presented threat of terrorism to the maritime industry as considerations about a regulatory response were emerging. Reproducing the target narrative he commented:

> "…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" (International Maritime Organization 2002a, 3).

Nearly two years later, as preparations were being made for the ISPS Code to come into force on 1 July 2004, the importance of responding to the presented terrorist threat and the idea that there should be constant vigilance and no complacency with regards to it were still being reiterated. In the aftermath of the terrorist attacks in Madrid in March 2004 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:

> 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 (International Maritime Organization 2004a).

As a final reminder the IMO 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.[xiv][14]

A typology of counter-terrorismpractice in UK ports

Attention now turns towards examining the counter-terrorism security response in more detail in relation to UK ports, providing a snapshot of what securitisation looked like on a day-to-day basis. The counter-terrorism security response can, to draw a little more directly on the terminology of the Copenhagen School, be understood as encapsulating the content of emergency measures, their delivery and impact on day-to-day activities. To provide additional structure to this process of shedding light on the securitised environment and to more effectively facilitate the process of highlighting trends, it is here that the formulation of a typology of counter-terrorism practice in UK ports is useful. This typology should be understood as a flexible, living framework that aspires to provide a useful starting point for analysts whether they are interested in port security, practical responses to international terrorism, or security practice as a whole. Towards the end of article reassembly takes places as wider conclusions are drawn about UK port security in the context of responses to international terrorism.

As a starting point of the typology the totality of counter-terrorism practice witnessed in relation to UK ports can be sub-divided, albeit with some overlap, in to three broad constituent parts. The first part - **'legislation and regulations'** – includes those

documents laid down in law which introduced or framed particular emergency measures relating to UK ports. The second part - **'institutional developments and infrastructure changes'** – often, though not always, emerged 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 ports. This includes physical changes within ports themselves, 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 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 ports.

A: Legislation and Regulations

Turning to 'Legislation and Regulations', to contextualise developments in the post-1 July 2004 period it is important to provide more information on the ISPS Code itself. The Code provides a framework made up of two parts and 38 sections (excluding annexes) through which both vessels and port facilities at the ship-port interface can be secured.[xv][15] 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" (IMO n.d).

The code is split in to two parts, the first is mandatory and the second is recommendatory. Within Part A there is, for example, 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. 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 (IMO 2003, 6-36). 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" (IMO 2003, 43) Within the United Kingdom, responsibilities are split between the Department of Transport (DfT) and the Maritime and Coastguard Agency (MCA).

While the ISPS Code was the clearest manifestation of the securitisation of UK ports in the context of responses to international terrorism, it did not stand alone. Two notable developments were evident with regards to 'Legislation and Regulations' in the years after 1 July 2004. The first was a general emphasis on ***information-gathering*** about the activities taking place on a day-to-day basis within UK ports. Considering the container port by way of illustration, one regulatory move pursued by the European Union was to introduce a 24-hour manifest rule for containers. If the ISPS Code through its restricted zones helped facilitate the monitoring of the physical ship/port interface; such a manifest rule would strengthen pre-screening of the cargo moving through that interface by collecting and sharing data on the cargo within containers bound for an EU port at least a day before loading commenced in the non-EU port. The rule was an example of the EU's emphasis on maintaining an intelligence-led approach to container security, an approach some in the US Congress at the time challenged as they instead sought 100% container scanning.[xvi][16] The manifest rule became mandatory across the EU on 1 January 2011, a delay of nearly 18 months on the initial target of July 2009, as the appropriate institutional structures and infrastructure were put in place across the union.[xvii][17]

Alongside the general emphasis on utilising legislation and regulations as a mechanism through which information-gathering about activities associated with ports could take place; a second notable characteristic of UK port security was the multi-levelled **auditing and inspection regime** that was implemented. If the former development illustrated a desire to locate potential challenges to UK port security that required a response, the latter was an effort to ensure compliance, encourage improvements of security standards and seek greater harmonisation of such standards within and between countries of those security measures that were already in place. In short, there was a desire to ensure ports went beyond simply approaching security as a paper exercise.

