

This electronic thesis or dissertation has been downloaded from the King's Research Portal at <https://kclpure.kcl.ac.uk/portal/>



A UK 'security-industrial complex'?

**A reassessment of the origins, characteristics, and consequences of private sector involvement in the counter-terrorism aspects of contemporary UK national security strategy**

Rosemont, Hugo David

*Awarding institution:*  
King's College London

The copyright of this thesis rests with the author and no quotation from it or information derived from it may be published without proper acknowledgement.

#### END USER LICENCE AGREEMENT



Unless another licence is stated on the immediately following page this work is licensed

under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International

licence. <https://creativecommons.org/licenses/by-nc-nd/4.0/>

You are free to copy, distribute and transmit the work

Under the following conditions:

- Attribution: You must attribute the work in the manner specified by the author (but not in any way that suggests that they endorse you or your use of the work).
- Non Commercial: You may not use this work for commercial purposes.
- No Derivative Works - You may not alter, transform, or build upon this work.

Any of these conditions can be waived if you receive permission from the author. Your fair dealings and other rights are in no way affected by the above.

#### Take down policy

If you believe that this document breaches copyright please contact [librarypure@kcl.ac.uk](mailto:librarypure@kcl.ac.uk) providing details, and we will remove access to the work immediately and investigate your claim.

**A UK 'security-industrial complex'?**

**A reassessment of the origins, characteristics, and consequences of private sector involvement in the counter-terrorism aspects of contemporary UK national security strategy**

by

**Hugo David Rosemont**

**Thesis submitted in fulfilment of the requirements of the degree of  
Doctor of Philosophy**

**Department of War Studies  
Faculty of Social Science and Public Policy  
King's College, London**

## ABSTRACT

An argument has arisen that a 'security-industrial complex' (SIC) exists in, and is damaging to, the United Kingdom. The oft-repeated assessment is that, like the 'military-industrial complex' (MIC) which existed before (and continues to operate alongside) it, a damaging system of public-private sector interaction has emerged in the non-military aspects of national security strategy. Critics portray the purported system - the SIC - as an organised alliance of self-interested government and profit-making entities that exploits the security environment for its own gain.

The suitability of using 'SIC' terminology is untested within security studies, however. This thesis reassesses how to conceptualise the public-private sector cooperation that has arisen in the contemporary security environment by analysing the origins, characteristics and consequences of the private sector's involvement in the domestic counter-terrorism (CT) aspects of contemporary UK national security strategy following the terrorist attacks on the US on 11 September 2001. It demonstrates through reference to existing theory on the MIC, original interviews, and analysis of certain contracts and other case studies concerning companies' involvement in the UK Government's CT strategy that, instead of replicating the MIC in the new security context exactly, a more nuanced system of public-private interaction has arisen. Whilst some of the dynamics associated with the MIC exist in the CT sector, this thesis questions whether the aggregation of these dynamics in the CT field should be understood and presented in the same way.

A lack of systemic scholarly research on 'the SIC' in the UK has hindered the development of policy-making and debate in respect of the private sector's involvement in the non-military aspects of national security. The thesis seeks to address this gap, making an original, policy-orientated contribution, which aims to stimulate informed discussion and policy improvements in the field.

## Table of Contents

<b>Abstract</b> .....	2
<b>Table of Contents</b> .....	3
<b>Index of Figures</b> .....	5
<b>Abbreviations</b> .....	6
<b>Acknowledgments</b> .....	9
<b>Chapter 1: Introduction and Methodology</b> .....	10
1.1 Introduction to the thesis.....	10
1.2 Justification for research into ‘the SIC’.....	17
1.3 Contextualisation within existing academic literature and debates....	19
1.4 A reassessment of the UK ‘security-industrial complex’.....	31
1.5 Research Questions.....	34
1.6 The scope of the thesis.....	36
1.7 Framework for analysis.....	42
1.8 Structure of the thesis and case study selection.....	47
1.9 Potential limitations arising from case study selection.....	55
1.10 Sources and methodology.....	56
<b>Chapter 2: The MIC and its evolution in a UK context</b> .....	59
2.1 Introducing the ‘MIC’ - concept and theory.....	59
2.2 Origins of the MIC Concept.....	64
2.3 An American expression?.....	69
2.4 A ‘pejorative’ term? Contrasting attitudes on the MIC.....	75
2.5 Coverage of the British MIC.....	78
2.6 Changing character of the British MIC.....	82
2.7 Towards a theory on the ‘industrial-complex’ in CT, and beyond.....	84
<b>Chapter 3: Emergency Preparedness</b> .....	89
3.1 Government policy approach and governance arrangements.....	92
3.2 Security expenditure.....	102
3.3 Public-private security interactions.....	106
- Suppliers (FiReControl Case Study).....	106
- Private Operators.....	124
- Wider Business.....	128
3.4 Character and impact of the ‘industrial-complex’ in sub-sector.....	131
<b>Chapter 4: Border Security</b> .....	135
4.1 Government policy approach and governance arrangements.....	137
4.2 Security expenditure.....	143
4.3 Public-private security interactions.....	146
- Suppliers and Private Operators (e-Borders Case Study).....	146
4.4 Character and impact of the ‘industrial-complex’ in sub-sector.....	168

<b>Chapter 5: Olympic Security</b> .....	171
5.1 Government policy approach and governance arrangements.....	174
5.2 Security expenditure.....	176
5.3 Public-private security interactions.....	179
- Suppliers (G4S security contract Case Study).....	180
- Private Operators.....	201
- Wider Business.....	204
5.4 Character and impact of the ‘industrial-complex’ in sub-sector.....	208
<b>Chapter 6: Strategic Engagement</b> .....	214
6.1 Origins of cooperation.....	216
6.2 Inappropriate Foundations?.....	223
6.3 From JNSRAC to RISC.....	228
6.4 An Effective Mechanism?.....	231
6.5 Origins and character of strategic engagement through RISC.....	244
<b>Chapter 7: Wider issues of concern</b> .....	246
7.1 The ‘Revolving Door’.....	247
7.2 Economic Emphasis – Procurement and Employment.....	262
7.3 Non-military, CT-related exports.....	271
7.4 Character and impact of the ‘industrial-complex’ in wider areas.....	284
<b>Chapter 8: Conclusion</b> .....	286
8.1 Origins.....	286
8.2 Characteristics.....	289
8.3 Consequences.....	301
8.4 Concluding remarks.....	309
<b>Appendix A: Interview Participants</b> .....	313
<b>Appendix B: Interview Process</b> .....	315
<b>Appendix C: About the Author</b> .....	319
<b>Bibliography</b> .....	320
Primary Material.....	320
Later Works.....	352

## Index of Figures

Figure 1: Framework for analysing private sector involvement in CONTEST .....	55
Figure 2: The 'Classic' MIC.....	67
Figure 3: CCS Spending 2008-2012.....	102
Figure 4: The exchange of data in the e-Borders programme.....	168
Figure 5: The industrial-complex in the CT aspects of UK national security strategy.....	297
Figure 6: A multitude of security-industrial complexes? .....	300

## Abbreviations

<b>ACBA</b>	Advisory Committee on Business Appointments
<b>AQ</b>	Al-Qaeda / Al Qaida
<b>BBC</b>	British Broadcasting Corporation
<b>BSIA</b>	British Security Industry Association
<b>BtG</b>	Bridging the Gap
<b>CAAT</b>	Campaign Against the Arms Trade
<b>CAST</b>	Centre for Applied Science and Technology
<b>CBI</b>	Confederation of British Industry
<b>CCA</b>	2004 Civil Contingencies Act
<b>CCS</b>	Civil Contingencies Secretariat
<b>CLG</b>	Communities and Local Government Committee (UK Parliament)
<b>CLM</b>	Consortium comprising CH2MHILL, Lang O'Rourke and Mace
<b>CNI</b>	Critical National Infrastructure
<b>COBR</b>	Cabinet Office Briefing Rooms
<b>CONTEST</b>	UK Government's Strategy for Countering Terrorism
<b>CPNI</b>	Centre for the Protection of National Infrastructure
<b>CSSC</b>	Cross-Sector Safety and Security Communications Project
<b>CT</b>	Counter-terrorism
<b>DCLG</b>	Department for Communities and Local Government
<b>DCMS</b>	Department for Culture, Media and Sport
<b>DE&amp;S</b>	Defence Equipment and Support
<b>DESO</b>	Defence Export Service Organisation
<b>DIB</b>	Defence Industrial Base
<b>DMA</b>	Defence Manufacturers Association
<b>DSO</b>	UKTI Defence and Security Organisation
<b>DSTL</b>	Defence Science and Technology Laboratory

<b>EU</b>	European Union
<b>FBU</b>	Fire Brigades Union
<b>FRSs</b>	Fire and Rescue Services
<b>G2G</b>	Government-to-Government (Export Arrangements)
<b>GCHQ</b>	Government Communications Headquarters
<b>GOCO</b>	Government-Owned Contractor-Operated
<b>HASC</b>	Home Affairs Select Committee (UK Parliament)
<b>HMRC</b>	HM Revenue and Customs
<b>IAG</b>	Industry Advisory Group
<b>ICT</b>	Information and Communication Technology
<b>IND</b>	Immigration and Nationality Directorate
<b>IOC</b>	International Olympic Committee
<b>IT</b>	Information Technology
<b>JNSRAC</b>	Joint National Security and Resilience Advisory Council
<b>LCIA</b>	London Court of International Arbitration
<b>LFB</b>	London Fire Brigade
<b>LOCOG</b>	London Organising Committee for Olympic Games and Paralympic Games
<b>MI5</b>	Security Service
<b>MI6</b>	Secret Intelligence Service
<b>MIC</b>	Military-industrial Complex
<b>MOD</b>	Ministry of Defence
<b>MPS</b>	Metropolitan Police Service
<b>NaCTSO</b>	National Counter Terrorism Police Office
<b>NAO</b>	National Audit Office
<b>NRR</b>	National Risk Register
<b>NSS</b>	National Security Strategy of the UK
<b>NSST</b>	National Security Through Technology



<b>ODA</b>	Olympic Delivery Authority
<b>OGC</b>	Office of Government Commerce
<b>OGDs</b>	Other Government Departments
<b>OSCT</b>	Office for Security and Counter-Terrorism
<b>OSD</b>	Olympic Security Directorate
<b>PAC</b>	Committee of Public Accounts (also known as Public Accounts Committee)
<b>PMSCs</b>	Private Military and Security Companies
<b>PMSRG</b>	Private Military and Security Research Group (King's College, London)
<b>RCC</b>	Regional Control Centre
<b>RISC</b>	UK Security and Resilience Industry Supplier's Community
<b>RUSI</b>	Royal United Services Institute
<b>SBAC</b>	Society of British Aerospace Companies
<b>SIC</b>	Security-industrial Complex
<b>SIET</b>	Security Industry Engagement Team
<b>SDSR</b>	Strategic Defence and Security Review
<b>SRO</b>	Senior Responsible Owner
<b>SSAG</b>	UKTI Security Sector Advisory Group
<b>TI</b>	Transparency International
<b>UK</b>	United Kingdom
<b>UKBA</b>	United Kingdom Border Agency
<b>UKTI</b>	United Kingdom Trade & Investment
<b>US</b>	United States

## **Acknowledgements**

I am indebted to all of the interviewees who devoted their time to participate in the research. Amongst them, I am particularly grateful to John Backhouse, Stephen Phipson, John Howe and Derek Marshall for their early support, encouragement, and ongoing participation.

I sincerely thank Smiths Detection for their interest in my work throughout the course of the project, and for so generously providing me with a scholarship that allowed for its completion.

I was deeply honoured that the late Professor Paul Wilkinson of the University of St. Andrews supported my application to complete the research; I regret that I will not be able to discuss this thesis with him, but offer my analysis in his memory.

Thank you to my academic colleagues who have helped or inspired me to complete the research; especially Philip Bobbitt, Mervyn Frost, John Horgan, John Morrison, Chris Kinsey, Birthe Anders, Ali Hawks and Mark Erbel.

I offer huge and very special thanks to my supervisors for their constant encouragement throughout the course of my doctoral research. It has been an honour and privilege to have benefited from the advice of Professor Ken Young and especially my Primary Supervisor, Professor John Gearson. I am indebted and extremely grateful to them both for their patience and support.

My family and friends on both sides of the Atlantic have offered me huge encouragement. I am very grateful to all of them for their interest in my endeavours, and wish to pay special thanks to Beth and Reilly Lewis, Dana and Tom Giardina, Nick and Caroline Van Wagoner, David and Daliah Rosemont, Jonny and Lucy Rosemont, and Abbey and Stephen Wright in particular for their kind and generous support of my efforts.

Above all, I wish to thank my wife, Helen, who has encouraged and supported me every step of the way during the course of my research. It is not an exaggeration to say that without her loving support, patience and confidence in me, this project would not have been attempted or completed.

**HDR**

**18.i.15**

## Chapter 1: Introduction and Methodology

### 1.1 Introduction to the thesis

The system known as the 'military-industrial complex' (MIC) - an expression famously introduced by US President Dwight D. Eisenhower in 1961 - is said to have undergone 'a considerable amount of restructuring'<sup>1</sup>, if not a major transformation since the end of the Cold War.<sup>2</sup> Contemporary theorists on the evolving character of the MIC including Dunne and Sköns, for example, have introduced the idea that the MIC has been deeply affected by changes arising in the 'new' post-Cold War security environment; these authors were pioneers in highlighting that different types of public and private interests were coalescing around contemporary security issues.<sup>3</sup> As a recent article put it; '...we are (...) witnessing the emergence of a new security-industrial complex that should be received with the same caution as that which Eisenhower sought to convey about the military-industrial complex in the 1960s.'<sup>4</sup>

Therefore an argument has arisen - and been advanced most notably by scholars associated with the school of critical security studies - that, particularly after 9/11, the negative dynamics that critics have associated with the MIC have emerged within 'new' non-military security sectors.<sup>5</sup> Most prominently, Neocleous has identified what he refers

---

<sup>1</sup> J Paul Dunne, 'The Changing Military Industrial Complex in the UK', *Defence Economics*, Vol.4 (1993), p.91

<sup>2</sup> As suggested in J Paul Dunne and Elisabeth Sköns, 'The Changing Military Industrial Complex', Economics Discussion Paper Series, School of Economics, University of the West Of England, March 2011, Via: <http://carecon.org.uk/DPs/1104.pdf> (accessed 01.06.11). Chapter 2 examines the origins of, and theory on the MIC.

<sup>3</sup> Their first paper highlighting these developments was J Paul Dunne and Elisabeth Sköns, 'The Military Industrial Complex', Economics Discussion Paper Series, School of Economics, University of the West of England, May 2009, Via: <http://carecon.org.uk/DPs/0907.pdf> (accessed 10.11.14). See also *ibid.*, p.7

<sup>4</sup> Richard Godfrey, Jo Brewis, Jo Grady and Chris Grocott, 'The private military industry and neoliberal imperialism: Mapping the terrain', *Organization*, Vol.21:1 (2014), p.119

<sup>5</sup> Critical security studies encompasses a large body of literature; for an introduction to the approach and work of this school, see Keith Krause and Michael C. Williams (Eds.), *Critical Security Studies: Concepts and Cases* (London: UCL Press, 1997)

to as ‘the deadly *complicity* between security and capital’<sup>6</sup>, documenting what he argues amounts to harmful interaction arising between government and the private sector in the ‘war on terror’:

To make a profit, the security industry must sell security. And to sell security, it must first help generate insecurities. In so doing, it reiterates the central logic around which the national security state is organized: that citizens need to be afraid, and need the state to secure them.<sup>7</sup>

The idea (if not accusation), then, is that, much like the MIC, governments and the private sector (amongst others) have inflated threats arising from the new security context and (deliberately or inadvertently) colluded to mutually profit from them.<sup>8</sup> In short, the proposition is that, particularly in the context of the increased Western attention being paid to non-military security issues such as terrorism, something resembling a ‘security-industrial complex’ (SIC) has emerged in the UK and other allied countries.<sup>9</sup>

At the theoretical level, the idea of the emergence of an ‘industrial-complex’ in the security sector has developed further recently with the contention that the MIC may have actually been *superseded* by a broader, all-encompassing system. According to two scholars; ‘...the ‘military-industrial-complex’ and other related ‘industrial complexes’, are parts of an overarching ‘security-industrial-complex’.<sup>10</sup> Whilst this thesis will argue that

---

<sup>6</sup> Mark Neocleous, ‘Security, Commodity, Fetishism’, *Critique: Journal of Socialist Theory*, Vol.35:3 (2007), p.341 (Emphasis in original)

<sup>7</sup> Neocleous, ‘Security, Commodity, Fetishism’, p.350

<sup>8</sup> Mueller calls this coalition of interests ‘the terrorism industry’. John Mueller, ‘The Terrorism Industry: The Profits of Doom’, in George Kassimeris (Ed.), *Playing Politics with Terrorism: A User’s Guide* (New York: Columbia University Press, 2008), pp.301-320

<sup>9</sup> This is the argument and terminology advanced most notably in Hughes’s disapproving analysis of companies’ involvement in the ‘War on Terror’. Solomon Hughes, *War on Terror, Inc.: Corporate Profiteering from the Politics of Fear* (London: Verso, 2007). This terminology and line of argumentation also appears in Robert P. Weiss, ‘From Cowboy Detectives to Soldiers of Fortune: Private Security Contracting and Its Contradictions on the New Frontiers of Capitalist Expansion’, *Social Justice*, Vol.34:3/4 (2007), pp.1-19

<sup>10</sup> This argument appears in the abstract of a paper titled ‘The Emergence of the Security-Industrial Complex’ by Baker-Beall and Robinson at ‘Neoliberalism and/as Terror: Critical Studies on Terrorism Annual Conference 2014’, *Full Program*, Via: [http://www.leejarvis.com/wp-content/uploads/2011/11/Neoliberalism-and\\_as-terror-2014.pdf](http://www.leejarvis.com/wp-content/uploads/2011/11/Neoliberalism-and_as-terror-2014.pdf) (accessed 10.11.14). See also Barry’s earlier argument that the MIC has evolved into a ‘National Security Complex’: The ‘...“military-industrial complex” no longer adequately describes the multi-headed monster that has

the application of SIC-type terminology in exactly the same way as the MIC has been used does not sufficiently capture the complexity of the public-private dynamics at play in the counter-terrorism (CT) arena, this conceptualisation might add some value in the sense that - at least in theory - it could help to provide a new way of thinking about the growing list of security-related 'industrial complexes' that several authors have posited now exist.<sup>11</sup>

Outside the academic community, over a dozen media reports, accounts from investigative journalists and political opinion pieces have suggested that a SIC has emerged, or more simply that the dynamics associated with the MIC have extended to non-military aspects of national security such as CT.<sup>12</sup> Many such accounts provide few

---

emerged in our times'. Tom Barry, 'Synergy in Security: The Rise of the National Security Complex', *Dollars & Sense: Real World Economics* (March/April 2010), Via:

<http://www.dollarsandsense.org/archives/2010/0310barry.html> (accessed 19.05.11).

<sup>11</sup> Shorrock has identified an 'intelligence-industrial complex', for example, arguing that '[t]he analogy between the intelligence industry and the military-industrial complex described by President Eisenhower in 1961 is fitting.' Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing* (London: Simon & Schuster, 2008), p.12-13. Risen refers to a 'Homeland Security-Industrial Complex' in James Risen, *Pay any Price: Greed, Power, and Endless War* (New York: Harcourt Publishing, 2014).