The idea of inspecting ISPS Code implementation for example had been around as the Code was first developed, but as the in-force date (1 July 2004) had drawn ever closer, focus increasingly turned towards setting out the mechanics of such a programme. While it had been decided that external inspections for UK ports were to be undertaken by a combination of European Union (EU), Department of Transport (DfT), and Maritime and Coastguard Agency (MCA) inspectors; the specific nature of the EU's role had been the subject of debate at the European level. There was 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 (Stares 2005, 1). For the industry itself, concerns centred on the logistical strains that could accompany multiple inspections, as Patrick Verhoeven of the European Sea Ports Organisation commented:

> we do not mind commissioninspectors 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 (Stares 2005, 1).[xviii][18]

The disagreements serve as a reminder of the multi-levelled governance of UK port security, blurring our traditional understanding of sovereignty. They also illustrate that tensions 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 gained primary responsibility for assessing compliance and standards within their territory, yet European inspectors were to undertake more than a 'screening role' as they were 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 structures" (European Commission 2004). The specific EU inspection procedures were laid down in 'European Commission regulation 884/2005' published on 10 June 2005 (European Commission 2005).

B: Institutional Structures and Infrastructure Developments

Shifting attention to the changes in institutional structures and infrastructure developments witnessed in UK ports in the years after 1 July 2004, the desire to gain information about and more effectively monitor activities within ports is evident once

more. There was considerable investment in ***protective security measures*** in UK ports as Closed-Circuit Television (CCTV) was introduced or upgraded and identity card technology embraced. This all sat alongside the construction of new and enhanced fencing and access gates to delineate between what were restricted areas and what were not, evidence of an interest in influencing behaviour alongside monitoring it. These changes were undoubtedly the most visible sign of securitisation for any outsider looking in. None were wholly new developments, but the pressures imposed by measures such as the ISPS Code to place security considerations at the centre of day-to-day activities ultimately led to higher quality infrastructure being installed across the board in the form of stronger fencing and more powerful cameras.[xix][19]

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. The costs would be met, partially at least, by the introduction of security charges to shipping companies. The UK's long-standing 'user-pays' principle in port security meant there was little to no financial support provided from central government. In future years Felixstowe would also be at the forefront of the investment in new technology, developing an IDentification and Access Control System (IDACS) to aid in the monitoring of both cargo and people and in 2006 an identification system for those road hauliers using the port called the Road Haulier IDEntification System (RHIDES) which utilised an ID card with biometrics.[xx][20] 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.

The introduction of technology as advanced as RHIDES is a reminder that the security practices undertaken in and around UK ports 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 to the author, while other ports took security seriously “there is a limit to what they can actually do, whilst trying to maintain a business” (Author’s Interview). Nevertheless another interviewee noted that a balance could be struck between security and operational requirements arguing that, “…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” (Author’s Interview).

The policy network responsible for implementing the counter-terrorism security response on a day-to-day basis also set up a variety of institutional structures to facilitate implementation. ***Port security committees*** met on an approximate monthly basis in major ports with a membership including representatives from central government (mainly from the Department for Transport), Special Branch (SB) ports officers, local Home Office force representatives, ports police and senior port management. Sometimes change in institutional structures came about more from compulsion than anything else. Emerging out of European directive EC 2005/65,

adopted by the European Council and Parliament in October 2005 (European Union 2005), was the requirement for Member states 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 (European Union 2005, paragraph 10). 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" (European Union 2005, Annex I),[xxi][21] representing a direct example of the reproduction of the two main threat narratives highlighted earlier within official regulatory documents. Member states had to comply with the directive by 15 June 2007 (European Union 2005, Article 18, 1).

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 been largely 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" (European Union 2005, Article 10,1 and Annex III), were already in place and on occasion had already been exceeded. UK authorities 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 (Butcher 2009, 10).[xxii][22] Eventually, in 2009, the UK introduced secondary legislation transposing

thedirective's requirements in to UK law and set about creating port authorities (United Kingdom Parliament 2009).

There were also efforts to more effectively pool resources and to share best practice. 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 range of members of the policy network responsible for the security of UK ports. Developed and monitored by the National Co-ordinator Ports Policing (NCPP),[xxiii][23] and 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" (All from: Douglass in Shahbazian, Rogova and de Weert 2009, 33). Each ***portal 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 in the years after 1 July 2004. These debates were fuelled by a series of factors including historical alliances between various police forces, considerations of police force size and threat

perception. Looking at East Anglia, concerns were, for example, 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. 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 (Douglass in Shahbazian, Rogova and de Weert 2009).

C: Working Practices

While legislation and regulations with an emphasis on port security proliferated, new institutional structures emerged, and investments in additional infrastructure took place; the working practices of those operating in and around ports changed too. The threat narratives that facilitated the counter-terrorism security response witnessed in relation to UK ports were particularly evident in efforts to ***build security awareness*** in and around ports amongst staff and visitors alike. To some extent the expectation held by port managers was that 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 more proactive role was also taken to ensure the existing response was further institutionalised and increasingly became second

nature. References to security were visible throughout the ports studied, below is one example of a sign at one port visited.

Figure 1 – Security level sign[xxiv][24]

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 ISPS Code. This level determines the nature of security activities undertaken, such as the minimum percentage of port users who should be searched. The DfT sets the relevant security level for UK ports 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 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 preventingunauthorised 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.

Figure 2 – Port security poster[xxv][25]

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 in to 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 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

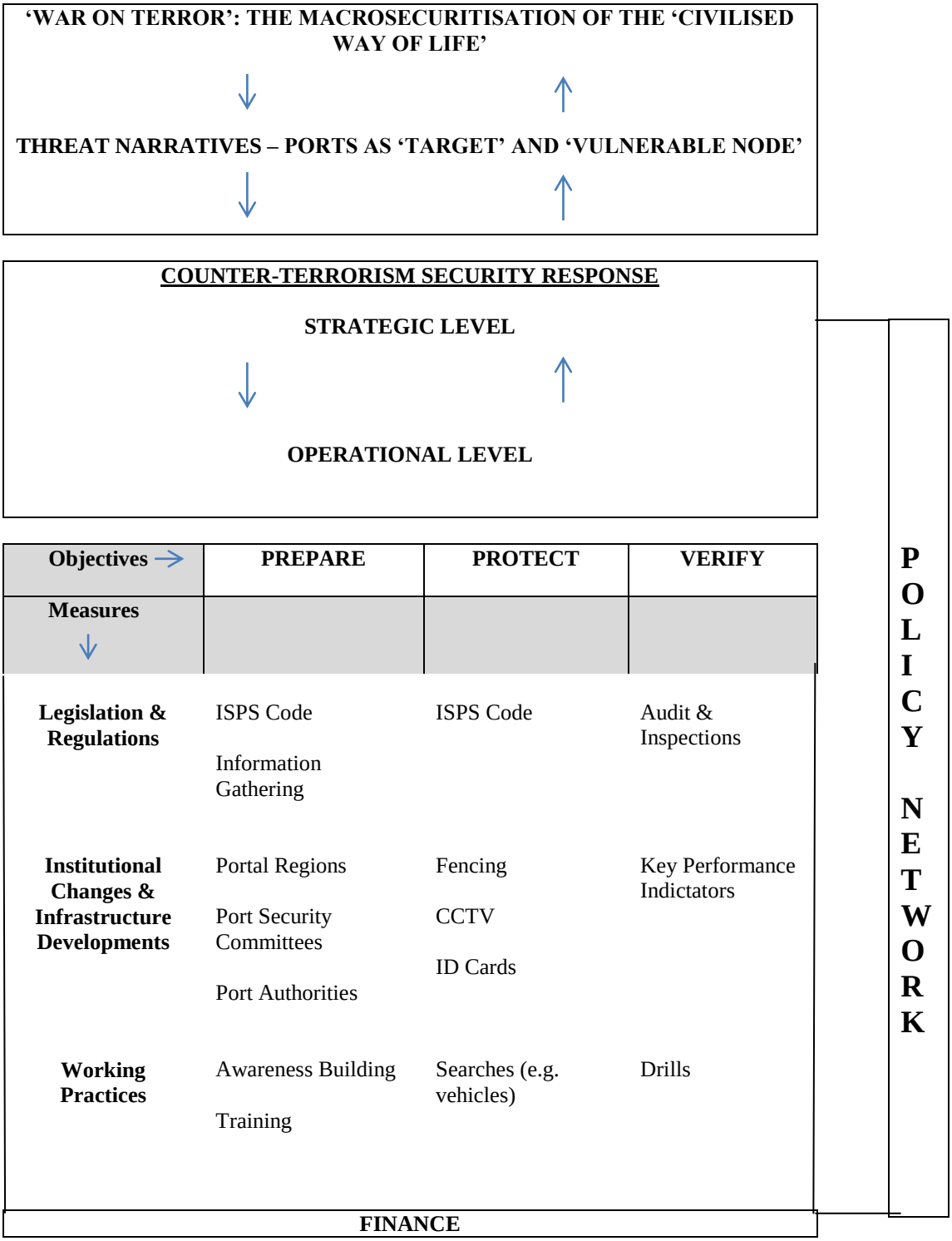
use of the one word ‘Suspicious’ with the affixed question mark provided an additional reminder that an inquisitive mind was what was sought.