<sup>12</sup> In addition to Barry, 'Synergy in Security', Shorrock, *Spies for Hire*, Risen, *Pay any Price*, and Hughes, *War on Terror, Inc.*, see especially: Paul Harris, 'How private firms have cashed in on the climate of fear since 9/11', *theguardian.com*, 5 September 2011, Via: <http://www.theguardian.com/world/2011/sep/05/private-firms-fear-9-11> (accessed 12.11.14); Louis Uchitelle and John Markoff, 'Terrorbusters Inc.', *New York Times*, 17 October 2004, Via: [http://www.nytimes.com/2004/10/17/business/yourmoney/17home.html?\\_r=0](http://www.nytimes.com/2004/10/17/business/yourmoney/17home.html?_r=0) (accessed 12.11.14); Linda Danil, 'The arms trade and the military-industrial complex: a UK perspective', *Critical Legal Thinking Blog*, 20 July 2012, Via: <http://criticallegalthinking.com/2012/07/30/the-arms-trade-and-the-military-industrial-complex/> (accessed 12.11.14); Aminata Kone, 'The Military-Industrial Complex in the United States: Evolution and Expansion from World War II to the War on Terror', *Student Pulse*, Vol.5:8 (2013), Via: <http://www.studentpulse.com/articles/749/the-military-industrial-complex-in-the-united-states-evolution-and-expansion-from-world-war-ii-to-the-war-on-terror> (accessed 12.11.14); Jonathan Turley, 'Big money behind the military-industrial complex', *Al Jazeera*, 11 January 2014, Via: <http://www.aljazeera.com/indepth/opinion/2014/01/big-money-behind-war-military-industrial-complex-20141473026736533.html> (accessed 12.11.14); Simon Jenkins, 'If the MoD can't name the enemy, it shouldn't buy the weapons', *theguardian.com*, 16 January 2014, Via: <http://www.theguardian.com/commentisfree/2014/jan/16/mod-cant-name-enemy-shouldnt-buy-weapons-threat-cold-war-defence> (accessed 12.11.14); Simon Jenkins, 'Oh! What a Lovely War on Terror - it's the number the arms dealers love', *theguardian.com*, 14 September 2007, Via: <http://www.theguardian.com/commentisfree/2007/sep/14/comment.politics> (accessed 12.11.14); Solomon Hughes, 'Shining A Light On Raytheon', *The People's Daily Morning Star*, 22 November 2013, Via: <http://www.morningstaronline.co.uk/a-b0f3-Shining-a-light-on-Raytheon> (accessed 12.11.14); David Rohde, 'The Security-Industrial Complex', *The Atlantic*, 15 June 2013, Via: <http://www.theatlantic.com/politics/archive/2013/06/the-security-industrial-complex/276906/> (accessed 12.11.14); Edward Luce, 'Data intelligence complex is the real story', *Financial Times*, 7 June 2014, Via: <http://www.ft.com/cms/s/0/a1dd626c-cf80-11e2-be7b->

references and resort to generalised statements on the supposedly corrosive character of this system; some, such as the work of Solomon Hughes, provide fuller (and more critical) analysis of what is seen as a highly damaging SIC in the UK.<sup>13</sup> In the US context, James Risen and Tim Shorrock have been amongst the most vocal critics to detail the same phenomenon.<sup>14</sup>

The presentation of 'the SIC' as the emergence of a detrimental system of public-private interaction around contemporary security issues can be seen to have arisen directly from - and by adopting its 'industrial-complex' terminology can be seen as an evolution of - what has been labelled the MIC: it follows that any study on this subject therefore needs to properly understand its predecessor concept. Put simply, the MIC has traditionally been viewed as an undesirable, even unethical<sup>15</sup> coalition of public-private (and often wider) entities pursuing shared (political-economic) objectives in the defence sector. In the popular imagination, it can be understood as a 'cosy' network of financially self-interested government and profit-making organisations that inappropriately pursue their own interests, which is considered to be unaccountable and/or highly damaging to society. Whilst (as will be discussed in thesis) both the character and impact of the MIC are contested within existing academic literature, this has not prevented the concept being presented almost invariably in 'pejorative'<sup>16</sup> terms.<sup>17</sup>

---

[00144feab7de.html?siteedition=intl](http://00144feab7de.html?siteedition=intl) (accessed 12.11.14); Glenn Greenwald, 'The decade's biggest scam', *salon.com*, 29 August 2011, Via: [http://www.salon.com/2011/08/29/terrorism\\_39/](http://www.salon.com/2011/08/29/terrorism_39/) (accessed 12.11.14); Stephen Armstrong, *War plc: The Rise of the New Corporate Mercenary* (London: Faber & Faber, 2008); Naomi Wolf, 'The spectacle of terror and its vested interests', *The Guardian*, 9 May 2012, Via: <http://www.guardian.co.uk/commentisfree/cifamerica/2012/may/09/spectacle-terror-vested-interests> (accessed 15.08.12); and Solomon Hughes, 'Follow the money: the "war on terror" and the multinationals who are profiteering from it', *Socialist Review* (March 2008), Via: <http://www.socialistreview.org.uk/article.php?articlenumber=10305> (accessed 24.02.12).

<sup>13</sup> Hughes, *War on Terror, Inc*

<sup>14</sup> Risen, *Pay any Price*; Shorrock, *Spies for Hire*.

<sup>15</sup> Edmund F. Byrne, 'The U.S. Military-Industrial Complex is Circumstantially Unethical', *Journal of Business Ethics*, Vol.95 (2010), pp.153-165

<sup>16</sup> Ledbetter argues this way in James Ledbetter, *Unwarranted Influence: Dwight D. Eisenhower and the Military-Industrial Complex* (Yale: Yale University Press 2011), p.7

As indicated above, contemporary characterisations of ‘the SIC’ have frequently but not always been presented in a similarly negative way.<sup>18</sup> In the modern-day security environment and particularly the context of the wider identified trend of the private sector’s *increasing involvement* in supporting governments on national security issues<sup>19</sup>, the idea has arisen that similarly harmful public-private dynamics have ‘followed the money’ as higher levels of public expenditure have been allocated towards mitigating non-military security issues such as terrorism. Whilst as Chapter 2 identifies much of the existing work focuses on the US example, the statistical basis for such claims is also clearly apparent in the UK according to Government figures; ‘...dedicated spending on counterterrorism, intelligence, and resilience (...) steadily increased from £923 million in 2001-2002 to £2.5 billion in 2007-2008 and will increase to £3.5bn by 2010/11’<sup>20</sup>. Given this budgetary context, the implications of such significant increases in non-military CT spending after 9/11 have often been read in a certain way. Critics have questioned the desirability of such expenditure and warned against what they see as the propensity to towards ‘threat inflation’ in this sector<sup>21</sup>; some explicitly argue that the interests traditionally associated with the MIC, or what amounts to an SIC, have begun to exert themselves negatively in the CT field.<sup>22</sup> Reflecting the growing prominence of this argument, the UK Government’s independent reviewer of CT legislation recently issued a

---

<sup>17</sup> Exceptions providing support for the MIC are John Stanley Baumgartner, *The Lonely Warriors: Case for the Military-Industrial Complex* (Los Angeles: Nash Publishing, 1970) and Charles J. Dunlap Jr., ‘The Military-Industrial Complex’, *Daedalus*, Vol.140:3 (2011).

<sup>18</sup> One recent exception argues that ‘...the suggestion that there is something sinister here is unfounded’. Nathan E. Busch and Austen D. Givens, *The Business of Counterterrorism: Public-Private Partnerships in Homeland Security* (New York: Peter Lang Publishing, Inc., 2014), p.32

<sup>19</sup> Section 1.3 analyses existing literature covering this trend.

<sup>20</sup> Cited in John Mueller and Mark G Stewart, *Terror, Security and Money: balancing the risks, benefits, and costs of Homeland Security* (Oxford: Oxford University Press, 2011), p.87

<sup>21</sup> See especially John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats and Why We Believe Them* (New York: Free Press, 2006); John Mueller and Mark G. Stewart, ‘The Terrorism Delusion’, *International Security*, Vol.37:1 (2012), pp.81-110; Steve Hewitt, *The British War on Terror* (London: Continuum, 2008), p.4; and Simon Palombi, ‘Foreign Fighters and Threat Magnification’, *Chatham House Expert Comment*, 12 August 2014, Via: <http://www.chathamhouse.org/expert/comment/15511> (accessed 10.11.14).

<sup>22</sup> Hughes, *War On Terror, Inc.; Risen, Pay any Price.*

warning over the existence of 'vested interests' in the CT field, arguing that expenditure must remain appropriate within this sector.<sup>23</sup>

Whilst no serious analyst would question the need for a proportionate policy response to terrorism, it can also be observed that the tone of criticism levelled towards the so-called SIC has rarely been dispassionate. In his dedicated account on the emergence of the SIC in the US and the UK, for example, Hughes adopts an accusatory attitude towards the interests which he considers have coalesced around, and have profited from, the new context:

...governments on both sides of the Atlantic created a well funded and well connected industrial lobby with a financial interest in extending and prolonging the war on terror. (...) Security firms could encourage the government to take military action simply by being there; the existence of companies who could help extend military action or increase 'homeland security' could seduce the British and US governments into more militaristic and authoritarian policies simply by presenting them as options.<sup>24</sup>

Whilst allegations using sweeping statements of this sort might be expected of investigative journalists and commentators, it is surprising that such arguments have been allowed to persist for so long unchallenged - or not been subjected to serious academic inquiry - crucially because they are lazy interpretations of the complexities at play.

Against this backdrop, this thesis reassesses how to conceptualise the public-private (and wider associated) interaction that has been fostered, or that has arisen, in response to the contemporary terrorism threat to the UK after 9/11. The dissertation will demonstrate - through the examination of selected case studies and by drawing on original interviews and other data arising from the UK CT sector - that whilst some of the dynamics

---

<sup>23</sup> The significance of this point is noted in Simon Palombi, 'Foreign Fighters'. For the original warning, see David Anderson, 'The Terrorism Acts in 2012: Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006', July 2013, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/243472/9780108512629.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/243472/9780108512629.pdf) (accessed 10.11.14), p.42

<sup>24</sup> Hughes, *War On Terror, Inc.*, pp.7-8



associated with the MIC clearly do now exist in the non-military CT arena, there are some other defining, differentiating and more nuanced characteristics which define public-private cooperation in the non-military security field. Whilst (like its MIC predecessor) the 'industrial-complex' in the CT sector is shown to encompass (or draw the attention of) a wide network of interested parties working closely together - people operating within government and non-government entities including private companies, research institutions, parliamentarians, first responders, the media, and other civil society organisations - the character of the system of public-private interaction in the non-military security arena is more disaggregated and significantly less coordinated than is evident in the defence sector. Data from original interviews will show that the UK's CT sector is characterised by a very broad set of actors and, in contrast to defence, possesses an almost incalculably larger set of purchasers of capability from both government and the private sector. The thesis contributes to a better understanding of this landscape and presents a picture of often chaotic public-private interaction on CT issues. In so doing, questions are raised over whether an SIC of a corrosive or damaging nature (i.e. in the same sense as the MIC has most often been presented) has actually emerged in the UK.

The dissertation concludes that whilst Eisenhower's 'warning'<sup>25</sup> should continue to be heeded in the modern security context, the SIC label has been used too simplistically to date; its usefulness in describing the system of public-private cooperation (and the actors engaged in it) has not been properly debated or understood by the scholarly community. Through its micro-level examination of selected CT-related contracts and other areas of concern associated with the SIC, the dissertation will present a more balanced, hitherto largely unseen view of how public-private cooperation really operates in the UK's non-military CT sector. This new analysis can be seen to challenge critics and in particular their

---

<sup>25</sup> Ledbetter, *Unwarranted Influence*, p.119

existing understandings of 'the SIC' profoundly; as such, the thesis makes a timely and original contribution to the field of security studies.

## **1.2 Justification for research into 'the SIC'**

It is worth briefly emphasising why this research has been conducted. This thesis is important because, as in the US until recently<sup>26</sup>, the volume and quality of scholarly investigation into the character and impact of 'the SIC' in the UK has been notable by its almost complete absence; rigorous academic debate or analysis on the SIC has simply not yet materialised. Whilst (as noted above) some academic work has begun to explore the evolution of the MIC at the conceptual level<sup>27</sup>, not a single attempt at systematic empirical analysis grounded in existing theory on the MIC has been conducted to test the appropriateness of the application of the SIC theory in the non-military UK security context.<sup>28</sup> This major research gap has arisen because, in short, authors who have referred or alluded to the existence of 'the SIC' have often done so without empirical support to their assertions.<sup>29</sup> This has led to a situation where conceptualisations of the SIC have been made on the basis of limited or anecdotal evidence; they have also (through their similar terminology) inherited negative perceptions associated from the MIC that are largely untested in the new context. This thesis will demonstrate this is misleading and that it is incorrect to portray 'the SIC' in exactly the same terms and terminology as its predecessor and namesake; the MIC.

This is not to seek to dismiss concerns that have been raised around the trend towards greater levels of public-private security cooperation; only to suggest that

---

<sup>26</sup> A 'gap in homeland security scholarship' is identified and addressed on this topic in the US context in Busch and Givens, *The Business of Counterterrorism*, p.3

<sup>27</sup> Dunne and Sköns, 'The Changing Military Industrial Complex'; Baker-Beall and Robinson, 'The Emergence of the Security-Industrial Complex'

<sup>28</sup> Hughes's *War On Terror, Inc.* might be seen as an exception. However, this analysis is journalistic in nature.

<sup>29</sup> Hughes, 'Follow the money' serves as a good example of such analysis.

characterisations of 'the SIC' have not yet been properly tested. The main reason for undertaking this dissertation, therefore, has been to address the current shortage of research and analysis on the scope of public-private interaction supporting UK national security, and the lack of balanced debate over the appropriateness of private sector involvement in this sector.<sup>30</sup> If there are now extensive interactions between the Government and the private sector in non-military aspects of UK national security strategy, as this thesis illustrates, it is fitting that the origins, characteristics and consequences of such cooperation be properly analysed. There should be improved scrutiny of private companies' activities in the sector.

There are two other main reasons why this research is justified. Firstly, as 'national security' comprises a significant proportion of the UK Government's overall budget<sup>31</sup>, the size, effectiveness and appropriateness of expenditure in this field - including but extending beyond the defence sector - deserves to be subjected to rigorous scrutiny. Whilst one study has (briefly) addressed this directly<sup>32</sup>, and the size of the domestic UK security market has been illustrated<sup>33</sup>, a lack of scrutiny exists on the size, allocation and appropriateness of UK national security expenditure outside military issues, including in

---

<sup>30</sup> In addition to the analyses outlined in Section 1.1, see Ben Hayes, 'NeoConOpticon: The EU Security-Industrial Complex', Statewatch/Transnational Institute Report, September 2009, Via: <http://neoconopticon.wordpress.com/read-the-report/> (accessed 24.06.11); Mel Kelly, 'Police, magistrates and prisons by G4S. Is this what the British people want?', *openDemocracy*, 6 March 2012, Via: <http://www.opendemocracy.net/ourkingdom/mel-kelly/police-magistrates-and-prisons-by-g4s-is-this-what-british-people-want> (accessed 19.04.12); Eric King, 'Selling arms and snooping technology is no way to help democracy, Cameron', *theguardian.com*, 11 April 2012, Via: <http://www.theguardian.com/commentisfree/2012/apr/11/selling-arms-cameron> (accessed 23.04.12)

<sup>31</sup> This is difficult to measure but 'Defence' (£38bn) and 'Public Order & Safety' (£32bn) combined totaled 9.6% of total UK government spending (£732bn) in 2014. 'Budget 2014: the government's spending and income visualised', *theguardian.com*, Via: <http://www.theguardian.com/news/datablog/2014/mar/21/budget-2014-tax-spending-visualised> (accessed 19.12.14)

<sup>32</sup> The cost-effectiveness of UK CT expenditure is assessed in Mueller and Stuart, *Terror, Security, and Money*, pp.87-91

<sup>33</sup> One trade association identified that its members completed business amounting to £1.8bn in 2010, for example. ADS Group, 'UK Security Survey 2011' (London: ADS Group, 2011), Via: <http://www.adsgroup.org.uk/articles/26154> (accessed 17.08.12), p.6

the CT field.<sup>34</sup> This thesis's micro-level examination of UK CT expenditure and contracts in itself constitutes a significant new contribution to the field.

Secondly, on the basis of the available literature and interviews conducted for this thesis there is evidently a lack of awareness and informed discussion at the policy level about the aggregated totality of the roles that 'industry' plays (or could play) in CT today, and a shortage of creative thinking on how such contributions could be managed better. This thesis argues that only after substantive new analysis has been completed can a proper debate begin around whether the existing 'terms of engagement'<sup>35</sup> for public-private security cooperation are effective and appropriate; there is currently a shortage of 'joined-up' thinking in this area that could help to realise meaningful policy-making improvements. This thesis seeks to provide a basis for future discussions; it is hoped that its analysis and conclusions will help to encourage an improvement in the level of policy focus and research attention given to the private sector's involvement in UK national security strategy.

### **1.3 Contextualisation of the thesis within existing academic literature and debates**

#### *Literature and debates on the privatisation of security*

In addition to the extensive existing academic literature covering the origins, character and operation of the MIC (covered in Chapter 2), the role that industry (or the private sector more generally) plays in contemporary national security strategy has also attracted significant scholarly scrutiny and policy attention. When considering the

---

<sup>34</sup> An exception is the analysis within a report by the Institute for Public Policy Research (IPPR) Commission on National Security, which found that in 2007/08 the UK spent 'in the region of £61bn' on national security defined in the widest sense. IPPR, 'Shared Responsibilities: A national security strategy for the UK', The final report of the IPPR Commission on National Security in the 21<sup>st</sup> Century, June 2009, Via: [http://www.ippr.org/images/media/files/publication/2012/01/shared-responsibilities\\_security-final\\_June2009\\_1704.pdf](http://www.ippr.org/images/media/files/publication/2012/01/shared-responsibilities_security-final_June2009_1704.pdf) (accessed 01.03.12), p.99

<sup>35</sup> David Omand introduced the author to this expression. This phrase is also used in Adam White, *The Politics of Private Security* (London: Palgrave Macmillan, 2010), p.55

'privatisation of security'<sup>36</sup>, it is often asserted - whether within Government, industry or academia - that States *depend* on companies to fulfil their military and security objectives.<sup>37</sup> This argument appears within the UK Government's defence policy documentation, for example, and especially in the large body of scholarship on private companies' support of Western armed forces in recent overseas conflicts; the contributions of private military and security companies (PMSCs) in supporting recent UK military deployments have attracted particular academic scrutiny<sup>38</sup>, for example, as have the governance frameworks for their involvement.<sup>39</sup> Such is the extensive use of companies in the security arena today that their involvement has even been described as 'ubiquitous'<sup>40</sup>.

There has been notable additional coverage of more traditional industrial aspects of the British Government's defence policy and posture<sup>41</sup>, the economic factors potentially

---

<sup>36</sup> This expression appears in Peter Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (New York: Cornell University Press, 2003), p.49

<sup>37</sup> Scholars including Stanger have argued that 'the U.S. Government can now conduct neither its foreign policy nor its wars and reconstruction efforts in Iraq and Afghanistan without the extensive and unprecedented support of contractors.' Allison Stanger, *One Nation Under Contract: The Outsourcing of American Power and the Future of Foreign Policy* (London: Yale University Press, 2009), p.2. For the argument in a UK context, see Charlie Edwards, *National Security for the Twenty-First Century* (London: Demos, 2007), Via:

<http://www.demos.co.uk/publications/nationalsecurityforthetwentyfirstcentury> (accessed 15.08.12), p.38. The author has noted elsewhere how other prominent figures have argued that Governments depend on private companies in terms of security. Hugo Rosemont, 'Getting down to Business: Industry's role in national security', *RUSI Journal*, Vol.155:1 (2010), p.80

<sup>38</sup> See especially Chapter 5 of Christopher Kinsey, *Private Contractors and the Reconstruction of Iraq* (Oxford: Routledge, 2009), pp.91-115; Henrik Heidenkamp, 'Sustaining the UK's Defence Effort: Contractor Support to Operations Market Dynamics' (London: Royal United Services Institute, 2012), Via: [http://www.rusi.org/downloads/assets/WHR\\_2-12\\_CSO\\_Final\\_WEB.pdf](http://www.rusi.org/downloads/assets/WHR_2-12_CSO_Final_WEB.pdf) (accessed 15.08.12); and Mark Erbel, 'Contractors in the "War on Terror": Enabling Global Military Deployment', *e-International Relations*, (18.08.11), Via: <http://www.e-ir.info/2011/08/18/contractors-in-the-%e2%80%9cwar-on-terror%e2%80%9d-enabling-global-military-deployment/> (accessed 15.08.12)

<sup>39</sup> See especially Elke Krahnmann, *States, Citizens and the Privatization of Security* (Cambridge: Cambridge University Press, 2010) and Rita Abrahamsen and Michael C. Williams, *Security Beyond the State: Private Security in International Relations* (Cambridge: Cambridge University Press, 2011)

<sup>40</sup> *Ibid.*, p.30

<sup>41</sup> See, for example, Trevor Taylor, 'Reforming UK Defence Industrial Policy', *RUSI Defence Systems*, Vol.14:1 (2011), pp.35-37; and Lord Drayson 'The Defence Industrial Strategy: Our Relationship with Industry', *RUSI Defence Systems*, Vol. 9:1 (2006), Via: [http://www.rusi.org/downloads/assets/020-025\\_The\\_Debate1.pdf](http://www.rusi.org/downloads/assets/020-025_The_Debate1.pdf) (accessed 01.06.11), p.20

accounting for rising costs within the defence budget<sup>42</sup>, and the extent to which outsourcing now exists as a core and indelible characteristic of British defence policy.<sup>43</sup> Therefore, alongside significant recent scholarly and policy interest in the activities of PMSCs, the role played by traditional defence suppliers (often referred to collectively as the 'defence industrial base' (DIB)) has remained under close scrutiny.<sup>44</sup> Perhaps owing to the dominance of the US Government's defence expenditure<sup>45</sup>, and especially since 9/11 and the subsequent military interventions conducted in the name of the 'War on Terror', analysis of the character, scope and implications of such corporate involvement in contemporary security has often concentrated on the North American experience.<sup>46</sup>

Some theoretical work has attempted to question, characterise or explain the causes of such extensive levels of corporate involvement in security.<sup>47</sup> The more convincing, evidence-based explanations have included, for example, Singer's idea that many national militaries down-sized following the end of the Cold War - for him, '[t]he end of the Cold War produced a vacuum in the market of security'<sup>48</sup> - and the wider historical fact that national defence industries in the US and the UK were privatised during the 1980s and 1990s. At a broader theoretical level, international relations scholars and political economists have advanced the now widely-accepted, almost clichéd idea that, following the Cold War, the nature of the State system has undergone a significant transformation

---

<sup>42</sup> David Kirkpatrick, 'Trends in the costs of weapon systems and the consequences', *Defence and Peace Economics*, Vol.15:3 (2004), pp.259-273

<sup>43</sup> Krahnemann argues that '[t]he UK has been one of the first countries to privatise and outsource significant proportions of its national defence establishment[.]' Krahnemann, *States, Citizens*, p.84

<sup>44</sup> See Henrik Heidenkamp, John Louth and Trevor Taylor, 'The Defence Industrial Ecosystem: Delivering Security in an Uncertain World', RUSI Whitehall Report 2-11, June 2011, Via: <http://www.rusi.org/publications/whitehallreports/ref:04E03231821048/> (accessed 20.02.11)

<sup>45</sup> Jacques Gansler, *Democracy's Arsenal: Creating a Twenty-First-Century Defense Industry* (London: MIT Press, 2011), p.20

<sup>46</sup> Widely-cited US treatments include Singer, *Corporate Warriors*; Stanger, *One Nation Under Contract*; and Dana Priest and William Arkin, *Top Secret America: The Rise of the New American Security State* (New York: Little, Brown and Company, 2011)

<sup>47</sup> See, for example, Patricia Owens, 'Distinctions, distinctions: 'public' and 'private' force?', *International Affairs*, Vol. 84:5 (2008), pp.977-990; and Lucia Zedner, *Security* (Oxford: Routledge, 2009).

<sup>48</sup> Singer, *Corporate Warriors*, p.49

within the context of a rapidly changing global environment.<sup>49</sup> As a result of new trends including increasing globalisation and rapid technological innovation - trends which some argue have reduced the ability of the classical Westphalian 'nation state' to exert influence and power globally<sup>50</sup> - it follows that Governments have sought to make increasing use of 'non-state actors' such as the private sector to fulfil their responsibilities, both within and beyond the national security sector.<sup>51</sup>

Whilst such trends and their potential implications have generated considerable scholarly attention in respect of the defence sector, there has been comparatively little dedicated theoretical and empirical scrutiny of - and public debate around - the origins, characteristics and consequences of the private sector's involvement within the non-military aspects of the UK's national security strategy.<sup>52</sup> With the exception of some limited interest in the private sector's involvement in CT<sup>53</sup>, scholarly attention in this field has remained largely focused on the PMSC sector or more traditional defence-industrial issues. This lack of scrutiny on privatisation within non-military security sectors is reflected at the highest policy levels; the Government's 2010 Strategic Defence and Security Review (SDSR) almost completely declined, for example, to contemplate how companies other than the DIB are involved in security.<sup>54</sup> As Abrahamsen and Williams have lamented in a separate

---

<sup>49</sup> See, for example, Saskia Sassen, *Losing Control? Sovereignty in an Age of Globalization* (New York: Cambridge University Press, 1996) and Robert Cooper, *The Breaking of Nations: Order and Chaos in the Twenty-first Century* (London: Atlantic Books, 2004)

<sup>50</sup> See especially Susan Strange, *The Retreat of the State: The Diffusion of Power in the World Economy* (New York: Cambridge University Press, 1996), especially pp.3-13

<sup>51</sup> Slaughter has posited, for example, that 'Government networks' now include 'private actors such as corporations and NGOs, and 'mixed' actors that are privately organized but increasingly perform public functions.' Anne-Marie Slaughter, 'Governing Through Government Networks' in David Held and Anthony McGrew (Eds.) *The Global Transformations Reader, Second Edition* (Cambridge: Polity Press, 2003), p.192

<sup>52</sup> The author sought to address this in Hugo Rosemont, 'Private Sector Engagement in the UK's Counter-Terrorism Strategy: A New Agenda', *Behavioral Sciences of Terrorism and Political Aggression*, Vol.6 (2014), pp.147-161

<sup>53</sup> See footnote 121 for a list of references.

<sup>54</sup> The SDSR's 'industry' section covered only its support to the Armed Forces and the MoD. HM Government, 'Securing Britain in an Age of Austerity: The Strategic Defence and Security Review' (London: TSO, 2010), Via:

context, we could say that there is almost an ‘invisibility of security privatization’<sup>55</sup> in the non-military UK security field.

This imbalanced, defence-focussed character of UK scholarly inquiry into (and policy focus on<sup>56</sup>) the ‘privatisation of security’ can be quite easily explained. In short, whilst (as shown below) contemporary definitions of ‘national security’ have changed considerably in incorporating non-military security issues, this important shift has only occurred quite recently. Whereas in the 20<sup>th</sup> Century a primary characteristic of any State’s national security approach has been in deterring and/or responding to *inter-state threats* by military means, the security environment has now fundamentally altered.<sup>57</sup> The UK Government’s 2010 National Security Strategy (NSS) explicitly recognised this, expressing the four top contemporary risks to UK security: international terrorism, hostile attacks upon UK cyber space, a major accident or natural hazard and an international military crisis.<sup>58</sup> The under-appreciated implication of this assessment is that many of the country’s most pressing security challenges require non-military security responses that often necessarily incorporate the support of many different companies. In short, as Edwards has

---

[http://webarchive.nationalarchives.gov.uk/20121015000000/http://www.direct.gov.uk/prod\\_consum\\_dg/groups/dg\\_digitalassets/@dg/@en/documents/digitalasset/dg\\_191634.pdf](http://webarchive.nationalarchives.gov.uk/20121015000000/http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf) (accessed 16.10.12), p.30

<sup>55</sup> Abrahamsen and Williams, *Security Beyond the State*, p.29

<sup>56</sup> There are signs that this may be changing: as noted elsewhere, the 2009 iteration of CONTEST stated that the UK now ‘depends on the expertise and knowledge of industry to combat terrorism.’ Rosemont, ‘Getting Down to Business’, p.80; As another example, the 2011 edition of the UK Government’s Cyber Security Strategy explained that it ‘will require everyone, the private sector, individuals and government to work together[.]’ Cabinet Office, ‘The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world’, November 2011, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/60961/uk-cyber-security-strategy-final.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf) (accessed 15.08.12), p.22

<sup>57</sup> There is a vast body of existing literature relating to this observation, most of which is not directly relevant to this thesis. The following section covers key texts on how the ‘national security’ concept has evolved.

<sup>58</sup> HM Government, ‘A Strong Britain in an Age of Uncertainty: The National Security Strategy’ (London: The Stationary Office, 2010), Via: <http://www.cabinetoffice.gov.uk/resource-library/national-security-strategy-strong-britain-age-uncertainty> (accessed 22.02.12), p.27



expertly highlighted, any country's military capacity in this context must be seen as only one element of its overall national security capability.<sup>59</sup>

This is not to suggest that the private sector's involvement in non-military security issues has been completely overlooked by scholars; the 'mushrooming of private security industries'<sup>60</sup> across Europe has been documented in this context, for example, and other core texts covering the private sector's involvement in national security (including CT) are also available<sup>61</sup>. However, analysis of security privatisation in the non-military security field tends to be less structured and/or has not yet considered the potentially larger implications of the private sector's involvement.<sup>62</sup> Whilst the involvement of companies in the policing<sup>63</sup>, intelligence<sup>64</sup> and cyber security<sup>65</sup> sectors has attracted scrutiny, such research has generally been conducted on a sector-specific basis. In another context, the UK Government's interactions with the private sector in protecting the country's critical infrastructure have been expertly documented<sup>66</sup>, but this form of cooperation is not

---

<sup>59</sup> Edwards, *National Security*, especially pp.70-71

<sup>60</sup> Ronald van Steden and Rick Sarre, 'The Growth of Private Security: Trends in the European Union', *Security Journal*, Vol.20 (2007), p.232

<sup>61</sup> See references listed in footnotes 37, 38, 121; Edwards, *National Security*, pp.49-51; and especially David Omand, 'What is the Future for the Critical National Infrastructure?', *RUSI Monitor*, Vol. 7:4 (2008)

<sup>62</sup> Reflecting the immaturity of discussions, Sempere has proposed a research agenda. Carlos Marti Sempere, 'The European Security Industry. A Research Agenda', *Defence and Peace Economics*, Vol.22:2 (2011), pp.245-264

<sup>63</sup> Ken Livingstone and Jerry Hart, 'The Wrong Arm of the Law?: Public images of Private Security', *Policing and Society*, Vol. 13:2 (2003), pp. 159–170; Ronald Van Steden, *Privatizing Policing: Describing and explaining the growth of private security* (Hoofddorp: BJU Publishers, 2007); and White, *The Politics of Private Security*. By contrast, Williams laments 'the previously neglected and domestically orientated domain of policing' in security studies. Michael C Williams, 'The Public, the Private and the Evolution of Security Studies', *Security Dialogue*, Vol.41:6 (2010), p.627

<sup>64</sup> Andrew Rathmell, 'Privatising Intelligence', *Cambridge Review of International Affairs*, Vol.11:2 (1998)

<sup>65</sup> Lewis Herrington and Richard Aldrich, 'The Future of Cyber-Resilience in an Age of Global Complexity', *Politics*, Vol.33:4 (2013), pp.299-310

<sup>66</sup> Omand, 'What is the Future for the CNI?'

routinely connected with other fields of non-military security privatisation.<sup>67</sup> In short, there is a 'neglect of the breadth of security privatization.'<sup>68</sup>

Finally, at the theoretical level, some of the most prominent recent philosophical thought on the interaction between the State and the market on security issues has gained considerable prominence. Amongst the most hotly-contested offerings in this space is Professor Philip Bobbitt's theory on the emergence of what he has called the 'market state'<sup>69</sup>. For Bobbitt, a transition of the 'constitutional order' is underway whereby the ability of the State to achieve its objectives is no longer drawn from its 'national' character, but derives largely from (and is deeply engrained in) the market economy. One of the implications of this is that, for underlying structural reasons, governments now have *no option* but to engage with companies. Under contemporary circumstances, he argues; '...governments will have to learn how to select and work with private sector collaborators, partly because the latter own most of the critical infrastructure that we must make less vulnerable'.<sup>70</sup> With this statement, Bobbitt appears to have been ahead of his time in identifying the deep significance of private sector's present day role in security.

Whilst Bobbitt's controversial ideas have received criticism<sup>71</sup>, he raises important questions about the potential strategic implications for CT and 'wider security' of the

---

<sup>67</sup> Omand's article is a rare exception in this regards. Ibid.

<sup>68</sup> Abrahamsen and Williams, *Security Beyond the State*, p.23. The author argued similarly in Hugo Rosemont, 'Outsourcing or interdependency? Why we need to widen our approach to the study of the private sector's involvement in UK national security', Presentation to inaugural conference of King's College, London, Private Military and Security Research Group, 18 November 2011 (unpublished)

<sup>69</sup> Bobbitt explores the main characteristic of the constitutional change he sees from the nation state to the market state: "Whereas the nation state justified itself as an instrument to serve the welfare of the people (the nation), the market-state exists to maximise the opportunities enjoyed by all members of society." Philip Bobbitt, *The Shield of Achilles: War, Peace and the Course of History* (London: The Penguin Press, 2002), pp.228-229

<sup>70</sup> Philip Bobbitt, *Terror and Consent: The Wars for the Twenty-First Century* (London: Allen Lane, 2008), p. 533.

<sup>71</sup> See especially Michael Howard, 'Philip Bobbitt's Terror and Consent: A Brief Critique' in David Fisher and Rian Wicker (Eds.) *Just War on Terror?: A Christian and Muslim Response* (Farnham: Ashgate Publishing, 2010)

confluence of the 'market' and the 'state' in what he convincingly argues is a significantly altered international system. In short, the controversial proposition he puts forward - a proposition nevertheless also advanced by other scholars<sup>72</sup> - is that the Governments *must* now cooperate with companies on non-military security issues such as CT.

#### *Literature and debates on the meaning of 'National Security'*

If there is, as this thesis will argue, a need to widen 'the empirical lens to include non-militarized forms of private security'<sup>73</sup>, then it is important to consider what is meant by 'security' in the first instance. Unfortunately 'national security' is not straightforward to define<sup>74</sup>, as it is considered by many leading scholars to be a subjective<sup>75</sup> or contested<sup>76</sup> concept. In the political press, accusations abound that the term 'national security' has been abused; Jenkins, for example, has criticised the approach of UK 'securocrats' for considering 'security' wrongly as something more than 'the integrity of the British state or its institutions.'<sup>77</sup> By contrast, other authors argue that not enough has been (or is being) done to ensure the UK's 'national security'; concerns are frequently articulated about the state of 'the UK's role in the world' and the fact that the defence budget has been

---

<sup>72</sup> See especially Zarate's powerful contention on the need for Government to work with non-state entities including companies on security issues through the adoption 'Strategic Suasion'. Juan C. Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: Public Affairs Books, 2013), pp.423-437

<sup>73</sup> Abrahamsen and Williams, *Security Beyond the State*, p.2

<sup>74</sup> For a masterful account of various conceptualisations of 'security' see David A. Baldwin, 'The Concept of Security', *Review of International Studies*, Vol.23 (1997)

<sup>75</sup> Nick Ritchie, 'Rethinking security: a critical analysis of the Strategic Defence and Security Review', *International Affairs*, Vol.87:2 (2011), p.360. Wolfers argues that security possesses subjective and objective senses. Arnold Wolfers, "'National Security" as an Ambiguous Symbol', *Political Science Quarterly*, Vol. 67:4 (1952), p.485

<sup>76</sup> Michael Sheehan, *International Security: An Analytical Survey* (London: Lynne Rienner, 2005), p.2. Baldwin challenges this idea; 'Security is more appropriately described as a confused or inadequately explicated concept than as an essentially contested one.' David A. Baldwin, 'The Concept of Security', p.12

<sup>77</sup> Simon Jenkins, 'The real threat to our way of life? Not terrorists or faraway dictators, but our own politicians and securocrats', *theguardian.com*, 27 August 2013, Via: <http://www.theguardian.com/commentisfree/2013/aug/27/real-threat-terrorist-politicians-national-security> (accessed 14.06.14)

dangerously underfunded in recent decades, for example.<sup>78</sup> This lack of consensus around how 'national security' should be invoked and delivered reflects how there is disagreement over how it should be conceptualised.

Public polling data also indicates the subjective nature of 'national security'. In their research on public attitudes, for example, Allouche and Lind present the 'evolution of public perception according to opinion polls on the perception of most worrying topics in 1997, 2003 and 2007.'<sup>79</sup> They show that the proportion of people considering 'crime and violence' as the most worrying issue steadily reduced from 68% in 1997, to 50% in 2003, down to 51% in 2007.<sup>80</sup> Terrorism, on the other hand, rose overall as an issue that the public most worried about during this period - from 21% in 2007 up to 42% in 2003, subsiding again to 33% in 2007.<sup>81</sup> This exemplifies both how security is difficult to define and how perceptions on the main threats can vary over time.

Useful attempts at a definition of 'national security' have been made, however. Within one of the most-widely cited works on this subject, Buzan et. al. compare what they see as the two main approaches in *Security: A New Framework for Analysis*; 'the new one of the wideners and the old military and state centred view of the traditionalists.'<sup>82</sup> Scholars associated with the latter, they argue, 'equate security with military issues and

---

<sup>78</sup> See, for example, Malcolm Chalmers, 'The Financial Context for the 2015 SDSR: The End of UK Exceptionalism?', *RUSI Briefing Paper*, September 2014, Via:

[https://www.rusi.org/downloads/assets/201409\\_BP\\_Financial\\_Context\\_of\\_the\\_2015\\_SDSR.pdf](https://www.rusi.org/downloads/assets/201409_BP_Financial_Context_of_the_2015_SDSR.pdf) (accessed 15.11.14); Con Coughlin, 'An army without soldiers is doomed to failure', *blogs.telegraph.co.uk*, 19 December 2013, Via:

<http://blogs.telegraph.co.uk/news/concoughlin/100251343/an-army-without-soldiers-is-doomed-to-failure/> (accessed 14.06.14); and United Kingdom National Defence Association, 'Inconvenient Truths – Threats Justify Prioritising Defence', UKNDA Report, September 2011, Via: [http://www.uknda.org/uploads/1/5/3/0/15302742/inconvenient\\_truths\\_tue\\_27\\_final\\_f1.3.pdf](http://www.uknda.org/uploads/1/5/3/0/15302742/inconvenient_truths_tue_27_final_f1.3.pdf) (accessed 15.11.14)

<sup>79</sup> Jeremy Allouche and Jeremy Lind, 'Public Attitudes to Global Uncertainties: A Research Synthesis exploring the trends and gaps in knowledge' (November 2010), Via: [http://www.esrc.ac.uk/\\_images/ESRC%20Global%20Uncertainties%20Research%20Synthesis%20FINAL\\_tcm8-14632.pdf](http://www.esrc.ac.uk/_images/ESRC%20Global%20Uncertainties%20Research%20Synthesis%20FINAL_tcm8-14632.pdf) (accessed 16.08.12)

<sup>80</sup> *Ibid.* p.12

<sup>81</sup> *Ibid.*

<sup>82</sup> Barry Buzan, Ole Waever and Jaap de Wilde, *Security: A New Framework for Analysis* (London: Lynne Rienner, 1998), p.1

the use of force'<sup>83</sup>; traditional interpretations of security are thus primarily associated with the risk of external invasion or other military threats, whereas in more recent decades scholars have encouraged the adoption of a broader perspective to the study of security issues.<sup>84</sup> This thesis adopts this latter interpretation of 'security' because - at the risk of repetition - the scholarly community has not yet given the private sector's involvement in the non-military security context the attention it deserves.

Whilst debates over the meaning of 'security' can generate more questions than answers, Ken Booth, David Omand and Julian Richards offer particularly useful definitions of the concept as they highlight certain, general characteristics which can be accepted. The former has argued, for example, that there exists 'a consensus on the standard definition of security - to do with being or feeling safe from threats and danger[.]'<sup>85</sup> Similarly, Omand offers a definition<sup>86</sup>:

*...national security today should be defined as a state of trust on the part of the citizen that the risks to everyday life, whether from man-made threats or impersonal hazards, are being adequately managed to the extent that there is confidence that normal life can continue.*

Such sensible interpretations illustrate how the concept of security cannot therefore be restricted - both in theory and in practice - to military issues; this was made very clear in a contemporary setting on 9/11. Furthermore, as Richards proposes "that "national security" is defined as a particular articulation of security priorities and concerns put forward by the

---

<sup>83</sup> Ibid.

<sup>84</sup> See, for example, Hella Engerer, 'Security as a public, private or club good: some fundamental considerations', *Defence and Peace Economics*, Vol.22:2 (2001). For a leading treatment on how 'national security' evolved to include such issues as natural disasters and catastrophic floods see Richard H. Ullman, 'Redefining Security', *International Security*, Vol.8:1 (1983), pp.133-135. For a useful discussion on the 'broadening' of security see Keith Krause and Michael Williams, 'Broadening the Agenda of Security Studies: Politics and Methods', *Mershon International Studies Review*, Vol. 40:2 (1996), pp.229-254.