For both security staff and port users ***regular searches***, specifically of vehicles, were one of the clearest manifestations of the securitisation of UK ports and an additional mechanism that security awareness was built. Conducting searches of vehicles coming from ferries in to the UK at Holyhead for example was predominantly the job of privately contracted security personnel who were tasked with looking for suspicious items. Across the ports visited great emphasis was placed on ensuring security staff were well prepared for their duties through the use of ***training and drills.*** 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” (Author’s Interview).

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” (International Maritime Organization 2003, 98, paragraph 18.4). 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” (Author’s Interview). 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. ***Key Performance Indicators (KPIs)*** were, for example, also utilised by the NCPP, with SB ports officers submitting information on a regular basis against these KPIs to the NCPP for auditing. The use of KPI’s was

by no means unique to ports policing, being a common practice across the maritime industry as a whole. One port manager was required by his superiors to submit information on a weekly basis in relation to his security staff's most recent operations.

Figure 3 – Typology of counter-terrorism practice[xxvi][26]



Emerging out of the empirical research undertaken, a typology of counter-terrorism practice is laid out helping to facilitate the highlighting of key characteristics and trends. The figure illustrates the way in which the 'war on terror' shaped the policy environment in which the different components of the counter-terrorism security response for UK ports became possible. At the operational level three main objectives being pursued by the policy network responsible for the counter-terrorism security response in UK ports can be located. First, those efforts to build awareness around the nature of the threat international terrorism was presented as posing and to ensure security readiness through training, were about preparing for all eventualities. Second, those measures pursued to strengthen the very fabric of the port and enhance awareness of activities taking place in and around it, such as the installation of fencing and CCTV, were about protecting the port from the terrorist threat. Third, the focus on compliance with legislation and regulations and the harmonisation of standards, encapsulated the desire to check the response was working and improving and rested on the understanding of the need for continual vigilance and no complacency with regards to the presented terrorist threat. To summarise even further, each of these three objectives can be captured in a single word - 'Prepare', 'Protect' and 'Verify' respectively.

Those measures discussed in this article and included in Figure 3 represent a snapshot of the totality of measures that could be witnessed, and of course all are underpinned by the need to finance their implementation on a day-to-day basis. What was also

evident in UK ports during this period, and is captured in the absence of dividing lines between the various measures in Figure 3, was that there was substantial overlap and mutually reinforcing relationships in play between the different objectives pursued and measures implemented to secure UK ports. Whilst CCTV cameras for example do serve a protective function flagging up potential active threats to the integrity of a port and its restricted zones, they also facilitate a checking function allowing the port to assess the behaviour of its personnel. The positioning of the policy network down the right side of the figure is designed to illustrate the multi-levelled governance in relation to UK port security evident, governance involving a range of state and non-state actors. The structure of the ISPS Code inspection regime or the EU's demand for statutory port authorities illustrate this clearly, reminding us once more that ports are part of a truly global maritime industry.

What is also clear is that not every security measure discussed in this article was initiated and designed with counter-terrorism exclusively in mind. The tri-partite role ports play asnodes in the global supply chain, hubs in the transport network, and as border management locations, ensured ports were rarely untouched by broader say, border security developments. Nevertheless the backdrop of the 'war on terror' cast a long shadow. The ISPS Code was a clear manifestation of this situation, a regulatory response pursued in the aftermath of 11 September 2001, shaping practice internationally. Furthermore, the roll out of inspection regimes, the creation of portal regions and the use of KPI's, also illustrates the rather mundane character of many measures implemented in UK ports.

Nevertheless, we should not underestimate the scale of change witnessed in UK ports in the years after 11 September 2001. It is very difficult to imagine such a counter-terrorism security response emerging without the backdrop of the 'war on terror'; the boundaries of what was regarded as necessary had clearly shifted. This situation reminds us that while a typology of practice can help us deconstruct the counter-terrorism security response to locate trends, re-aggregation to look at the complete whole is still required.

Conclusion: The spatial dimension to the securitisation of UK ports

With this re-aggregation in mind, three main characteristics of the counter-terrorism security response relating to UK ports can be highlighted. First, the counter-terrorism security response constantly evolved. 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. If we understand institutionalisation as the process of embedding particular activities, roles, even ideas in day-to-day operations so as they become like second nature, it was pursued prominently here via efforts to ensure universal compliance with emergency measures and the harmonisation and improvement of security standards. This institutionalisation had placed attention on enhancing security awareness and expanding security training seen with regards to the ISPS Code after 1 July 2004 for example.