<sup>85</sup> Ken Booth, 'Critical Explorations' in Ken Booth (Ed.), *Critical Security Studies and World Politics* (London: Lynne Rienner Publishers, 2005), p.13

<sup>86</sup> David Omand, *Securing the State* (London: C. Hurst & Co., 2010), p.9 (Emphasis in original)

political leaders of a state, at a given time in its history<sup>87</sup>, so any dissertation addressing contemporary security strategy (including the private sector's involvement therein) must recognise how these 'articulations' vary over time.

One recognised feature of evolving thinking on 'national security' is what has been referred to as the 'blurring' of defence and security issues. Omand has outlined this trend, arguing that by 9/11 the UK's approach was '...blurring the previous boundaries between the overseas and domestic theatres and broadening thinking about risks to include hazards as well as threats.'<sup>88</sup> Similarly, Edmunds has described the 'conceptual desegregation of defence within UK security as a whole'<sup>89</sup> and, more recently, Phillips notes that 'the blurred (if not false) distinction between home and abroad' was one of the two key drivers behind the rationale to widen the planned Defence Review to include security issues after the 2010 General Election.<sup>90</sup> The argument put forward by these and other such prominent thinkers<sup>91</sup> - that defence and security issues are increasingly connected within any country's overall conceptualisation of 'national security' - is extremely compelling; there has even been a precedent for considering industry's involvement in this context.<sup>92</sup> This thesis agrees that security has 'broadened' in this way; as such, it is deemed important that the private sector's involvement is properly understood in this wider context.

Understanding how 'national security' is now routinely considered broadly is especially relevant to this thesis' core interest - i.e. analysing *how* and *why* companies are

---

<sup>87</sup> Julian Richards, *A Guide to National Security: Threats, Responses, and Strategies* (Oxford: Oxford University Press, 2012), p.17

<sup>88</sup> Omand, *Securing the State*, p.9

<sup>89</sup> Timothy Edmunds, 'The defence dilemma in Britain', *International Affairs*, Vol.86:2 (2010), p.390

<sup>90</sup> Mark Phillips, 'Policy-Making in Defence and Security: Lessons from the Strategic Defence and Security Review', *RUSI Journal*, Vol.157:1 (2012), p.28

<sup>91</sup> See also Edwards, *National Security* and Jonathan Shaw, *Britain in a Perilous World: The Strategic Defence and Security Review We Need* (London: Haus Publishing, 2014)

<sup>92</sup> European Commission, 'Study on the industrial implications in Europe of the blurring of dividing lines between Security and Defence - Final Report' (2010), Via: [http://ec.europa.eu/enterprise/sectors/defence/files/new\\_defsec\\_final\\_report\\_en.pdf](http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf) (accessed 24.02.12)

involved in CT - because it is from the Government's definition of 'national security' that strategic, operational and investment decisions are made in the security sector. Whilst their respective security policies and practices have varied, both the New Labour Governments after 1997 and the Conservative-Liberal Democratic Coalition Government which succeeded them both placed a significant emphasis on addressing non-military security risks. According to the current Government, for example, the UK faces a wide variety of challenges that extend beyond potential military threats; as stated above, its 2010 NSS expresses a tiered list of risks to UK security and the 'tier one' category (i.e. the most serious risks) includes international terrorism, hostile attacks upon UK cyber space, a major accident or natural hazard and an international military crisis.<sup>93</sup> In practical policy terms, this means that the responses to three of the four principal risks to the UK's national security are now 'owned' by departments other than the Ministry of Defence (MoD).<sup>94</sup> This thesis is an investigation into such wider security machinery; it recognises that the MoD has also developed interactions with the private sector on non-traditional security issues, but focuses on the under-researched public-private cooperation that has been fostered in the CT sector by non-military security departments such as the Home Office.

Two final points can be made about scholarly discussions on 'national security' in so far as they relate to this thesis. Firstly, it should be stressed that the debates over the meaning of 'national security' rightly show no sign of being 'resolved'; in short, the concept is likely to continue to be viewed in a variety of ways<sup>95</sup>, and a vigorous debate is likely to

---

<sup>93</sup> HM Government, 'A Strong Britain', p.27

<sup>94</sup> Richards argues similarly that three out of the four top tier risks are drawn from 'a wide range of transnational, non-state, and 'human security' factors (...) alongside those of traditional statist military threats.' Richards, *A Guide to National Security*, p.172. For a discussion on how military issues 'are now part of a wider and more diverse policy nexus', see Edmunds, 'The defence dilemma in Britain', pp.389-393

<sup>95</sup> For example, advocates of 'Human Security' discourse take the view that 'that people rather than the State should be the priority focus, or referent object, of security policy and practice.' Nick Ritchie, 'Rethinking security', p.356

continue to take place around the effectiveness of the UK Government's national security machinery and its ability to conduct 'strategy'.<sup>96</sup> This thesis seeks to contribute to this field of scholarship in so far as the private sector is involved in UK national security strategy; this topic has unfortunately rarely featured in discussions on strategy-making to date.

Secondly, this study is constrained by length and so choices have been made in framing which aspects of the private sector's involvement in 'national security' are analysed. As noted above, many scholars have convincingly argued that it is no longer sufficient to solely address the military aspects of security in implementing UK national security strategy<sup>97</sup>; the author strongly agrees with this assessment. This thesis does not seek to dismiss the importance of defence issues<sup>98</sup>, but argues that new research is needed on other important aspects of security privatisation.

#### **1.4 A reassessment of the UK 'security-industrial complex'**

More academic research is needed, therefore, on the private sector's involvement in contemporary UK national security strategy beyond the defence sector. Whilst it has been argued that an emerging 'SIC' has exerted a negative influence in the 'domestic security' arena<sup>99</sup>, no academic work has yet systematically considered the characteristics and the consequences of the extensive range of public-private security interactions that have been fostered by UK national security-related departments outside the military arena. Whilst some theoretical work has been completed (or is emerging) on the evolution

---

<sup>96</sup> Gearson and Gow argue, for example, that there is an 'absence of a developed and integrated national security strategy' in the UK. John Gearson and James Gow, 'Security, Not Defence, Strategic, Not Habit: Restructuring the Political Arrangements for Policy Making on Britain's Role in the World', *Political Quarterly*, Vol. 81:3 (2010), p.407

<sup>97</sup> See especially *ibid.*; Edwards, *National Security*; and Phillips, 'Policy-Making', pp.28-35

<sup>98</sup> Some authors seem to feel that the pre-eminence of defence is under threat, such as Edmunds's notion that the military's role in national security is 'to some degree *subordinate* to (...) a much wider set of security goals, priorities and instruments[.]' Edmunds, 'The defence dilemma', p.390 (Emphasis added)

<sup>99</sup> As noted in Section 1.1, this argument was introduced by Hughes in *War on Terror, Inc.*



of the MIC and/or 'the SIC' concept<sup>100</sup>, the problem is that, prior to this thesis, detailed analytical work had not been completed on the structure and operation of public-private cooperation in the non-military context. Whilst Dunne and Sköns have suggested that that the MIC has evolved in the new security environment, for example, they decline to investigate its dynamics in detail.<sup>101</sup> As argued in Chapter 2, Hughes' fierce critique of the SIC appears more concerned with presenting the system as a conspiracy than with actually analysing its complexity. This thesis seeks to offer a fuller, more balanced analysis of the origins, characteristics and consequences of the private sector's role in contemporary UK national security strategy.

The thesis will demonstrate that, as security risks have 'broadened' away from military issues<sup>102</sup>, so a system of extensive public-private security interaction has emerged in the CT aspects of the UK's national security strategy. As a result of multiple new interactions - some of which are detailed for the first time - the dissertation argues with specific reference to the UK Government's CT Strategy known as 'CONTEST' that an 'industrial complex' of a different variety to the MIC has emerged in the CT sector. In short, the 'British military-industrial complex'<sup>103</sup> can be seen to have evolved in the sense that some of its dynamics also now exist in the context of the responses established to tackle various non-military, contemporary security risks. However, as Section 1.1 introduced, the character of the aggregation of the public-private interactions in CT differs from the

---

<sup>100</sup> Dunne and Sköns, 'The Changing Military Industrial Complex'; Baker-Beall and Robinson, 'The Emergence of the Security-Industrial Complex'

<sup>101</sup> Dunne and Sköns, 'The Changing Military Industrial Complex'

<sup>102</sup> To re-cap, Engerer summarises: 'Whereas the notion of "security" formerly had a military focus, the notion broadened during the 1980s and 1990s from military to non-military issues, such as infectious diseases or food security.' Engerer, 'Security as a public, private or club good', p.135

<sup>103</sup> This phrase is used in David Edgerton, 'The British military-industrial complex in history: the importance of political economy', *The Economics of Peace and Security Journal*, Vol.3:1 (2008), pp. 5-10

defence-orientated and now arguably outdated concept (introduced in the following chapter) known as the MIC.<sup>104</sup>

The thesis will show that there are some distinct origins, characteristics and consequences of the private sector's involvement in the non-military aspects of national security that deserve to be understood. Crucially, the UK Government and its associated agencies are not solely concerned with engaging commercial *suppliers* of products and services as they interact with the private sector on CT issues; engagement with this part of 'industry' is a (if not *the*) defining feature of most existing theoretical work on the MIC. Whilst recognising that some traditional defence and security sector suppliers have played a role in CONTEST, this thesis shows that in the post 9/11 security context the UK Government has also developed relationships with both private operators of security and a wide range of other business sectors. Furthermore, whereas 'the term "military-industrial complex" is almost always used as a pejorative'<sup>105</sup>, this thesis strives for neutrality in examining the proposition that the private sector's involvement within CT Strategy might now properly be considered as a *necessary* element of UK national security strategy. It has already been found that the use of contractors by governments in support of military operations is now widespread<sup>106</sup>; this thesis examines the UK Government's use of companies in CT to reassess the dynamics of corporate involvement in this field.

The UK has been selected as the sole country case study for this thesis because, despite the apparently extensive level of privatisation within the country's national security strategy, the actual or potential impact that any public-private interactions have had upon its non-military elements has not hitherto generated significant research. This contrasts with the US experience where there is already serious scholarly interest in

---

<sup>104</sup> See Chapter 2 for a discussion on the origins, definition and evolution of the MIC concept.

<sup>105</sup> Ledbetter, *Unwarranted Influence*, p.7

<sup>106</sup> Kinsey, *Private Contractors*, p.91

companies' involvement in contemporary security fields such as 'homeland security', cyber security and emergency preparedness, for example.<sup>107</sup>

Alternative approaches were considered before choosing the UK as the focus for this thesis. Firstly, the development of a comparative study - either a US-UK study, or one including other European case studies - was considered. Whilst future research along such lines might offer utility in further analysing the factors which account for public-private security cooperation in the non-military arena, the approach was not selected because room is needed to allow for a thorough investigation into the many, currently under-researched CT sub-sectors in the UK. Furthermore, this thesis is concerned with the question of whether the expressed system of public-private interaction has impacted upon security policy or expenditure, as traditional MIC theories assert, rather than on the question of how those influences may vary from country to country. A single country case study allows for a more considered analysis of the extent to which any 'industrial-complex' in the CT sector has had any such impact.

### 1.5 Research Questions

Given the ease with which existing accounts on the private sector's involvement in contemporary UK national security have presented the MIC as having made a simple linear transfer into the non-military aspects of UK national security strategy<sup>108</sup>, it was tempting to seek to examine theories on 'the SIC' against a testable hypothesis. However, as hypothesising solely on the *existence* of the MIC (and thus any supposed successor) is

---

<sup>107</sup> See especially Nathan Busch and Austen Givens, 'Public-Private Partnerships in Homeland Security: Opportunities and Challenges', *Homeland Security Affairs*, Vol.8 (October 2012); Jerry Brito and Tate Watkins, 'Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy', Mercatus Center Working Paper No.11-24, April 2011, Via: <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy> (accessed 24.06.11); and Ami Jihan Abou-Bakr, 'Managing Disaster: Public-Private Partnerships as a tool for disaster mitigation, preparedness, response and resiliency in the United States', PhD Dissertation, King's College London, 2011.

<sup>108</sup> See, for example, Danil's assertion that 'the 21<sup>st</sup> century neo-liberal military-industrial complex, it seems, has successfully permeated even our civilian life.' Danil, 'The arms trade and the military-industrial complex'

recognised to present a number of methodological challenges<sup>109</sup> - and was in any event also judged not to provoke sufficient examination into the characteristics and potential policy consequences of any such system - an alternative type of inquiry has been pursued. Whilst existing theoretical work on the MIC informs the analysis, the central, guiding research question that removes assumptions on whether the MIC has 'transferred' into the CT sector, and which seeks to examine the character of any 'industrial-complex' in this sector between 2002 and 2014 on its own terms, is therefore as follows:

- What are the origins, characteristics and consequences of the private sector's involvement in the (non-military) CT aspects of UK national security strategy?

Three more specific, supporting questions inform the analysis of the system under examination:

- Is the character of 'industry engagement' in the UK's CT sector comparable with 'defence'?
- Has any industrial-complex in the UK's CT sector exerted any 'unwarranted influence'?
- What are the consequences of any such system for researchers and practitioners?

Thus, this thesis examines the origins, character and consequences of the private sector's involvement in an individual sector (CT) of the non-military aspects of contemporary UK national security strategy. In so doing, it considers the extent to which the dynamics traditionally associated with the MIC - dynamics which have often been subjected to considerable criticism - exist in the non-military security arena. It develops a new approach, backed by micro-level empirical analysis of recent non-military, CT-related security contracts and other public-private dynamics in the UK, to cast new light on the private sector's involvement in contemporary national security. What has been labelled as 'the SIC' is reassessed, and in so doing the analysis offers new insights into why and how companies have become so involved in CT. Finally, the thesis contributes a new framework

---

<sup>109</sup> Levine notes that 'it is not sufficient to hypothesise the existence of the military-industrial complex' as 'some input or output variables must be related to that sub-system'. Edward P. Levine, 'Methodological Problems in Research on the Military-Industrial Complex' in Steven Rosen (Ed.), *Testing the Theory of the Military-Industrial Complex* (Lexington: DC Heath and Company, 1973), p.295

for analysing public-private cooperation in the security environment, as well as offering recommendations on how collaboration might be developed in this sector.

### **1.6 The scope of the thesis: public-private interactions in the UK's CT Strategy ('CONTEST')**

Given the challenges already identified around defining 'national security', it is important to clarify which parts of the UK Government's security agenda (and areas of public-private interaction) the thesis will focus upon. It is worth stressing that it would not be possible in the space available to properly analyse in detail *every* public-private interaction that has emerged in *all* fields of contemporary national security strategy; that is not the purpose of this research. Instead, the aim is to develop an approach that allows for investigation into a specific area of the private sector's involvement in the (under-researched) non-military aspects of the UK's national security strategy that might have wider application. This section justifies the selection of the private sector's involvement in CT as the focus of the research, placing it in the context of existing work in this field.

This thesis analyses some of the main public-private interactions to have emerged within the UK Government's CT strategy known as 'CONTEST' between 2002 and 2014.<sup>110</sup> Before embarking upon this work, it is important to recognise that the UK Government's CT policy framework underwent a radical upheaval throughout the 2000s. Most notably, a brand new overarching CT strategy was created and developed considerably during this time; this was in large part in response to the Al-Qaeda (AQ) related terrorist threat that had existed for some time, but that only really entered the public's consciousness on 9/11.

---

<sup>110</sup> Three iterations of CONTEST were published during this period: HM Government, 'Countering International Terrorism: The United Kingdom's Strategy', Cm6888, (London: TSO, 2006), Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/272320/6888.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/272320/6888.pdf) (last accessed 02.01.15); HM Government, 'Pursue Prevent Protect Prepare: The United Kingdom's Strategy for Countering International Terrorism', Cm7547, (London: TSO, 2009), Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228644/7547.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228644/7547.pdf) (last accessed 02.01.15); and HM Government, 'CONTEST: The United Kingdom's Strategy for Countering Terrorism', Cm8123, (London: TSO, 2011), Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/97995/strategy-contest.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf) (accessed 19.07.13)

The architect of the new strategy, David Omand, has recalled how he ‘launched work’ on what he called ‘CONTEST’ (an acronym he reveals was drawn from; COuNter-Terrorism SStrategy) in November 2002.<sup>111</sup> He explains how the new approach would be structured under the so-called ‘four Ps’:

By 2003, the UK government had its counter-terrorist strategy, CONTEST, with four strategic campaigns: Pursue (near term) and Prevent (longer term to reduce the likelihood of terrorist attack; Protect to reduce the vulnerability of the public and of national infrastructure to attack; and Prepare to reduce the impact and duration of disruption from attacks should they take place, integrating all the work done on civil contingencies and ensuring that the arrangements are well exercised.<sup>112</sup>

Alongside the establishment and development of CONTEST, the Government introduced (after the attacks on London on 7 July 2005 (7/7)) a significant change to the machinery of Government in the CT sector; Hennessy identifies that by 2007 the role of the Home Secretary had been strengthened considerably and that ‘a new Office for Security and Counter-Terrorism [OSCT] inside the Home Office would take over all responsibility for CONTEST from the Cabinet Office.’<sup>113</sup> As this thesis shows, private sector engagement has become a growing priority for the OSCT.

A full analysis of the aims, objectives and effectiveness of all aspects of CONTEST throughout its lifecycle is outside the scope of this thesis - its focus is restricted to analysing the private sector’s involvement therein - but two of its main aspects help to set the scene for this thesis’s analysis. Firstly, whilst the strategy was revolutionary it has been noted that, unlike in the US, it was never the intention of CONTEST to completely eradicate the risk of terrorism<sup>114</sup>; this might run contrary to the thinking of critics who believe that ‘the SIC’ has used the terrorist threat to justify the introduction of any or all unnecessary

---

<sup>111</sup> Omand, *Securing the State*, p.86

<sup>112</sup> Omand, *Securing the State*, pp.64-65

<sup>113</sup> Peter Hennessy, *The Secret State: Preparing For The Worst 1945-2010* (London: Penguin Books, 2010), p.379

<sup>114</sup> David Omand, ‘The Terrorist Threat to the UK in the Post-9/11 Decade’, *Journal of Terrorism Research*, Vol.3:1 (2012), Via: <http://ojs.st-andrews.ac.uk/index.php/jtr/article/view/412/371> (accessed 22.07.13)

CT measures. In short, its approach has consistently been ‘...to reduce the risk to the UK and its interests overseas from terrorism, so that people can go about their lives freely and with confidence.’<sup>115</sup> Secondly, CONTEST’s emphasis on achieving effective coordination across all the various UK government departments, agencies and other actors involved in countering terrorism has been rightly heralded as a major aspect of its effectiveness<sup>116</sup>; supporting this, the strategy has been in place for over 10 years and the Government’s independent reviewer of terrorism legislation has observed that its ‘four p’s’ ‘categorisation functions well’<sup>117</sup>. In short, any contemporary CT-focussed thesis must understand that CONTEST introduced a fundamentally new, often welcomed approach to UK CT policy, and that this was driven largely in response to AQ-related terrorism arising from 9/11. It was in this context specifically that arguments purporting to the emergence of ‘a SIC’ arose; hence why this thesis covers the years 2002-2014.

Whilst terrorism is only one of the contemporary security risks facing the UK, its selection as the main focus for this thesis is justified for four main reasons. Firstly, terrorism has been the highest priority UK security threat since 9/11; the UK has been ‘a prime Al-Qaeda target’<sup>118</sup> and the British Security Service’s (MI5) website has stated that AQ ‘...presents the single greatest threat to the UK.’<sup>119</sup> It is considered important, therefore, to consider how the Government has interacted with private companies in

---

<sup>115</sup> ‘Counter-terrorism strategy (CONTEST)’, Home Office Website, 12 July 2011, Via: <https://www.gov.uk/government/publications/counter-terrorism-strategy-contest> (accessed 14.11.14). Omand explains that ‘The UK counter-terrorism strategy contains an important implicit assumption, that there is no complete defence against modern determined terrorists[.]’ Omand, *Securing the State*, p.93

<sup>116</sup> CONTEST is cited as an exemplar of UK strategy-making in Shaw, *Britain in a Perilous World*, pp.30-32

<sup>117</sup> David Anderson, ‘The Terrorism Acts in 2011: Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006’, June 2012, Via: <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2013/04/report-terrorism-acts-2011.pdf> (accessed 01.01.15), p.28

<sup>118</sup> Paul Wilkinson, ‘The threat from the Al-Qaeda network’, in Paul Wilkinson (Ed.), *Homeland Security in the UK: Future preparedness for terrorist attack since 9/11* (Oxford: Routledge, 2007), pp.31-32

<sup>119</sup> ‘International Terrorism’, Security Service, Via: <https://www.mi5.gov.uk/output/international-terrorism.html> (accessed 24.02.12)

managing this threat, especially in view of (as the thesis shows) the substantial investment it has made in the field. Secondly, the UK Government's response to terrorism has drawn on the resources and capabilities of a wide variety of departments and agencies during the period under investigation; research on CT therefore allows for analysis of public-private security interaction beyond the defence arena. Thirdly, surveys suggest that terrorism has been the security issue attracting the most UK public interest from 9/11 to the present day; a 2011 Chatham House-You Gov survey found, for example, that the public continued to consider international terrorism as 'the overriding threat.'<sup>120</sup> Analysis of the private sector's involvement in addressing terrorism has simply not reflected this high level of UK public concern about the problem, reinforcing the idea that a major research 'gap' exists in this area. Finally, as the thesis shows, the private sector's involvement in CONTEST has been widespread, yet, notwithstanding some short scholarly contributions on this subject<sup>121</sup>, the significance of its interactions with the Government in this field has rarely been addressed.