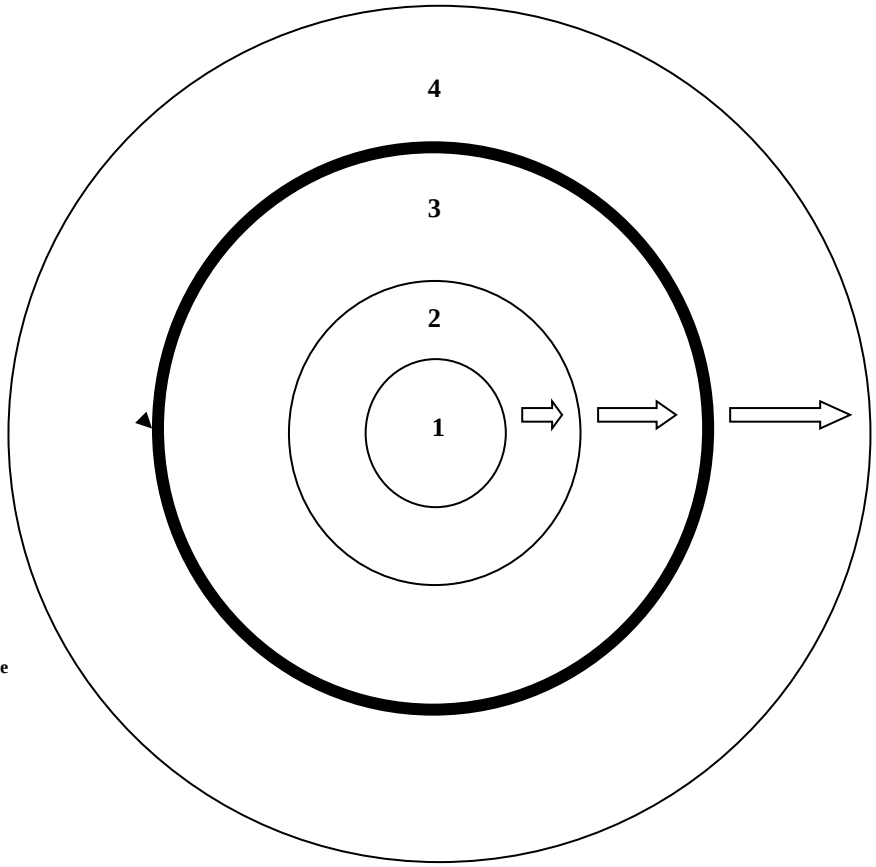
Second, the counter-terrorism security response was layered. This characteristic primarily emerged out a desire to ensure that if one element of the response failed to secure UK ports, another would be in place to tackle the presented terrorist threat. For example, while restricted zones around the port/ship interface could be seen, amongst other things, as being able to help prevent an attack on a ship whiledocked or prevent terrorists from gaining access to the entire port, other measures were taken here too. The EU designed 24-hr container manifest scheme for example 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 response was also layered in a more generic sense. If the security level in relation to UK ports varied so the security practices undertaken would vary. Moreover practice was shaped by a mixture of measures, some of which were developed with ports 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. The response was also layered in the way in which emergency measures were initiated at different levels of governance.

Third and finally the counter-terrorism security response was increasingly expansive in scope. This 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 ports. To illustrate, a senior port manager in the UK during the period 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' (European Union 2005) on enhancing port security for example ensured that an ISPS-style regime was introduced to the entire port. This spatial dimension would be a trend witnessed further as attention steadily focused on securing smaller harbours and even the coastline as a whole. Indeed with UK government schemes such as e-Borders and the associated focus on exporting the UK border, efforts to extend the zone of security further still were very evident. This spatial dimension is captured in the following figure, whilst also showing the layered characteristic of the response.

Figure 4 – The spatial dimension to the securitisation:[xxvii][27]



Key:
1 – Ship/Port Interface
2 – Port
3 – Coastline
4 – Beyond territorial borders.

The expanding circles represent the way in which the space that was deemed to require securing in relation to UK ports, harbours and coastline collectively, expanded. The arrows illustrate the general 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 the UK's maritime domain thus making it more difficult for it to be attacked or exploited by terrorists. What is evident in the new measures introduced since 1 July 2004 is that there was a self-perpetuating dynamic

to this process as an increase in security in one area was understood to increase the threat elsewhere. This dynamic in turn demanded that the space secured be further expanded and so forth.