Three main additional factors contributed to CT being chosen ahead of other non-military areas of contemporary security strategy also involving the private sector. Firstly, as suggested in Section 1.3 the private sector's support of the military aspects of UK security

---

<sup>120</sup> Chatham House, 'The Chatham House-YouGov Survey 2011, British Attitudes Towards the UK's International Priorities', July 2011, Via:

[http://www.chathamhouse.org/sites/default/files/0711ch\\_yougov\\_analysis.pdf](http://www.chathamhouse.org/sites/default/files/0711ch_yougov_analysis.pdf) (accessed 24.02.12), p.6

<sup>121</sup> See David Veness, 'The safety of the realm in retrospect and prospect', *RUSI Journal*, Vol.148:4 (2003), pp.14-17; Frank Gregory, 'Private sector roles in counter-terrorism' in Paul Wilkinson (Ed.) *Homeland Security in the UK*, pp.321-330; David Evans, 'The role of the private security industry', in Anthony Richards, Pete Fussey and Andrew Silke (Eds.), *Terrorism and the Olympics: Major event security and lessons for the future* (London: Routledge, 2011), pp.163-179; Paul Cornish, 'Technology, Strategy and Counterterrorism', *International Affairs* Vol. 86:4 (July 2010); Andrew Stewart, 'The UK Private Sector and the Threat from Terrorism' in Wyn Q Bowen and Andrew Stewart (Eds.), *Terrorism in the UK: Broadening the UK Government's Counter-Terrorist Response – CONTEST* (Swindon: Strategic and Combat Studies Institute, 2005), pp.69-77; Hugo Rosemont, 'Industry's role in counter terrorism', *Defence Contracts Bulletin*, Vol.9:22 (2011), pp.14-15; Rosemont, 'Private Sector Engagement'; Pauline Neville-Jones and Neil Fisher, 'Homeland Security and the Role of Business' in Esther Brimmer (Ed.), *Transforming Homeland Security: U.S. and European Approaches* (Washington, DC: Center for Transatlantic Relations, 2006).



policy has already attracted (and continues to receive) extensive academic coverage; it is judged that whilst a dedicated reassessment of the MIC could be timely, an investigation into the character of the private sector's involvement in the defence sector would add relatively limited value in an already crowded field. Secondly, the UK Government's engagement of the private sector on what it calls other 'wider security'<sup>122</sup> issues attracting significant investment - including, perhaps most notably, around the current major policy focus on cyber security - is only at an early stage of development. Indeed, a view existed amongst the majority of those practitioners interviewed for this thesis that the level of public-private interdependence in the cyber arena is perhaps more significant than in any other area of contemporary UK national security strategy. Such was the rapidly-evolving character of the UK Government's strategies on cyber security and other non-military security issues at the time of writing that it was judged that - unlike in the case of CT between 2002-2014 - it would be premature to accumulate and examine data in such fields. Reliable material on the full scope of public-private engagement in this sector is not yet available, and time is needed to see how contracts issued in this sector will play out over the course of their lifecycle. Finally, it is noticeable that despite the private sector's extensive involvement in CONTEST, its potential impact upon UK CT policy (or related investment decisions) has attracted almost no serious academic contemplation to date.<sup>123</sup> This ongoing gap in analysis, well over a decade after 9/11, allows the researcher to make a significant new contribution through the use of new, under researched case studies.

Before outlining this thesis's analytical approach, it is customary for any CT-related dissertation to recognise that debates are ongoing around what actually constitutes

---

<sup>122</sup> Other 'wider security' risks identified by the UK Government's include, for example; cyber security, civil emergencies, energy security, organised crime and border security. HM Government, 'Securing Britain in an Age of Austerity', p.41

<sup>123</sup> The two main exceptions are arguably Dunne and Sköns, 'The Military Industrial Complex' and Neocleous, 'Security, Commodity, Fetishism'; albeit neither provides systematic empirical analysis.

'terrorism'; this is relevant for this dissertation because how, otherwise, can the character of the private sector's role in CT be properly considered if we do not sufficiently understand the difficulties of defining terrorism is in the first place? The challenges associated with this endeavour have been well documented in many leading accounts in the field, including Schmid and Jongman's major work; *Political Terrorism*. In the interests of space, their masterful (albeit rather lengthy) definition is not reproduced here; even the authors concede when presenting their end product that '[s]ome will find this too complex a definition, with too many elements included'<sup>124</sup>. However, comparing other prominent definitions neatly illustrates the difficulties identified by Schmid and Jongman. In *Inside Terrorism*, for example, Hoffman devotes a chapter to the question of 'defining terrorism', concluding:

We may therefore now attempt to define terrorism as the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change.<sup>125</sup>

Wilkinson adopts a different emphasis in *Terrorism Versus Democracy*:

Terrorism is the systematic use of coercive intimidation, usually to service political ends. It is used to create and exploit a climate of fear among a wider target group than the immediate victims of the violence, as well as to coerce a target to acceding to the terrorists' aims.<sup>126</sup>

Here, two of terrorism studies' most prominent scholars vary in how they characterize terrorism; they differ in terms of the rigidity with which they see such acts as always necessarily 'political'. Other leading academics have recognised the problem. Richards has recently published a comprehensive discussion of the challenges associated with defining

---

<sup>124</sup> Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature* (New Jersey: Transaction Publishers, 1998), p.28

<sup>125</sup> Bruce Hoffman, *Inside Terrorism: Revised and Expanded Edition* (New York: Columbia University Press, 2006), p.40

<sup>126</sup> Paul Wilkinson, *Terrorism Versus Democracy; The Liberal State Response* (London: Frank Cass, 2005), pp.12-13

terrorism<sup>127</sup>, for example, and, summarizing the situation, Gearson has argued that ‘there remains no agreed definition’<sup>128</sup> of terrorism and that ‘[t]he question of what is (and what is not) terrorism has, for many, disappeared down an academic dead end’<sup>129</sup>. Horgan has also neatly observed that ‘[w]hile terrorism is an accepted concept, it remains unclear and inconsistent.’<sup>130</sup>

It seems clear, therefore, that there is little prospect of a singular definition of terrorism ever being agreed upon; Andrew Silke recently summed up well in concluding that the definition of terrorism has ‘never been resolved’ and that ‘it never will be’.<sup>131</sup> Whilst as Richards argues engaging in this definitional debate does have utility at the policy level<sup>132</sup>, an important point to acknowledge is that this lack of agreement poses challenges for any terrorism-related study seeking to justify the inclusion of certain case studies within its scope. Nevertheless, in the interests of clarity (and despite any possible limitations and dangers of doing so) this thesis adopts an institutional understanding of terrorism (and CT); it focuses on the UK Government’s understanding of the threat of terrorism since 9/11, and on the public-private interactions that have been fostered in this context. Against this background, the thesis’ framework for analysis can be presented.

## **1.7 Framework for analysis**

### *Existing approaches*

Several theoretical frameworks or approaches already exist for analysing private actors’ involvement in the provision of security. In the field of sociology, for example,

---

<sup>127</sup> Anthony Richards, ‘Conceptualizing Terrorism’, *Studies in Conflict and Terrorism*, Vol.37:3 (2014), pp.213-236

<sup>128</sup> John Gearson, ‘The Nature of Modern Terrorism’ in Lawrence Freedman (Ed.), *Superterrorism: Policy Responses* (Oxford: Blackwell Publishing Ltd, 2002), p.8

<sup>129</sup> Ibid.

<sup>130</sup> John Horgan, *The Psychology of Terrorism* (Oxford: Routledge, 2005), p.22

<sup>131</sup> Andrew Silke, ‘The Golden Age? Assessing the State of Terrorism Studies’, Keynote Speech at 7<sup>th</sup> Annual Conference of Society of Terrorism Research, London, 27 June 2013.

<sup>132</sup> Richards ‘Conceptualizing Terrorism’, pp.213-236

Wood and Dupont have put forward a 'nodal governance' approach for the study of power that 'can be public, private, hybrid or yet uncategorized.'<sup>133</sup> Given the range of private actors that are involved in CONTEST, the manner in which the approach encourages '[a] comprehensive empirical 'mapping' of existing governance nodes and networks within specific sites'<sup>134</sup> as one of its primary methodological attributes is an attitude that has been adopted in this thesis. Similarly, Krahmman is also a recognised leading contemporary theorist who has charted the shift from 'government' to 'governance' in security. She identifies a 'greater role for private actors'<sup>135</sup> in security and characterises governance as 'the fragmentation of political authority among a diversity of public and private actors across levels of analysis.'<sup>136</sup> Her argument that 'governance denotes the non-hierarchical co-ordination of social relations and the fragmented provision of public services by a multitude of public and private actors'<sup>137</sup> is an appreciation that will also be applied in this thesis. Finally, Abrahamsen and Williams offer the concept of 'global security assemblages' to characterise the structure of contemporary security policy relationships; these are 'transnational structures and networks in which a range of different actors and normativities interact, cooperate and compete to produce new institutions, practices and forms of deterritorialized security governance.'<sup>138</sup> Whilst in its theoretical outlook this thesis declines to differentiate between 'domestic' and 'transnational' entities, the recognised possibility that multiple actors (including the private sector) can cooperate in

---

<sup>133</sup> Jennifer Wood and Benoit Dupont (Eds.), *Democracy, Society and the Governance of Security* (Cambridge: Cambridge University Press, 2006), p.x

<sup>134</sup> Jennifer Wood, 'Research and innovation in the field of security: a nodal governance view' in *Ibid.* p.230

<sup>135</sup> Elke Krahmman, 'Conceptualizing Security Governance', *Cooperation and Conflict: Journal of the Nordic International Studies Association*, Vol. 38:1 (2003), p.19

<sup>136</sup> *Ibid.* p.19. Shearing is similarly sceptical of the solely 'state-centred view of governance.' Clifford Shearing, 'Reflections on the refusal to acknowledge private governments' in Wood and Dupont, *Democracy, Society and the Governance of Security*, p.13

<sup>137</sup> Krahmman, 'Conceptualizing Security Governance', pp.5-6

<sup>138</sup> Abrahamsen and Williams, *Security Beyond the State*, p.90

groupings of security provision is applied in this study on the CT aspects of UK national security.

#### *A nuanced approach*

Despite these important contributions, it is judged that an even more nuanced approach is needed to analyse the origins, character and consequences of any 'industrial-complex' operating in non-military fields of national security such as CT. Whilst some research on *military* issues has shown how threat perceptions and economic considerations have affected the levels of (and account for changes in) defence expenditure<sup>139</sup> - and, separately, analysis has suggested that industry often underestimates (or that there exists a 'conspiracy of optimism' around) the 'true' cost of programmes at the bidding stage of UK *military* acquisitions<sup>140</sup> - the extent to which such (or similar) dynamics exist and/or bear influence upon CONTEST has not previously received systematic empirical analysis. Furthermore, an unjustifiably narrow attitude currently exists around how research should be pursued in respect of public-private cooperation on security issues; there is currently an over-emphasis on inquiry into the PMSC sector and even leading security scholars who encourage a broader perspective argue, for example, that 'little is gained by broad-brush analyses that treat all forms of security privatization as the same.'<sup>141</sup> Whilst this argument has merit in the sense that the private sector's involvement in some non-military aspects of national security differ to defence, the framework for this thesis is established in the belief that from a policy perspective there is much to be gained by striving to look more holistically at security privatisation *across* national security strategy. For the sake of effective strategy-making, policymakers and

---

<sup>139</sup> Ernest Schneider, 'Causal Factors in Variations in US Postwar Defense Spending', *Defense Analysis*, Vol. 4:1 (1988), pp. 53-79

<sup>140</sup> Antonia Feuchtwanger, *The Best Kit: Why Britain's Defence Doesn't Need an All-British Defence Industry* (London: Policy Exchange, 2004), p.60; and Francis Tusa, 'Buying Defence', BBC Radio Documentary, 27 Dec. 2011, Via: <http://www.bbc.co.uk/programmes/b017mtfc> (accessed 16.08.12)

<sup>141</sup> Abrahamsen and Williams, *Security Beyond the State*, p.38

outside observers should be able to consider and assess the potential implications of the totality of these extensive (not to mention potentially interdependent) public-private security relationships; both within and beyond the defence sector.

### *Bespoke design elements*

A first key characteristic of this thesis' analytical approach, therefore, is that it seeks to include all those parts of the 'private sector' that interact with the Government on selected CT issues. Unlike the MIC - which as Chapter 2 explains is generally characterised as a three-way system comprising the Executive, the Legislature and the DIB - the thesis agrees with other authors who argue that the private sector plays a 'multiplicity of roles'<sup>142</sup> in UK national security, and that these extend beyond the supply contributions of the 'security industry'. The framework therefore seeks to build on the pioneering work of Omand to examine how in selected CT sub-sectors the UK Government has directly engaged, or has an interest in interacting with *three* main categories of private companies in relation to national security strategy<sup>143</sup>: 1) Interactions (including contracts) with security suppliers (of all sizes) on non-military capacity and capability issues ('Private Suppliers'); 2) Interactions with the private organisations responsible for (or with a direct interest in) operational security delivery in the UK ('Private Operators') - a category which includes those private sector organisations comprising the critical national infrastructure (CNI); and 3) Interactions with wider business sectors on various corporate security and resilience matters ('Wider Business'). Recognising that the remit (or business objectives) of some companies' operations may extend to more than one of these categories, and that the commercial motivations within or between them may vary; the involvement of actors

---

<sup>142</sup> Neville-Jones and Fisher, 'Homeland Security and the Role of Business', p.170

<sup>143</sup> This builds on Omand, 'What is the Future for the CNI?', which argues that both suppliers and operators play important roles in supporting Government on security ('The Omand Triangle').

falling within each of these three groupings is examined within each field of CONTEST under investigation.<sup>144</sup>

The second main design element of this thesis' organising framework is that, having selected them according to the rationale listed in Section 1.8, the empirical sections covered in Chapters 3-5 are deliberately organised *thematically* to allow for detailed analysis of three CT sub-sectors. In addition to allowing room for detailed contextual analysis to be completed on each of the three selected sub-sectors (Emergency Preparedness, Border Security and Olympic Security), this decision was also taken with the intention that the approach might be adapted for future research into the private sector's role in mitigating other security risks (such as, for example, cyber security or serious organised crime). At one level, therefore, it is unimportant which specific thematic security issue is selected for investigation at the empirical level; this thesis has selected terrorism (and the response to it) for the reasons articulated in Section 1.6.

The final main aspect of the design of this thesis' framework is that - in addition to examining (as Section 1.8 explains) the main strategic interface between Government and industry on CT issues after 9/11 ('RISC') and a number of other cross-cutting 'issues of concern' across the CT sector - the public-private dynamics which emerged around a selection of large, CT-related public sector security contracts are analysed within each of the three selected CT sub-sectors; this allows for substantive new analysis to be completed in a similar manner to the way in which government-industrial dynamics around defence contracts have previously been examined.<sup>145</sup>

By developing and utilising a framework that analyses the origins, characteristics and consequences of the private sector's involvement in selected areas of CT, this thesis

---

<sup>144</sup> The author is grateful to Mark Erbel for his helpful comments on how these categories might overlap.

<sup>145</sup> See, for example, Feuchtwanger, *The Best Kit*.

casts new light on an important area and also offers an approach that can be adopted for the study of other contemporary security issues. It is easy to say that the private sector is involved in many other diverse aspects of security strategy; its involvement has recently been shown to include, for example, the supply of intelligence-related services<sup>146</sup>, the provision of support to humanitarian organisations<sup>147</sup>, and in anti-terrorist financing.<sup>148</sup> However, the priority now must be to address the fact that the precise character of the roles, motivations and any impact that private interests (and/or any broader coalition) have exerted in these fields is under-researched.

After conducting its empirical analysis of companies' involvement within CONTEST, the thesis concludes with a summary of the origins, characteristics and consequences of the 'industrial-complex' operating within the UK CT sector. The thesis will demonstrate that an 'industrial-complex' of a different character to the MIC exists in the CT aspects of UK national security strategy; what has happened since 9/11 is thus not simply a linear transfer of the MIC into the non-military security arena. This perspective suggests that the use of the term 'the SIC' may be unsustainable and presents significant implications of policymakers and the research community.

### **1.8 Structure of the thesis and case study selection**

Having presented the thesis' argument, conceptual framework, case study selection and methodology in this introduction, the remainder of the thesis is structured as follows:

#### *The British Military-Industrial Complex and its Evolution*

---

<sup>146</sup> Simon Chesterman, "'We Can't Spy... If We Can't buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Government Functions'", European University Institute (EUI) Working Paper (AEL 2009/2), Via: [http://cadmus.eui.eu/bitstream/handle/1814/11403/AEL\\_2009\\_02.pdf?sequence=1](http://cadmus.eui.eu/bitstream/handle/1814/11403/AEL_2009_02.pdf?sequence=1) (accessed 22.05.11)

<sup>147</sup> Birthe Anders, 'Private Military and Security Companies and Humanitarian Organisations: Partners in Aid?', *World Defence Systems* (2010:2)

<sup>148</sup> Oldrich Bures, 'Private Actors in the Fight Against Terrorist Financing: Efficiency Versus Effectiveness', *Studies in Conflict and Terrorism*, Vol.35:10 (2012), pp.712-732



Chapter 2 provides an introduction to the theoretical underpinnings of the MIC; introducing the reader to the origins of the concept and analysing both its relevance and evolution in a UK context. It considers the similarities, differences and potential overlap between the British MIC and its US counterpart, before further highlighting differing attitudes towards - and the difficulties associated with defining - the concept in a contemporary setting.

### *Empirical Analysis of Three CT Policy Fields*

Chapters 3-5 analyse the private sector's involvement in three selected sub-sectors of CONTEST. Empirical analysis on public-private interactions is conducted as follows: Firstly, the governance arrangements for the approach in each area is presented, including an outline of the roles of the main 'actors' involved in the strategy; secondly, a 'snapshot' is provided of the main elements of the UK's strategic approach in each area since 9/11; third, the thesis presents an indication of the levels of expenditure that have been allocated during the period under study; fourth, empirical analysis is conducted in the spirit of a 'map-making enterprise'<sup>149</sup> on the interactions that have arisen between the Government and 'private suppliers', 'private operators' and 'wider business' - as stated above, particular attention is given to the dynamics which have emerged around amongst three of the most valuable identified CT-related security contracts<sup>150</sup>; finally, analysis is conducted on the character and potential impact of the 'industrial-complex' in each area.

There are five main reasons for the selection of the three specific CT policy areas (Emergency Preparedness, Border Security and Olympic Security) within which analysis of major CT-related contracts and other public-private interactions is conducted:

- All three areas have been routinely addressed as core aspects of CONTEST;

---

<sup>149</sup> Wood, 'Research and innovation in the field of security', p.220

<sup>150</sup> These are e-Borders, the IT aspects of the 'FiReControl' project, and the G4S Olympic Security contract.

- All three areas have been routinely addressed as core aspects of the CT research agenda;
- Each area received significant new levels of monetary/financial investment after 9/11;
- Three of the largest post-9/11 CT-related public sector contracts were let in these fields; and
- Each area includes the three main types of public-private interaction identified in this thesis.