Ultimately the central thread running through the counter-terrorism security response was the pursuit, particularly by the British state and port owners, for greater knowledge about, and through this control over, activities associated with UK ports. For the state this took place through institutions such as DfT staff and SB ports officers, while for port owners it was through senior management teams and their work. An investment in material capabilities such as new fencing and information technology systems coupled with the growth in the number of individuals with some responsibilities for, and awareness of security, provided the means through which behaviour within UK ports was more effectively managed, with movement determined by physical boundaries and desirable behaviour emphasised through a cohort of 'enlightened' individuals.[xxviii][28] The pursuit of enhanced port security did then leave UK ports as increasingly exclusive sites.

[ii] Italics added by author for emphasis. 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.

[ii] In this article 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.

[ii] The definition of maritime domain utilised in this article is taken from the UK's National Maritime Security Strategy (United Kingdom 2014, 54): "All areas and things of, under, to, or bordering on a sea or ocean including all maritime-related activities, infrastructure, people, cargo, ships and other conveyances".

[ii] The three strategies are all available online and are listed in the article's bibliography.

[ii] For example, in his address to the nation on 11 September 2001 President George W. Bush presented the terrorist attacks as an attack "on our fellow citizens" and "on our way of life, our very freedom", immediately projecting outwards their significance (CNN.com US, 2001). A few days later UK Prime Minister Tony Blair would say in the House of Commons: "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" (Blair, 2001). At the October 2001 UK Labour Party Conference, the Foreign Secretary Jack Straw would comment, "there are some who wish completely to destroy our values and our way of life" (Guardian Online, 2 October 2001).

[ii] Rita Taureck notes in, 'Securitisation Theory – The Story so far: Theoretical inheritance and what it means to be a post-structural realist', (unpublished paper presented at the 4th annual CEEISA convention, University of Tartu, 25-27th June 2006), that the theory has its roots in language theory. In particular, this performative function was originally set out in Austin, J.L. (1962) *How to do things with words* (Oxford: Clarendon Press), 110, note 2.

[ii] This is a point advanced in Buzan and Waever, 2009, 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".

[ii] This kind of analysis on responses to international terrorism can be seen in Silberstein, S. (2004) *War of Words: language, politics and 9/11* (London: Routledge) and Jackson, R. (2005) *Writing the war on terrorism: language, politics, and counter-terrorism* (Manchester: Manchester University Press). More generally in relation to US foreign policy it is undertaken by Campbell, D. (1998) *Writing Security.*

[ii] Richard Jackson includes a copy of a number of speeches from the Bush administration in the appendix to Jackson, R. (2005) *Writing the war on terrorism.*

[ii] The idea of securitisations being institutionalised is also discussed on page 28 in Buzan, B., Waever, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis*. An examination of how the discourse has been reproduced by the media and other institutions in society, further institutionalising it, can be found in Schechter, D. (2003) *Media Wars: News at a Time of Terror* (Oxford: Rowland & Littlefield); Lewis, J. (2005) *Language Wars: The role of Media and Culture in Global Terror and Political Violence* (London: Pluto Press) and Croft, S. (2006) *Culture, Crisis and America's War on Terror* (Cambridge: Cambridge University Press).

[ii] 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.

[ii] The phrase 'site of securitisation' has also been utilised in Arne Davidsen, P. (2006) 'The Making and Unmaking of the Politics of Exceptionality: Studying Processes of Securitisation and Desecuritisation in the Orange and Okavango River Basins' (Master's Dissertation, University of Bergen, 2006) and Copper Luiss-Cersdu, D. (2009) 'Gender Conflict Society and Human Rights: SHUR Findings', 4-6 June. (Presentation at SHUR Final Conference, Rome).

[ii] For example International Maritime Organization (2004b) 'Press Release: ISPS Code Status Update 01', 11 June 2004.

[ii] The ship-port interface is 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 to or from the ship" (IMO 2003, 113).

[ii] During 2006 and 2007 there was disagreement in the United States (US) over whether all containers bound for the US should be scanned prior to their departure. 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 weapon into this country – yet this Administration has been content to let 95 percent of the shipping containers we receive go uninspected" (Office of Congressman Jerrold Nadler 2006). Ultimately a compromise was reached with the passing 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 (Act available online: see bibliography).

[ii] An initial report highlighting possible delays was Justin Stares: (Lloyd's List 2008, 3). The European Commission introduced a regulation laying down 1 January 2011 as the point at which the rule would be mandatory. See European Commission (2009) 'Commission Regulation (EC) No 273/2009 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code, derogating from certain provisions of Commission Regulation (EEC) No 2454/93', *Official Journal of the European Union*, 2 April.

[ii] The reference to US inspectors related to the presence of some US customs officials within European ports as part of the US Container Security Initiative (CSI).