### 1. Core CONTEST themes

The UK Government's policy documentation clearly shows that the three selected themes were quickly established (and have routinely featured) as core elements of CONTEST. For example, the first published version (2006) of CONTEST explicitly includes 'border security' as one of the 'range of issues' within the PROTECT strand of the strategy, stating the following priority:

Strengthening border security – so that terrorists and those who inspire them can be prevented from travelling here and we can get better intelligence about suspects who travel, including improving our identity management, for example by use of biometrics[.]<sup>151</sup>

The same iteration of CONTEST is equally transparent about its emphasis on 'emergency preparedness'; a 'text box' spreading across three pages detailed the work being undertaken to 'build resilience across all parts of the United Kingdom.'<sup>152</sup>

The inclusion of 'Olympic Security' within a CT-focused study might at first seem to be a rather tenuous selection. Whilst it is apparent that Olympic Security comprises more issues than CT, it can be observed that from as early as 2004 the responsibility for the security governance aspects of the project lay firmly within the purview of the Home Office, and that CT was always a core, if not primary aspect of the planning. That the OSCT was formally tasked with overseeing the security strategy for London 2012 in 2008 confirms its relevance for this thesis.

---

<sup>151</sup> HM Government, 'Countering International Terrorism: The United Kingdom's Strategy', p.2

<sup>152</sup> Ibid. pp.26-27

## 2. Core CT Research Themes

Respected scholarly material validates the relevance of the three selected sub-sectors as core CT themes; each has regularly appeared in leading terrorism journals.<sup>153</sup> A separate useful indication that they are *core* aspects of the CT research agenda is to be found in the work of leading figures in the field. Paul Wilkinson's 2007-edited, policy-orientated volume, *Homeland Security in the UK*, for example, places a significant emphasis on emergency preparedness issues; the subtitle of the work is 'Future Preparedness for Terrorist Attack since 9/11' and two sections of this major work are concerned with emergency preparedness and response respectively<sup>154</sup>. Separately, a group of prominent UK terrorism researchers have recently compiled a respected volume on 'Terrorism and the Olympics'<sup>155</sup>; this established 'major event security' as a core aspect of terrorism research.

## 3. Transparent, additional CT Expenditure

In its consideration of the 'SIC' concept, this thesis examines the private sector's involvement in CT through an analysis of three sub-sectors that have received sizable amounts of new *public expenditure* after 9/11. The fourth reason that the three themes have been selected, therefore, is because (as Chapters 3-5 show) these aspects of CONTEST have all attracted substantial levels of financial investment from the public sector. The selection of CT themes which can demonstrate large amounts of new investment is an important consideration for any thesis considering whether the commercial interests of companies (and/or any wider coalition of interests) have affected policy or expenditure.

---

<sup>153</sup> For example, the three selected themes have featured regularly in the journal *Terrorism and Political Violence* (number of references in brackets): 'Border Security' (375), 'Emergency Preparedness' (30) and 'Olympic Security' (34) <http://www.tandfonline.com/> (04.09.13)

<sup>154</sup> Paul Wilkinson (Ed.), *Homeland Security in the UK: Future preparedness for terrorist attack since 9/11* (London: Routledge, 2007)

<sup>155</sup> Richards et al, *Terrorism and the Olympics*

It was also judged in selecting these themes that access to financial data in these sectors, whilst sensitive, would be considerably less impenetrable than other areas of CT attracting new investment after 9/11 such as, for example, intelligence and cyber security.<sup>156</sup>

#### 4. Large, accessible non-military contracts

The fourth main reason for choosing the three selected themes is because they have each exhibited examples of some of the largest, non-military (i.e. non-MoD), CT-justified security contracts to be let in the sector after 9/11. As already suggested, the purported existence of disproportionate levels of expenditure is an important characteristic of the MIC in the eyes of critics, and indeed those who have been concerned that its dynamics have transferred into the non-military security sector. Whilst this thesis does not draw the same conclusions as such authors, it chooses to engage on the same issues; in other words, it judges that it is helpful to examine the public-private dynamics around some of the *largest* public sector contracts to be let in the sector.

In considering this aspect of case study selection, confidence was needed that data pertaining to the contracts would be available. It is understandable that some UK security contracts are of such a sensitive nature that budgetary and contract information is not easily accessible; it might also be inappropriate to analyse and/or publish any such details. The FiReControl, e-Borders, and London 2012 G4S contracts - identified within the 'Emerging Preparedness', 'Border Security' and 'Olympic Security' themes respectively -

---

<sup>156</sup> Data pertaining to contracts let by the UK intelligence agencies is restricted, for example, as evidenced by the redactions of all budgetary/cost figures relating to sensitive programmes within the annual reports of the Parliamentary Intelligence and Security Committee. See, for example, Intelligence and Security Committee, 'Annual Report 2010-2011', July 2011, cm8114, Via: <http://isc.independent.gov.uk/committee-reports/annual-reports> (accessed 15.11.14), p.25

were all selected on the basis that, in contrast to some more sensitive contracts<sup>157</sup>, data was known to be available in the public domain.

In selecting non-military CT contracts for examination, consideration was also given to whether their associated costs had grown substantially during their lifetime (i.e. in line with MIC theory which purports to its ability/desire to inflate costs); as illustrated below, this clearly occurred in all three cases. Each contract therefore provided the opportunity to examine in the security sector the potential causes of such rising expenditure.

### 5. Three private dimensions

The final reason for choosing the three selected CT themes is that they each appeared to exhibit all three types of public-private interaction that it is argued help to characterize the operation of the UK's non-military security sector. As argued by the author in a similar way elsewhere<sup>158</sup>, the 'security industry' in the UK (in contrast to the defence sector) should be seen to comprise a wide range of technology providers and other contractors ('Suppliers') operating alongside a variety of other private sector actors such as infrastructure companies ('Private Operators') and other sectors of the economy ('Wider Business'); all of which play important roles in the non-military security arena. The empirical chapters which follow seek to explore these interactions within each theme.<sup>159</sup>

### *Empirical Analysis of Strategic Engagement (RISC)*

---

<sup>157</sup> For example, the contracts developed under 'Programme Cyclamen' for UK border security screening

<sup>158</sup> Rosemont, 'Private Sector Engagement', pp.157-8

<sup>159</sup> Chapter 5 shows, for example, how for London 2012 the Organising Committee for the Games ('LOCOG') was a private company (an 'operator') responsible for contracting with the private security company G4S (a 'supplier') for the largest security contract associated with the Games. These interactions developed alongside other security initiatives developed between the government and 'Wider Business' sectors.

Chapter 6 analyses the origins of the main current mechanism of strategic engagement created between the UK Government and the security industry on CT issues after 9/11 - the UK Security and Resilience Industry Suppliers' Community (RISC) - analysing its development and leading practitioners' perceptions of its utility and effectiveness to date. Analysis of RISC was judged to be necessary because, prior to this thesis, no research had been conducted previously on the origins, role and potential impact of this main strategic channel of communication between UK Government and industry on CT issues. By analysing the historical foundations and activity of RISC within a dedicated, bespoke chapter - an analysis that is conducted in a similar manner to that recently completed on strategic Government-industry engagement in the military arena<sup>160</sup> - the thesis addresses a research gap on strategic-level public-private interaction in CONTEST.

#### *Empirical Analysis of Three Areas of Concern*

Chapter 7 analyses three additional areas of concern in the CT arena that have been traditionally associated with the MIC and the SIC, and which either 'cross-cut' or have developed outside the three selected policy areas: the employment movement dynamics associated with the 'revolving door'; economic considerations relating to UK CT Strategy (including the operation of the security procurement system); and CT-related security exports. Research on these topics is justified because, firstly, whilst the implications of the movement of officials between Government and the private sector have been considered in a US Homeland Security context<sup>161</sup> - what has been labelled the 'Revolving Door'<sup>162</sup> dynamic - these are under-examined in respect to CONTEST. Secondly, evidence is provided on how job creation and wider economic considerations have (or have not) featured in the UK's non-military CT field generally, and in the context of the three

---

<sup>160</sup> Abou-Bakr, 'Managing Disaster', especially pp.138-174

<sup>161</sup> See Paul R. Verkuil, *Outsourcing Sovereignty: Why Privatization of Government Functions Threatens Democracy and What We Can Do About It* (New York: Cambridge University Press, 2007)

<sup>162</sup> *Ibid.* p.36

selected CT-related contracts in particular; this helps to establish whether the dynamics associated with the MIC have ‘transferred’ into the security sector. Finally, it has recently become increasingly apparent that the UK Government’s engagement with industry on CT-related security exports is growing as a political priority; this dynamic has been considered in research conducted in the defence sector<sup>163</sup>, but not yet substantially in the equally sensitive non-military aspects of UK security policy.

### *Conclusion*

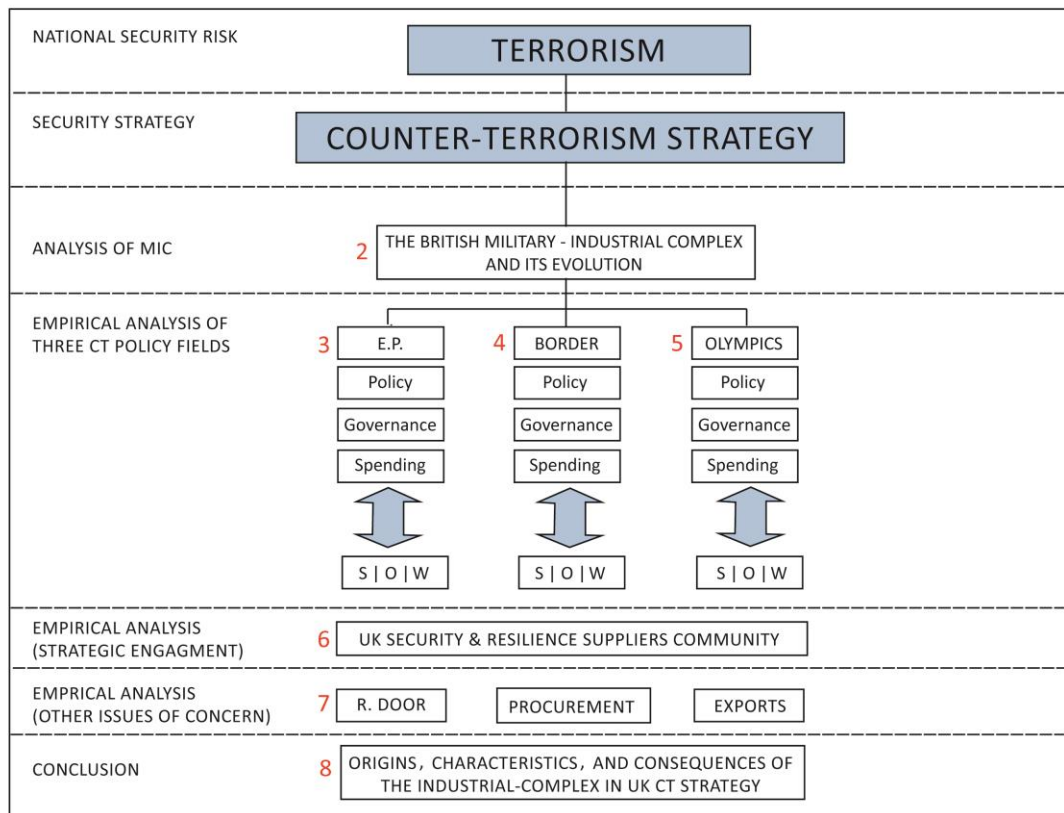
The conclusion presents the thesis’s final assessment of the origins, characteristics and consequences of the ‘industrial-complex’ within the CT aspects of the UK’s national security strategy. It presents the rationale for public-private cooperation in the post 9/11 period, and summarizes how the involvement of the private sector has impacted on CONTEST in several respects. Overall, the dissertation found little evidence that any significant ‘unwarranted influence’ has been exerted on policy development or specific investment decisions. Some final observations are offered on the system’s consequences for policymakers, researchers, political accountability, and what the ‘industrial-complex’ in the CT sector might say about the proposition that a wider ‘SIC’ is operating across UK national security strategy more broadly.

It is against this backdrop that the framework for the completion of this thesis (together with its selected case studies) can be visualised, as per Figure 1 below.

---

<sup>163</sup> See, for example, Dan Smith and Ron Smith, *The Economics of Militarism* (London: Pluto Press, 1983); Malcolm Chalmers, Neil V Davies, Keith Hartley and Chris Wilkinson, ‘The Economic Costs and Benefits of UK Exports’, *Fiscal Studies*, Vol.23:3 (2002), p.343; and Stephen Martin, ‘The subsidy savings from reducing UK arms exports’, *Journal of Economic Studies*, Vol.26:1 (1999).

**Figure 1: Framework for analysing private sector involvement in CONTEST<sup>164</sup>**



### 1.9 Potential limitations arising from case study selection

Several CT themes are not addressed for reasons of space, and also because they included few examples of such varied, multi-dimensional public-private interaction. The author declined, for example, to include (amongst others) ‘CT Policing’ as one of the thematic chapters; whilst there was substantial additional public sector expenditure in this area after 9/11, this theme did not appear to exhibit many of the sorts of relationship with companies that are relevant to this thesis. Similarly, the field of ‘Aviation Security’, whilst enormously important, was also not chosen on the grounds that the Government is not a

<sup>164</sup> EP = Emergency Preparedness. BORDER = Border Security. R. DOOR = Revolving Door. S | O | W denotes how Chapters 3-5 will conduct analysis of the involvement of ‘Private Suppliers’ (S), ‘Private Operators’ (O) and ‘Wider Business’ (W), as described in section 1.7. Red numbers denote chapter numbers.



substantial purchaser in this sector - rather it is the policy lead and regulator. Indeed, it was not possible to identify a significant public sector contract in the UK aviation security sector that would allow for examination of such public-private dynamics.

Whilst the fact that not all of the public-private sector dynamics in CT are the same, or indeed covered, might present limitations in the sense that this thesis is not fully representative of the entire sector - thus potentially complicating the overall argument that something resembling an 'industrial complex' exists across the CT sector - the dissertation nevertheless makes an original contribution through analyses in the available space of an under-researched selection of case studies, and opts simply to recognise that diversity is clearly evident. It deliberately focuses on those important parts of the sector where both the public and private sectors are substantial purchasers, and where other business sectors are also clearly engaged. In recognizing at the outset that the State is not a major purchaser in some areas of CT, one can already begin to see how a problem exists with the apparently seductive idea that the MIC has simply linearly transferred into the non-military aspects of national security creating an SIC.

#### **1.10 Sources and methodology**

The thesis analyses a wide range of primary and secondary sources including academic and journalistic literature, think tank reports and journals, conference programmes and speeches, company press releases, media reports, Parliamentary reports, meeting minutes, employment advertisements and trade publications. All of these sources are valuable in revealing the multitude and character of the public-private interactions that exist in the UK's CT sector.

Owing to the existing shortage of data on the operation (and attitudes pertaining to the role and impact) of public-private interaction in UK national security strategy outside

the defence sector, it was decided that the generation and analysis of additional primary material should be an essential component of the research. In addition to analysis of relevant, publicly-available Government and private sector speeches, documentation and websites, the thesis' methodology incorporated as a primary data collection mechanism a programme of 26 semi-structured, in-depth elite interviews with leading figures in the UK security sector (listed in Appendix A). As outlined in Appendix B, potential interviewees were invited to participate after they were identified - on the basis of their biographical data - as experts on, and/or seen to be directly engaged in, the areas of public-private CT cooperation under examination in this thesis.

The thesis followed the elite interviewing approach introduced by Lewis Anthony Dexter<sup>165</sup> and the purpose of conducting an interview programme was twofold. Firstly, it provided a useful mechanism through which additional areas of public-private cooperation in the CT sector could be identified and analysed. Secondly, the interview programme generated in a project-oriented, semi-structured manner a selection of hitherto unheard leading figures' views on the character, effectiveness and consequences of the public-private interactions that have arisen in (and beyond) the CT arena.<sup>166</sup> Interviews were sought and arranged with individuals from the following constituent groups:

- Current/former Government policymakers/officials involved in CT/national security strategy;
- Current/former senior industrialists involved in CT/national security strategy;
- Current/former senior trade association figures operating in CT/national security sector; and
- Prominent academic experts on the private sector's involvement in CT/national security strategy.

---

<sup>165</sup> Lewis Anthony Dexter, *elite and specialized interviewing* (Colchester: ECPR Press, 2006). Tips and guidance were also drawn from David Richards, 'Elite Interviewing: Approaches and Pitfalls', *Politics*, Vol.16:3 (1996), pp.199-204; and Philip H.J. Davies, 'Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services', *Politics*, Vol.21:1 (2001), pp.73-80

<sup>166</sup> A breakdown of the number/categories of participants (including their willingness to be quoted or participate under the condition of anonymity) and a list of interview questions appear in Appendix B.

The interview programme received ethical approval from King's College London's War Studies Group Research Ethics Panel<sup>167</sup> and was justified because, as argued from the outset, the quantity and quality of primary research material arising from the field was lacking prior to this thesis. In addition, whilst after 9/11 there was (and continues to be) considerable criticism of 'the SIC', no academic dissertation has (to the researcher's knowledge) hitherto sought to provide balance through incorporating the attitudes of leading figures from *within* government and industry on the character and impact of the public-private relationships that exist in the UK's CT arena, alongside external analysis and comment.

In short, an additional research mechanism was needed which could take account of the nuances of, and attitudes within, the CT aspects of national security strategy, and which could generate primary research material in a timely manner; other methodological approaches (such as written surveys or questionnaires) were rejected as they were considered likely to have simply not captured the philosophical considerations that the thesis explores, and that has helped the author to make an original contribution to the field.

---

<sup>167</sup> Key aspects of this process also appear in Appendix B.

## Chapter 2: The MIC and its evolution in a UK context

### Introduction

This chapter introduces existing theory on, and the characteristics of, the 'classic' MIC, outlining how the theoretical proposition of this thesis - the emergence of a different 'industrial-complex' in the UK CT sector - relates to this concept but possesses a different set of overall characteristics. To explore these dynamics, the chapter introduces the differing historical conceptual treatments of the MIC, presenting it as a contested concept and arguing that it should not be considered as a solely US phenomenon; a 'British MIC' has existed (and evolved) in the UK defence sector. The final section recalls how the UK Government has broadened its approach to national security in recent decades, arguing that it has sought to engage with a wide range of industry actors on various emerging non-military security issues such as CT. The chapter concludes with further context and a presentation of this thesis's argument that some but not all of the dynamics traditionally associated with the MIC are present within the contemporary CT arena.

### 2.1 Introducing the 'MIC' - concept and theory

The idea of the existence of a self-serving, potentially sinister 'MIC' has become deeply engrained in the popular imagination. US President Eisenhower's farewell address in 1961 is widely cited as the origin of this infamous phenomenon and its implicitly dangerous connotations; more often than not the concept is seen as at worst 'a self-conscious conspiracy acting mainly in its own self-interest'<sup>1</sup> or, at best, as 'a network of public and private forces that combine a profit motive with the planning and implementation of strategic policy.'<sup>2</sup> Unquestionably, Eisenhower's remarks have been (and continue to be)

---

<sup>1</sup> Steven Rosen, 'Testing the Theory of the Military-Industrial Complex', in Rosen (Ed.), *Testing the Theory*, p.3

<sup>2</sup> Ledbetter, *Unwarranted Influence*, p.6

taken as a dire warning over the potential dangers he saw arising in the early 1960s. His concerns are expressed in perhaps the most widely-cited passage of his original speech:

In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. The potential for the disastrous rise of power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes.<sup>3</sup>

These remarks, whilst quite general in nature, have invited powerful ideas to be formed around how there is great potential for power to be abused in the national security arena. But whether the MIC (or any potential successor, like ‘the SIC’) should be understood this way or ‘...not best understood as a conspiracy, but as a subtle interplay of interests and perceptions’<sup>4</sup>, what did Eisenhower mean by the phrase? An analysis of the history of the MIC and the theories associated with the concept illustrates how elusive it has become to reach a singular, agreed definition.

Whilst the expression, ‘the MIC’, was coined historically only recently, it is important to recognise that the idea of necessary interaction between ‘public’ and ‘private’ enterprise in the pursuit of military or wider strategic objectives has long existed; Parrott has documented, for example, ‘the centrality of mercenaries (...) in early modern armies’<sup>5</sup> and the rarity of States to become directly involved in the production of military goods in Europe at that time.<sup>6</sup> Recognition of the existence of these dynamics has also been noted in accounts of national security-related public-private coordination in pre-Cold War US history; one recent work has documented how during the First World War, for example, a

---

<sup>3</sup> Dwight D Eisenhower, ‘The military-industrial complex’ 17 January 1961, radio and television broadcast from Washington, DC, USA in *Chambers Book of Speeches* (Edinburgh: Harrap Publishers, 2006), p.288

<sup>4</sup> Rosen, ‘Testing the Theory’, p.24

<sup>5</sup> David Parrott, *The Business of War: Military Enterprise and Military Revolution in Early Modern Europe* (Cambridge: Cambridge University Press, 2012), p.29

<sup>6</sup> *Ibid.*, pp.202-203

‘War Industries Board’ was created ‘to resolve how to harness together industry and the military to ensure that the United States was mobilized[.]’<sup>7</sup>

Whilst the MIC expression was coined in (and is arguably still most associated with) the US experience, the existence of military-industrial coordination has not only been considered in this context; according to Roland, ‘military-industrial complexes have been sighted on every continent and as far back in history as the Middle Ages.’<sup>8</sup> For example, the dynamics of the Russian MIC during the Soviet era have been documented<sup>9</sup> and, when considering the UK policy implications of the Defence Industry’s post-Cold War position, Latham explains that from the late 1940s various ‘Governments (...) were dependent on their national industries for delivering the means of providing military power.’<sup>10</sup> For this thesis, therefore, we should be sceptical of any effort to deny the existence of ‘the MIC’ outside the US - the need for military-industrial coordination in other contexts (including the UK) has often been recognised.

The ‘requirement’ for armaments - and in particular the development of a dedicated industry for their manufacture - appears, however, to have not been universally accepted (or desired) by everyone at all times in the UK. Another former US President, John F. Kennedy, suggested, for example, that in the run-up to the Second World War there was an absence of a ‘lobby for armaments’ in the UK and that ‘England’s’ lack of preparedness, and thus failure to deter Nazi aggression, can in part be explained by the Englishman’s natural psychological reluctance to rearm.<sup>11</sup> This is notwithstanding differing levels of support in the literature around the legitimacy of industry’s role in national

---

<sup>7</sup> Abou-Bakr, ‘Managing Disaster: Public-Private Partnerships’, p.138

<sup>8</sup> Alex Roland, ‘The Military-Industrial Complex: Lobby and Trope’ in Andrew J. Bacevich (Ed.) *The Long War: A New History of National Security Policy since World War II* (New York: Columbia University Press, 2007), p.335

<sup>9</sup> Vernon V. Aspaturian, ‘The Soviet Military-Industrial Complex: Does It Exist?’, in Rosen, *Testing the Theory*, pp.103-133

<sup>10</sup> Neil Latham, ‘Defence Industry in a Global Context: Policy Implications for the United Kingdom’, Royal United Service Institute, Whitehall Paper 57:1 (2003), p.8

<sup>11</sup> John F. Kennedy, *Why England Slept* (New York: Wilfred Funk Inc., 1940), pp.3-23, 223

security, as discussed in Section 2.4, and however pronounced disagreements may be over any nation's industrial capacity for conflict at any given time.<sup>12</sup>

Indeed, more generally, it has been argued that Eisenhower's 1961 speech which famously introduced the MIC concept was not necessarily designed as a critique of the emergence of an arms industry per se; on the contrary, it can be suggested that he saw the development of national industries in this sector as an important consideration. In his unusually robust defence of the MIC, Baumgartner makes this argument by presenting what he argues is a 'rarely noted passage' of the speech:

But we can no longer risk emergency improvisation of national defense. (...) We have been compelled to create a permanent armaments industry of vast proportions.<sup>13</sup>

He is not alone. Dunlap has similarly identified that Eisenhower 'appreciated the need for a powerful military buttressed by a strong and creative industrial infrastructure'<sup>14</sup> and another leading commentator has noted that the President's speech was 'arguably neutral' regarding any potential impact of the system.<sup>15</sup> Whilst he warned of its potential effects, it seems that Eisenhower understood that there was a *requirement* for an arms industry. It is arguably the same outlook that witnessed the 'defence industry' being seen in the Cold War era as an important contributor towards a country's strategic posture or, as Hayward puts it, 'an element of national sovereignty.'<sup>16</sup>

---

<sup>12</sup> Edgerton has strongly challenged the idea, for example, 'that by the early 1930s the British arms industry barely existed', arguing that 'it is important to stress the depth and complexity of the specialized arms industry' at the time. David Edgerton, *Britain's War Machine: Weapons, Resources and Experts in the Second World War* (London: Penguin Books, 2012), pp.28-29

<sup>13</sup> Passage from President Eisenhower's 'Farewell Address' cited in John Stanley Baumgartner, *The Lonely Warriors: Case for the Military-Industrial Complex* (Los Angeles: Nash Publishing, 1970), p.8 (Emphasis in original)

<sup>14</sup> Charles J. Dunlap Jr., 'The Military-Industrial Complex', *Daedalus*, Vol.140:3 (2011), p.136 (Emphasis added)

<sup>15</sup> Ledbetter, *Unwarranted Influence*, p.7

<sup>16</sup> Keith Hayward, 'The Globalisation of Defence Industries', *Survival*, Vol.43:2 (2001), p.116

If it is widely (if not universally) acknowledged, then, that an industrial base has been needed to supply capabilities to the Armed Forces at certain points in history, why did Eisenhower's address achieve such durable resonance? In short, it was arguably the strength of his warning about the potential dangers arising from the amalgamation of the different parts of the 'complex' he envisaged - rather than necessarily the effect or orientation of each of them in turn - that subsequently so stirred up the popular imagination. Famously, it was Eisenhower's identification of the risk of an emerging system of aligned interests exerting 'unwarranted influence' that was his speech's main legacy; this was the true danger that was identified in what has been identified as the first reference to the MIC.<sup>17</sup> The image of an unaccountable and 'cosy' military-industrial coalition comprising politicians, bureaucrats and industrialists able to dictate policy and/or spending has persisted ever since.

If these are the origins and popular perceptions of the 'MIC', what are its precise characteristics? In short, there are differing views; some even suggest that 'there is no clear theoretical conceptualisation of the MIC.'<sup>18</sup> Several definitions have been attempted, however; Pursell argues, for example, that '[t]he key to understanding the complex is to see it as a system.'<sup>19</sup> Seen in this way, the most effective way of understanding the MIC could be to identify the full range of actors that interact with each other. That being said, existing definitions also tend to incorporate, or allude to, the motivations of the purported system. Citing Pilisuk and Hayden, Pursell explains:

The military-industrial complex can be defined as 'an informal and changing coalition of groups with vested psychological, moral, and material interests in the continuous development and maintenance of high

---

<sup>17</sup> Dunne and Sköns, 'The Changing Military Industrial Complex', p.2; Fallows agrees this was when '[t]he phrase entered the lexicon.' James Fallows, 'The Dustbin of History: The Military-Industrial Complex', *Foreign Policy*, (November/December 2002), p.46

<sup>18</sup> Dunne and Sköns, 'The Military Industrial Complex', p.4

<sup>19</sup> Carroll W. Pursell, Jr. (Ed), *The Military-Industrial Complex* (New York: Harper and Row, 1972), p.13



levels of weaponry, in preservation of colonial markets and in military-strategic conceptions of international affairs.<sup>20</sup>

As discussed below, disagreement persists around the true motivations of any such system, and whether it could ever be beneficial to society; this type of research, whilst understandable, blunders debate on the character of the system and does not help in providing clarity that the MIC may be most usefully considered as a set of military-industrial interactions (whatever their impact).

Providing further clarity, Slater and Nardin have helpfully explained that ‘...[i]n most of the literature, the concept of a military-industrial complex functions as both a description and an explanation (or theory) of what is being described.’<sup>21</sup> This is important to understand because whilst it has often been presented as a conspiracy, the MIC concept is in fact multidimensional. It can be suggested from the outset, therefore, that ‘the MIC’ has emerged (and remains) as much a (contested) theory on the potential effects of the system of military-industrial interaction as it is a (generally negative) description of the actual system of interaction between its constituent parts.<sup>22</sup>

## **2.2 Origins of the MIC Concept**

Before examining whether it is appropriate to apply the same ‘industrial-complex’ type terminology to the CT sector, it is important to properly contextualise the origins of Eisenhower’s ‘warning’<sup>23</sup> and in particular to note the concerns that were being expressed at the time about the state of US politics, the structure of the country’s national leadership, and how these related to the military sector. Against the grain of most accounts on ‘the MIC’, Moskos, Jr. argues that discussions on the MIC should start with C.

---

<sup>20</sup> Marc Pilisuk and Thomas Hayden, ‘Is there a military-industrial complex which prevents peace?’, *Journal of Social Issues*, Vol.21:3 (1965), quoted in *Ibid*, Preface, p.ix

<sup>21</sup> Jerome Slater and Terry Nardin, ‘The Concept of a Military-Industrial Complex’ in Rosen (Ed.), *Testing the Theory of the Military-Industrial Complex*, p.28 (Emphasis added)

<sup>22</sup> This reflects Pilisuk and Hayden’s useful conceptualisation of the MIC as a ‘system’ above.

<sup>23</sup> Roland describes the effect of Eisenhower’s speech as such in Alex Roland, ‘The Military-Industrial Complex: Lobby and Trope’, p.336

Wright-Mills' major 1956 work, *The Power Elite*<sup>24</sup>; Rosen has also argued that such was the similarity in outlook that Eisenhower 'legitimized' Mills' theory.<sup>25</sup>

Even a cursory examination of Mills's 'Power Elite thesis' shows that Eisenhower was not the first person to write on, or warn about, the potential dangers of converging military-industrial interests. Indeed, it was Mills who is credited with highlighting 'the often uneasy coincidence of economic, military, and political power'<sup>26</sup> and by clarifying the risks it posed: '[W]hen political institutions and economic opportunities are at once concentrated and linked, then public office can be used for private gain.'<sup>27</sup> However, as Roland correctly argues, unlike later criticisms of the MIC it was not Mills' belief that 'this power elite operates conspiratorially to subvert the will of the people.'<sup>28</sup> Whilst famously recognizing 'that power (...) was concentrated in the hands of a few hundred government officials, corporate executives, and military officers'<sup>29</sup>, Mills' argument was that the most substantial potential danger was 'that the elites developed among themselves a shared worldview that bred consensus among them on the fundamental policies guiding American life.'<sup>30</sup> In Mills' account, therefore, it was not that the US had become victim to a sinister conspiracy - he actually argued to the contrary<sup>31</sup> - but that it was because 'never before have the means of power been so enormous (...) that makes our situation so precarious.'<sup>32</sup> Whilst for Mills both military and business leaders were now able to exert more 'power' than ever before, there was no naivety in his account that it would have to lie somewhere;

---

<sup>24</sup> Charles C Moskos, Jr., 'The Military-Industrial Complex: Theoretical Antecedents and Conceptual Contradictions' in Sam C. Sarkesian (Ed.), *The Military-Industrial Complex: A Reassessment* (London, Sage Publications, 1972), p.5

<sup>25</sup> Rosen, 'Testing the Theory', p.1

<sup>26</sup> C Wright Mills, *The Power Elite* (New York: Oxford University Press, 1956), p.278

<sup>27</sup> *Ibid.*, p.346

<sup>28</sup> Roland, 'The Military-Industrial Complex: Lobby and Trope', p.338

<sup>29</sup> *Ibid.*

<sup>30</sup> *Ibid.*

<sup>31</sup> Mills argues that 'The rise of the elite (...) was not and could not have been caused by a plot[.]'  
Mills, *The Power Elite*, p.293

<sup>32</sup> *Ibid.*, p.25

the concern lay more around the consolidated character and unprecedented level of influence handed to the new governing elite.

Mills and Eisenhower clearly shared a similar world view. Whilst several differences in their approaches have been expertly highlighted<sup>33</sup>, neither of their conceptualisations of the 'Power Elite' and 'the MIC' was conceived of as *necessarily* being a conspiracy; both were seen as *wider systems* of elite relationships comprising individuals from Government, industry and beyond. Furthermore, their joint concern was primarily over the potentially negative political or economic effects that might result from converging (especially public-private) interests - not necessarily each individual part of the system per se. Therefore, at the risk of repetition, whilst the presence of 'industry' within 'the MIC' must be viewed as a component of the potentially dangerous system, its presence should be considered as just that; one category of participant within a wider system of military-industrial interaction. This is important to understand because even notable scholars sometimes incorrectly use 'the MIC' and the 'defence industrial base' interchangeably<sup>34</sup>; this fails to identify 'industry' as just one component of the MIC. It is therefore the potential impact of the 'confluence'<sup>35</sup> of public-private interests that Eisenhower and Mills - and indeed this thesis - are concerned with.

At the risk of over-simplification, therefore, we can conceptualise Mills and Eisenhower's general understanding of the MIC as the (potentially damaging) three-cornered system of interaction within the defence arena of the political establishment, the

---

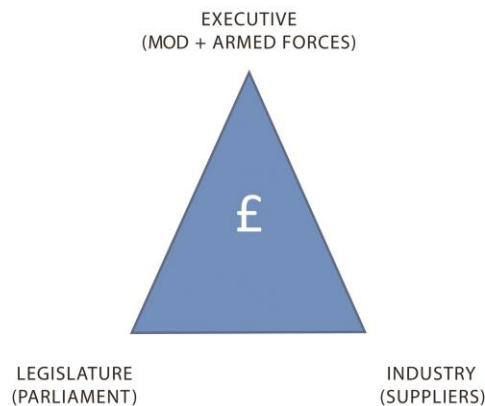
<sup>33</sup> Roland argues, for example, that 'Eisenhower's address was rooted in a very different framework'; concerned as it was primarily with 'his attempts to restrain government spending', Roland, 'The Military-Industrial Complex: Lobby and Trope', pp.339-40. Ledbetter also argues that 'Eisenhower's warning focussed on the negative side of the war economy theses[.]' Ledbetter, *Unwarranted Influence*, p.119

<sup>34</sup> For example, Dunlap laments the Defence Science Board's 2008 assessment of the changes to the military-industrial complex following Eisenhower's speech, before citing one of its quotations which refers to changes in the 'defence industrial base'. Dunlap Jr., 'The Military-Industrial Complex', p.136

<sup>35</sup> Smith and Smith, *The Economics of Militarism*, p.41

military and industry; an alliance focused on certain shared security and economic priorities. The system has been described by Adams as the 'iron triangle'<sup>36</sup> of US defence politics and can be represented in the UK context as follows:

**Figure 2: The 'Classic' MIC**



Establishing this as our core understanding of the MIC, considerations for this thesis (as introduced in Chapter 1) are whether it is appropriate to apply the same concept to the UK political system, and whether the same or similar purported 'MIC' dynamics exist in the non-military CT arena.

Whatever the precise membership of the MIC<sup>37</sup> - or any modern-day version of it - debate over whether any converging interests within such a system should ever exert any political and/or economic influence would be triggered by the most powerful man in the world; just five years after Mills' major work, the US President would declare his now oft-repeated warning. It would be impossible in the available space to sufficiently record the frequency with which this expression has subsequently been invoked by various competing

<sup>36</sup> Gordon Adams, *The Politics of Defense Contracting: The Iron Triangle* (New York: Transaction Publishers, 1981). Adams's and other author's description of this system is covered in Theo Farrell, *Weapons Without A Cause: The Politics of Weapons Acquisition in the United States* (London: MacMillan Press, 1997), p.5

<sup>37</sup> For an early discussion on the lack of agreement around 'Who Are the Members of the Complex?' see Slater and Nardin, 'The Concept of a Military-Industrial Complex', pp.40-42

parties. It is helpful for this thesis, therefore, that on the occasion of the 50<sup>th</sup> anniversary of Eisenhower's speech, in January 2011<sup>38</sup>, several important 'retrospectives' offered new analysis on the meaning, significance and long-term impact of his remarks. Amongst them, Dunlap has neatly summarised the popular image and allegedly negative impact of the MIC triggered by the speech:

When President Eisenhower uttered this warning in his farewell address, he forever fixed in the public mind the idea – in its most histrionic manifestation – of an ever-present menace posed by grasping arms merchants in league with war-mongering generals. This cabal, so the theory goes, lurks in the shadows waiting for an unguarded moment in which to subvert the American way of life for its own venal purposes.<sup>39</sup>

Ledbetter's work, *Unwarranted Influence*, has similarly argued that '[t]he case against the MIC is an indictment with multiple counts, to which any given critic may subscribe to varying degrees.'<sup>40</sup> The 'charges' are worth noting and variously suggest that the MIC<sup>41</sup>: '...creates wasteful military spending'; '...takes away from spending on social needs.'; '...distorts the American economy.'; '...has institutionalized an outsized role for the military in American society'; '...creates and extends a culture of secrecy'; and '...leads to the suppression of individual liberty.' Numerous other contemporary commentators have presented the MIC in negative light<sup>42</sup>; elsewhere, campaign groups oppose the interaction of governments and industry in the arms trade, regularly decrying the 'pain and destruction it causes'.<sup>43</sup>

As introduced in Section 1.1, similar charges have been levelled against the system of public-private cooperation in the CT sector; critics accuse the 'SIC' of incorporating similar, if not identical characteristics and flaws. Mainstream newspapers have also

---

<sup>38</sup> By coincidence, work on this thesis commenced in the same month.

<sup>39</sup> Dunlap Jr., 'The Military-Industrial Complex', p.135

<sup>40</sup> Ledbetter, *Unwarranted Influence*, p.7

<sup>41</sup> The following 'counts' are analysed by Ledbetter at Ibid., pp.7-14

<sup>42</sup> See, for example, Jonathan Turley, 'Big money behind war: the military-industrial complex'; and Kone, 'The Military-Industrial Complex in the United States'.

<sup>43</sup> Campaign Against the Arms Trade, 'Introduction to the Arms Trade', April 2011, Via: <http://www.caat.org.uk/resources/publications/intro-briefing-2011.pdf> (accessed 16.07.14), p.8

presented the character of the post-9/11 security 'market' as displaying those dynamics which have been traditionally associated with defence; the *Financial Times* and *Guardian* newspapers, for example, have both presented in linear terms how after 9/11 companies re-focused their strategies on the growing CT market.<sup>44</sup> This type of analysis presents a serious problem, however, because, whilst such accounts are seductive in their simplicity, they decline to analyse the complexity of the private sector's involvement in contemporary national security strategy. Poorly-informed journalists and busy scholars have not taken time to properly understand the new landscape, or plot out precisely how companies are now involved in areas of security such as CT. Before Section 2.4 addresses whether the 'MIC' system has always been considered in negative light, the next section establishes the validity of applying the concept to the UK experience.

### **2.3 An American expression?**

As the MIC - what Roland labels both a 'lobby' (for armaments) and a 'trope' (the expression generally used critically)<sup>45</sup> - unquestionably originated in the US, it might seem that it is a uniquely American phenomenon. But this would be to underplay the extent to which the aforementioned public-private dynamics (and their potential impact) have also been considered in a UK military context. This section provides further background to illustrate how, alongside the American experience, something called a 'British MIC'<sup>46</sup> certainly exists; it may differ from its American cousin but, as suggested above, military-industrial coordination in the UK has had a long heritage built up over many centuries.

Several distinct features of the US MIC thought of as a system can be considered when drawing comparisons with the UK example. Firstly, it is well documented that the US defence budget has for many decades (and in the period under examination) been

---

<sup>44</sup> Harris, 'How private firms have cashed in'; Sylvia Pfeifer, 'Defence groups turn focus to security at home', *Financial Times*, 4 August 2008.

<sup>45</sup> Roland, 'The Military-Industrial Complex', p.345

<sup>46</sup> As noted in footnote 103 (Chapter 1), Edgerton has used this expression.

substantially larger than that of any other nation. According to SIPRI's military expenditure database, for example, US military spending (in 2010 constant prices) rose from to \$385.14bn in 2001 to 689.51bn in 2011<sup>47</sup>; the UK's military expenditure, by contrast, grew from \$46bn in 2001 to \$57.87bn in 2011.<sup>48</sup> More broadly, *The Economist* recently highlighted the US's current superiority in the military sector; it published data which showed that at nearly \$700bn US 'defence spending (...) is bigger than that of the next 17 countries combined'<sup>49</sup>, including the UK. The US's dominant position is not a recent phenomenon; Walker has shown that as a percentage of GDP the US defence budget 'ranged from a high of 15 percent in 1952 (during the Korean War) to a low of 3.7 percent in 2000[.]'<sup>50</sup> By contrast, UK military expenditure accounted for 9% of GDP in 1953<sup>51</sup> and 2.4% during the 'relatively tranquil' period of 2000.<sup>52</sup> It is important to recognise that the MIC in the UK revolves around a considerably smaller allocation of budgetary resources for defence - both in actual terms and in comparative GDP scale.