[ii] The fact that the Department for Transport 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. See: House of Commons Transport Committee (2008) *Transport Security: Travelling without Fear (Oral and Written Evidence).*

[ii] Further information about the RHIDES system can be found at the website: http://www.rhides.com/.

[ii] Italics added by author for emphasis.

[ii] Also see an article utilised in the Library report: Infrasite.net (2008) 'EC: Port security: Estonia, UK late with transposing Community rules', *Infrasite.net*.

[ii] The NCPP was an office funded by the Home Office through the Association of Chief Police Officers Council Committee on Terrorism and Allied Matters (ACPO(TAM)). The NCPP had expanded its role in 2003 from co-ordinating Special Branch activity in UK ports to include the ACPO(Ports) portfolio that encapsulated those protective services in ports provided by uniformed officers.

[ii] Image 1 – 'Security Level Sign', taken by author on site visit.

[ii] Image 2 – 'Port Security Poster', taken by author on site visit. Contact phone number removed by author for the purposes of anonymity.

[ii] Designed by author.

[ii] Designed by author.

[ii] The idea that a wide range of individuals, including those who do not have security responsibilities as part of their day-to-day job, should nevertheless become more security aware and active is something discussed elsewhere. See: Malcolm 2013.

Bibliography

African Union (2014) '2050 Africa's Integrated Maritime Strategy', Adopted January. Available online at: http://pages.au.int/maritime/documents/2050-aim-strategy-0

Arne Davidsen, P. (2006) 'The Making and Unmaking of the Politics of Exceptionality: Studying Processes of Securitisation and Desecuritisation in the Orange and Okavango River Basins' (Master's Dissertation, University of Bergen, 2006). Available online at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.112.6567&rep=rep1&type=pdf

Austin, J.L. (1962) *How to do things with words* (Oxford: Clarendon Press).
Bormann, N. and Sheehan, M. (eds.) (2009) *Securing Outer Space* (London; New York: Routledge).

Blair, Tony. (4 October 2001) 'Coalition against International Terrorism', House of Commons, Hansard column 675. Available online at: http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo011004/debtext/11004-01.htm#11004-01_spmin0.

Bueger, C (2015) 'What is Maritime Security?', *Marine Policy*, 53, 159-164.

Butcher, L. (2009), 'Ports: Security', *House of Commons Library*, last updated 15 June. Available online at: http://www.parliament.uk/briefingpapers/commons/lib/research/briefings/snbt-03106.pdf

Buzan, B. and Waever, O. (2009) 'Macrosecuritisation and security constellations: reconsidering scale in securitisation theory', *Review of International Studies*, 35:2, 253-276.

Buzan, B., Waever, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis* (Boulder, Colorado: Lynne Rienner).

Campbell, D. (1998) *Writing Security* (Manchester: Manchester University Press).

CNN.com US (2001) 'Text of Bush's Address' 11 September. Available online at: http://articles.cnn.com/2001-09-11/us/bush.speech.text_1_attacks-deadly-terrorist-acts-despicable-acts?_s=PM:US

Copper Luiss-Cersdu, D. (2009) 'Gender Conflict Society and Human Rights: SHUR Findings', 4-6 June. (Presentation at SHUR Final Conference, Rome). Available online at: http://shur.luiss.it/files/2009/05/copper.pdf

Croft, S. (2006) *Culture, Crisis and America's War on Terror* (Cambridge: Cambridge University Press).

Douglass, J. (2009) 'Police National Maritime Security Strategy', in Elisa Shahbazian, Galina Rogova and Michael J. de Weert (eds.), *Harbour Protection Through Data Fusion Technologies* (Dordrecht, The Netherlands: Springer).

European Commission (2004) 'Regulation (EC) No 725/2004 of the European Parliament and of the Council on enhancing ship and port facility security', *Official Journal of the European Union*, 31 March. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:EN:PDF

European Commission (2005) 'Commission Regulation (EC) No 884/2005 laying down procedures for conducting Commission inspections in the field of maritime security', *Official Journal of the European Union,* 10 June. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:148:0025:0029:EN:PDF

European Commission (2009) 'Commission Regulation (EC) No 273/2009 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code, derogating from certain provisions of Commission Regulation (EEC) No 2454/93', *Official Journal of the European Union,* 2 April. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:091:0014:0015:EN:PDF

European Union (2005) 'Directive 2005/65/EC of the European Parliament and of the Council on enhancing port security', *Official Journal of the European Union,* 26 October. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:0039:EN:PDF

European Union (2014) 'European Union Maritime Security Strategy', Published 24 June. Available online at: http://ec.europa.eu/maritimeaffairs/policy/maritime-security/index_en.htm

Guardian Online (2001) 'Full Text: Straw's Speech'. Available online at: http://www.guardian.co.uk/politics/2001/oct/02/labourconference.labour2.

Hansen, L. (2006) *Security as Practice: Discourse Analysis and the Bosnian War* (Abbingdon, Oxford, England: Routledge).

House of Commons Transport Committee (2008) *Transport Security: Travelling without Fear (Oral and Written Evidence)* (London: The Stationery Office Ltd).

Available online at:
http://www.publications.parliament.uk/pa/cm200708/cmselect/cmtran/191/191we01.htm

Infrasite.net (2008) 'EC: Port security: Estonia, UK late with transposing Community rules', *Infrasite.net*, last updated 18 September. Available online at:
http://www.infrasite.net/news/news_article.php?ID_nieuwsberichten=10455&language=en

'IMO: Frequently Asked Questions' (n.d), *IMO website,* accessed 8 February 2008, www.imo.org/Newsroom/mainframe.asp?topic_id=897.

International Maritime Organization (2001) 'Address by Mr David Jamieson MP (A 22/INF.7)', *22nd Regular Session of the IMO Assembly*, 19 November.

International Maritime Organization (2002a) 'Opening Address by Mr W.A O'Neil (SOLAS/CONF.5/INF.4)', *Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974*, 9 December.

International Maritime Organization (2002b) 'Address by Admiral Thomas H. Collins (SOLAS/CONF.5/INF/5)', *Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974*, 9 December.

International Maritime Organization (2003) *International Ship and Port Facility (ISPS) Code* (London: International Maritime Organization).

International Maritime Organization (2004a) 'Opening Address by Mr Efthimios Mitropoulos', *12th session of the sub-committee on Flag State Implementation*, March.

International Maritime Organization (2004b) 'Press Release: ISPS Code Status Update 01', 11 June 2004. Available online at:
http://www5.imo.org/SharePoint/mainframe.asp?topic_id=892&doc_id=3650

Jackson, R. (2005) *Writing the war on terrorism: language, politics, and counter-terrorism* (Manchester: Manchester University Press).

Lewis, J. (2005) *Language Wars: The role of Media and Culture in Global Terror and Political Violence* (London: Pluto Press).

Malcolm, J.A. (2013) 'Project Argus and the Resilient Citizen' *Politics,* 33:4, 311-321.

Office of Congressman Jerrold Nadler (2006) 'Press Release: Transportation Committee Passes Nadler-Oberstar Amendment to Scan 100% of Shipping Containers', *Congress Jerrold Nadler's official website*, 4 April. Available at:
http://nadler.house.gov/press-release/transportation-committee-passes-nadler-oberstar-amendment-scan-100-shipping-containers

O'Neil, W.A. (2001) 'The work programme of the International Maritime Organization', *Conference on Safety in Maritime Transport, La Coruna (Spain)*, 17-18 September. Available online at:
http://www.imo.org/Newsroom/mainframe.asp?topic_id=82&doc_id=1426

Security and Accountability for Every Port Act (2006), signed in to law 13 October. Available online at: http://www.gpo.gov/fdsys/pkg/PLAW-109publ347/content-detail.html

Schechter, D. (2003) *Media Wars: News at a Time of Terror* (Oxford: Rowland & Littlefield).

Silberstein, S. (2004) *War of Words: language, politics and 9/11* (London: Routledge).

Stares, J. (2005) 'Port inspectors plan starts row with EU member states', *Lloyd's List*, 8 April.

Stares, J. (2008) 'EU cargo security rules may miss 2009 deadline', *Lloyd's List,* 20 June.

Taureck, R. (2006) 'Securitisation Theory – The Story so far: Theoretical inheritance and what it means to be a post-structural realist', 25-27 June. (Unpublished paper presented at the 4th annual CEEISA convention, University of Tartu).

United Kingdom (2014) 'The UK National Strategy for Maritime Security', Published 13 May. Available online at: https://www.gov.uk/government/publications/national-strategy-for-maritime-security

United Kingdom Parliament (2009) 'The Port Security Regulations 2009', laid before Parliament 24 July. Available online at, http://www.legislation.gov.uk/uksi/2009/2048/introduction/made

Waever, O. (1995) 'Securitization and Desecuritization' in R.D. Lipschultz (ed.), *On Security* (New York: Columbia Press).