Secondly, the 'dominance' of one part of the MIC - the US defence industry - when compared to the UK's military sector (and, for that matter, other internationally-domiciled national defence industries) has been widely acknowledged.<sup>53</sup> Whilst the UK may continue

---

<sup>47</sup> This constitutes a 79% increase in the sample period. Stockholm International Peace Research Institute, 'The SIPRI Military Expenditure Database', Military Expenditure of USA, Via:

<http://milexdata.sipri.org/result.php4> (accessed 04.02.13)

<sup>48</sup> This constitutes a 26% increase in the sample period. Stockholm International Peace Research Institute, 'The SIPRI Military Expenditure Database', Military Expenditure of UK, Via:

<http://milexdata.sipri.org/result.php4> (accessed 04.02.13)

<sup>49</sup> The Economist, 'Defence Costs', *The Economist online*, 8 Aug. 2011, Via:

<http://www.economist.com/blogs/dailychart/2011/06/military-spending> (accessed 04.02.13)

<sup>50</sup> Dinah Walker, 'Trends in U.S. Military Spending', *Council on Foreign Relations*, 23 Aug. 2012, Via: <http://www.cfr.org/geoeconomics/trends-us-military-spending/p28855> (accessed 04.02.13). It was, of course, to be not long after this 'high' when President Eisenhower would issue his MIC warning.

<sup>51</sup> 'Historic Spending By Area', *Guardian Datablog*, Via:

<http://www.guardian.co.uk/news/datablog/2010/oct/18/historic-government-spending-area#data> (accessed 04.02.13)

<sup>52</sup> Stockholm International Peace Research Institute, 'The SIPRI Military Expenditure Database', Military Expenditure of UK, Via: <http://milexdata.sipri.org/result.php4> (accessed 04.02.13)

<sup>53</sup> See, for example, Seth G. Jones, 'The Rise of Europe's Defense Industry', U.S.-Europe Analysis Series No.18, The Brookings Institution (May 2005), Via:

<http://www.brookings.edu/research/papers/2005/05/europe-jones> (accessed 04.02.13), p.3;

to act as a 'home' to at least one leading global defence company, BAE Systems<sup>54</sup>, and scholarly discussions over the 'transnationalization of the arms industry'<sup>55</sup> have raised (and continue to raise) questions over the extent to which defence industries should be considered 'national' entities<sup>56</sup>, few would dispute the emergence of what one scholar calls a 'unipolar global defense industrial sector.'<sup>57</sup> Certainly, US industrial dominance in defence can be further illustrated through analysis of data pertaining to the success<sup>58</sup> it achieves in export markets. Although concerns have been expressed over the longevity of its superiority<sup>59</sup>, the US accounted for over 40% of the total arms deliveries worldwide between 1999 and 2006.<sup>60</sup> Whilst for its size the UK has more than 'pulled its weight' in this area<sup>61</sup>, the idea that there is a 'crisis in the European defense industrial base'<sup>62</sup> - of which the UK sector is part<sup>63</sup> - has gained considerable resonance. In short, American industrial dominance is generally still seen to remain 'unassailable'<sup>64</sup> in this sector.

---

Stephanie G. Neuman, 'Power, Influence, and Hierarchy: Defense Industries in a Unipolar World', *Defence and Peace Economics*, Vol.21:1 (2010), p.112; and Feuchtwanger, *The Best Kit*, p.11

<sup>54</sup> The UK-owned BAE Systems has previously been labelled the only European global 'mega prime'. Hayward, 'The Globalisation of Defence Industries', p.118

<sup>55</sup> Bryan Mabee, *The Globalisation of Security: State Power, Security Provision and Legitimacy* (Basingstoke: Palgrave, 2009), pp.90-98.

<sup>56</sup> See especially Hayward, 'The Globalisation of Defence Industries' and Trevor Taylor, 'Defence industries in international relations', *Review of International Studies*, Vol.16:1 (1990), pp.59-73.

<sup>57</sup> Neuman, 'Power, Influence, and Hierarchy', p.112

<sup>58</sup> 'Success' here is considered here in the way Governments measure it (i.e. income by sales). For an account presenting arguments on the damaging elements of the arms exports, see Andrew Feinstein, *The Shadow World: Inside The Global Arms Trade* (London: Penguin Books, 2011)

<sup>59</sup> Jonathan Caverley and Ethan B. Kapstein, 'Arms Away: How Washington Squandered Its Monopoly on Weapons Sales', *Foreign Affairs* (September-October 2012), Via: <http://www.foreignaffairs.com/articles/138035/jonathan-caverley-and-ethan-b-kapstein/arms-away> (accessed 20.02.13)

<sup>60</sup> Neuman, 'Power, Influence, and Hierarchy', p.112

<sup>61</sup> ADS published Government figures in 2012 which claimed that the 'UK gained over 15 per cent of the world defence market, ahead of Russia and France' in 2011. ADS Group, 'UKTI DSO: UK Defence and Security Exports 2011 – UK Maintains Position as Second Most Successful Defence Exporter', ADS News (01.05.12), Via: <http://www.adsgroup.org.uk/articles/29509> (accessed 05.02.13)

<sup>62</sup> Robert Dover, 'Britain, Europe and Defense in the Post-Industrial Age', *Defence & Security Analysis*, Vol.27:1 (2011), p.23-25

<sup>63</sup> This thesis considers the UK-based defence industry to part of the European DIB because that is where it is geographically located.

<sup>64</sup> Feuchtwanger, *The Best Kit*, p.11



Despite these differences, important similarities exist in so far as public-private interaction on military issues in the UK and the US can be contextualised, characterised and understood. Firstly, the US and UK Governments have shared a broadly similar view of the principal risks facing their respective countries' national security during the past decade. Even a swift review of the UK Government's strategic security documentation illustrates how, like the US, it views international terrorism as a principal threat to its national security.<sup>65</sup> However differently the UK Government may have chosen to work with industry in response to these threats, its assessment of the security landscape (and therefore the context within which any MIC dynamics operated) closely reflected the US world view.

Secondly, like the US military, the British Armed Forces became deeply engaged in military conflict against AQ after 9/11; it similarly remained on a permanent 'war footing' across many geographical locations during the 2000s.<sup>66</sup> Of relevance to this thesis, this sustained and extensive use of the military has inevitably resulted in additional demand for new capabilities from industry. Whilst differences have existed in the character of the 'industrial strategy' being pursued during the period - in contrast to the Labour Party under Tony Blair and Gordon Brown, the coalition Government formed in May 2010 stated its preference to procure military equipment 'off the shelf' rather than develop a 'defence industrial strategy'<sup>67</sup> - additional capability purchased by the MoD through 'urgent operational requirements' for Iraq and Afghanistan amounted to £3.6 billion since the

---

<sup>65</sup> See footnote 58 (Chapter 1)

<sup>66</sup> For an account on the UK's prolific military involvement in overseas conflicts after 9/11, see John Kampfner, *Blair's Wars* (London: Simon & Schuster Ltd, 2004)

<sup>67</sup> One Parliamentary inquiry concluded that the 'absence of a defence industrial strategy' under the coalition Government 'puts the UK at a disadvantage against competitor countries.' Defence Select Committee, 'Defence Acquisition', Seventh Report of Session 2012–13, 5 Feb. 2013, Via: <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/9/9.pdf> (accessed 08.02.13), p.20

beginning of those operations.<sup>68</sup> Since 9/11, therefore, the UK Government has, like the US, clearly used its Armed Forces as a significant component of the response to international terrorism. Accordingly, it has been highly active in the acquisition of additional military capabilities from industry, even if the size of its programme has been dwarfed by US capabilities.

Thirdly, even during 'peacetime' the UK MoD has, like its American equivalent, long been 'a major buyer of defence equipment and services[.]'<sup>69</sup> Whilst the size of the UK defence equipment budget pales in comparison to the US, its equipment programme is hardly insignificant - and certainly not for the contractors which provide it with capability. For example, it was noted in 2009 that defence equipment acquisition accounted for '[a]round 40% of the MoD's total annual cash spend on defence, c. £12bn p.a.'<sup>70</sup> Despite the weak state of the UK economy and the associated 7.5% cuts being made to the UK defence budget at the time of writing, the MoD announced in 2012 its intention to grow its equipment plan each year to total £159bn between 2012-2020.<sup>71</sup> Furthermore, the requirement (as most parties see it) for the Government to routinely work with suppliers in the development and acquisition of new military capability has been articulated consistently by senior Government officials. The current Chief of Defence Materiel, Bernard Gray, for example, once stated in a report on defence acquisition that 'the MoD does have a symbiotic relationship with the defence industry.'<sup>72</sup> This mirrors the American

---

<sup>68</sup> Ministry of Defence, 'Standing Commitments', Gov.uk, 12 Dec. 2012, Via: <https://www.gov.uk/standing-commitments> (accessed 05.02.13)

<sup>69</sup> Keith Hartley, 'The Economics of the UK Defence Industrial Strategy', *Security Challenges*, Vol.3:2 (2007), Via: <http://www.securitychallenges.org.au/ArticlePDFs/vol3no2Hartley.pdf> (accessed 04.02.13), p.19

<sup>70</sup> Bernard Gray, 'Review of Acquisition for the Secretary of State for Defence - An independent report by Bernard Gray', October 2009, Via: <http://www.bipsolutions.com/docstore/ReviewAcquisitionGrayreport.pdf> (accessed 05.02.13), p.54

<sup>71</sup> Ministry of Defence, 'The Defence Equipment Plan 2012', [www.gov.uk](http://www.gov.uk), 31 Jan. 2013, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/70258/Defence\\_Equipment\\_Plan\\_2012\\_20130130.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/70258/Defence_Equipment_Plan_2012_20130130.pdf) (accessed 05.02.13), p.5

<sup>72</sup> Gray, 'Review of Acquisition', pp.51-52

experience where the national DIB is routinely considered as an essential component of US military power.

Fourth, from an academic perspective it is evident that it is not only the American MIC system that has received independent scrutiny; although on a lesser scale, what has been referred to as the 'British MIC' has also attracted dedicated literature.<sup>73</sup> An introduction to the tone, character and content of this literature is provided below; suffice to say for this section's purposes that the British MIC as defined in this thesis has, like in the US, been treated as a distinct topic worthy of scholarly consideration; even if this has mainly focused on defence procurement.<sup>74</sup>

Finally, it is worth noting not only the similarities but also the *direct overlap* that exists between what might be considered as two separate American and British 'MICs'. The increased integration of the global defence sector generally and the industrial supply chain in particular, as noted below, has meant that US-owned defence companies now operate widely in the UK. If the existence of a powerful American MIC is no longer disputed, and the industrial parts of that system also supply capability to the UK Government, what can be said about the impact of that system on the UK? Could it be said, for example, as Rosen has argued, that '[t]he result is a trend to the multinationalization of the military industrial-complex'<sup>75</sup>? Consideration of such dynamics is crucial to take into account when studying the British MIC, or any variety of it.

---

<sup>73</sup> See especially Edgerton, 'The British military-industrial Complex' and Dunne and Sköns, 'The Changing Military Industrial Complex'.

<sup>74</sup> See, for example, Matthew Uttley, 'Defence Procurement and Industrial Policies' in Stuart Croft, Andrew Dorman, Wyn Rees and Matthew Uttley, *Britain and Defence 1945-2000: A Policy Re-evaluation* (Harlow: Pearson Education Limited, 2001); Jonathan Aitken MP, 'Defence Procurement: Past, Present and Future', *RUSI Journal*, Vol.139:1 (1994); Bill Kincaid *Changing the Dinosaur's Spots: The Battle to Reform Defence Acquisition* (London: RUSI, 2008); Keith Hartley, 'Defence Procurement in the UK', *Defence and Peace Economics*, Vol.9:1 (1998).

<sup>75</sup> Rosen, 'Testing the Theory', p.25

Despite some differences in the context and character of the American and British MICs, this thesis argues that the similarities and overlap that exist between them justify the use of the same terminology. Naturally, this is not to say that the US and UK 'MICs' are identical, or indeed that they are able to exert equal influence on policy. In the final analysis, however, both countries clearly possess a network of public-private interaction that has been established to support, and which potentially impacts upon developments in, the military sector. As the next section shows, prevailing attitudes towards any MIC thought of as a system have been varied, but are frequently negative.

#### **2.4 A 'pejorative' term? Contrasting attitudes on the MIC**

How could it ever be beneficial that '[t]he military-industrial complex rationalizes high levels of military spending with an ideology of international conflict'<sup>76</sup>? Such concerns have been expressed regularly in analytical treatments on the MIC; as noted above, Ledbetter refers to its frequent use in the 'pejorative'.<sup>77</sup> Indeed, it can be noted that some *fundamental objections* have even been raised against the existence and/or development of any system of military-industrial interaction. One critic has argued, for example, that the MIC is 'circumstantially unethical'<sup>78</sup>; another has castigated the PMSC sector, expressing deep concern around the use of such companies in the security field.<sup>79</sup>

The impact of the MIC is a particularly worrisome state of affairs, it has been argued, because, as Rosen has summarised; 'high levels of expenditure have given rise to powerful domestic groups within the major states who have vested interests in the

---

<sup>76</sup> Rosen, 'Testing the Theory', p.3

<sup>77</sup> Ledbetter, *Unwarranted Influence*, p.7

<sup>78</sup> Byrne, 'Circumstantially Unethical', pp.153-165

<sup>79</sup> See, for example, Anna Leander, 'The Market for Force and Public Security: The Destabilizing Consequences of Private Military Companies', *Journal of Peace Research*, Vol.42:5 (2005), pp.605-622.

continuance of military spending and international conflict.<sup>80</sup> Gottlieb elaborates on the supposedly self-interested dynamics:

The defense-industry culture, the fear of further job loss, the competition among the military services for the slice of the budget pie, and the eagerness of members of Congress to hold onto military contracts and facilities for their constituents - together these create a defense addiction.<sup>81</sup>

It should be stressed that the political-economic aspects of this 'culture' are not limited to the US experience: the controversy which followed the downsizing of a UK military shipyard in November 2013 (resulting in the loss of over 1,000 jobs<sup>82</sup>), for example, is a recent instance of these dynamics existing in the UK. Related to these employment dynamics, the allegedly inappropriate impact of Government officials joining the defence-related industries upon retirement<sup>83</sup> - the so-called 'revolving door'<sup>84</sup> - is another avenue of MIC criticism.<sup>85</sup>

The tendency of the MIC system (or its individual elements) to inflate or 'overblow'<sup>86</sup> security threats - or, more recently, exert a 'vested interest in maintaining and extending the military and security aspects of the 'war on terror''<sup>87</sup> - has also been criticised. Whilst such reservations have been most frequently expressed about (and within) the US context, similar worries have emerged about how threats are articulated in

---

<sup>80</sup> Rosen, 'Testing the Theory', p.2

<sup>81</sup> Sanford Gottlieb, *Defense Addiction: Can America Kick the Habit?* (Oxford: Westview Press, 1997), p.9

<sup>82</sup> 'BAE Systems cuts 1,775 jobs at English and Scottish shipyards', *BBC News*, 6 Nov. 2013, Via: <http://www.bbc.com/news/uk-scotland-glasgow-west-24831779> (accessed 17.07.14)

<sup>83</sup> Janine R. Wedel and Linda Keenan, 'Shadow Elite: Eisenhower's Dark Vision Realized – The Military-Industrial Complex at 50', *The Huffington Post*, 13 Jan. 2011, Via: [http://www.huffingtonpost.com/janine-r-wedel/emshadow-eliteem-eisenhow\\_b\\_808410.html](http://www.huffingtonpost.com/janine-r-wedel/emshadow-eliteem-eisenhow_b_808410.html) (accessed 02.06.11)

<sup>84</sup> Fallows summarises this practice: 'Most career soldiers leave the service by their mid-40s. A tiny handful last until their mid-50s, and nearly all the retirees look for a second career. Far and away the most lucrative opportunities are with defense industries.' Fallows, 'The Dustbin of History', p.48

<sup>85</sup> Wedel and Keenan argue that this phenomenon - analysed in a contemporary UK security context in Chapter 7 - results in 'twisted arrangements and resulting lapses in accountability are rife[.]' Wedel and Keenan 'Shadow Elite: Eisenhower's Dark Vision Realized'

<sup>86</sup> Mueller makes this argument in his analysis of the 'terrorism industry's' reaction to the 9/11 terrorist attacks. Mueller, *Overblown*, especially pp.29-48

<sup>87</sup> Hughes, *War On Terror, Inc.*, p.7

the UK.<sup>88</sup> Against this backdrop, it has been noted that some have ‘found the complex even more sinister and dangerous than the simple lobby that Eisenhower had experienced.’<sup>89</sup> By contrast, it can be observed that only a limited number of accounts explicitly conceptualise the MIC as representing a *necessary* system of military-industrial cooperation. Baumgartner is the most widely-cited early supporter of the MIC, arguing that its ‘defense, if it needs one, is its record: it performs.’<sup>90</sup> More recently, Dunlap Jr. has also criticised accusations levelled against the MIC, arguing that ‘a robust “military-industrial complex” remains an essential element of a democracy facing diverse and existential threats in a dangerous world’<sup>91</sup>.

Perhaps owing to the comparative scale of the US system, the British MIC has attracted a smaller volume of scholarly scrutiny. However, like in the US, there has also been criticism in the UK context of efforts to foster the economic aspects of military or security-industrial cooperation, or of the trend towards greater levels of privatisation within UK national security strategy. For example, Feuchtwanger argues that the assumption ‘that there is a substantial and indefinitely sustainable defence industry in this country [the UK] that requires preferential treatment, if not protection, is out of date’<sup>92</sup>, arguing forcefully that the UK’s approach to defence industrial policy ‘should be rewritten to place less emphasis on creating and maintaining manufacturing jobs in the UK.’<sup>93</sup> As introduced in Section 1.1., Hughes is even more damning in his criticism of the interests which he considers profit from insecurity in a contemporary CT context.<sup>94</sup> Such criticism extends beyond the literary community and into the political sphere; the failure of G4S to

---

<sup>88</sup> See, for example, Jenkins, ‘If the MoD can’t name the enemy’; Peter Osborne, ‘The Use and Abuse of Terror: The Construction of a False Narrative on the Domestic Terror Threat’ in George Kassimeris (Ed.), *Playing Politics with Terrorism: A User’s Guide* (Chichester: Columbia University Press, 2008), pp.101-138; and Palombi, ‘Foreign Fighters’.

<sup>89</sup> Roland, ‘The Military-Industrial Complex’, p.346

<sup>90</sup> Baumgartner, *The Lonely Warriors*, p.13

<sup>91</sup> Dunlap Jr., ‘The Military-Industrial Complex’, p.137

<sup>92</sup> Feuchtwanger, *The Best Kit*, pp.15-16

<sup>93</sup> *Ibid.*, p.25

<sup>94</sup> Hughes, *War On Terror, Inc.*, especially pp.7-8

provide sufficient numbers of private security officers to protect the London 2012 Olympic Games - the circumstances around which are analysed in Chapter 5 - rekindled the debate, for example, over the extent to which private companies should ever be handed responsibility to fulfil important security tasks.<sup>95</sup>

It can also be noted, however, that some literature pertaining to the British MIC makes the implicit assumption that military-industrial interaction is a *necessary* element of security strategy; as noted above, an important body of literature addresses UK defence procurement, for example, the great majority of which leaves unchallenged (or assumes) the need for public-private interaction. Furthermore, some accounts actually promote the need for a system of enhanced public-private cooperation in UK defence issues. A report analysing the characteristics of what is described as the 'defence-industrial ecosystem'<sup>96</sup> is a good example; it 'conceptualises the spaces where the policy-maker, military operator, industrialist, employee, taxpayer, citizen, commentator and other stakeholders interact'<sup>97</sup> and makes the case for continued Government-industry collaboration. The next section details the main avenues of investigation into the British MIC.

## 2.5 Coverage of the British MIC

This thesis argues that whilst some of the public-private dynamics associated with the MIC have 'transferred' into the UK's CT sector, there are important differences in terms of how the 'new' system operates and should be conceptualised. Before proving this proposition, and analysing its consequences, it is important to address whether something called the

---

<sup>95</sup> For example, at the peak of the G4S Olympic security 'fiasco' the Leader of the Labour Party in the UK questioned the extent to which policing functions should be outsourced. Alexandra Topping, 'G4S Olympic scandal: Ed Miliband calls for rethink of police outsourcing', *The Guardian*. 19 July 2013, Via: <http://www.guardian.co.uk/politics/2012/jul/19/g4s-olympic-ed-miliband-police> (accessed 10.02.13)

<sup>96</sup> Heidenkamp et. al., *The Defence Industrial Ecosystem*

<sup>97</sup> *Ibid.* p.12

'British MIC' has ever existed; the use of 'industrial-complex' terminology in depictions of the 'SIC' has, after all, been drawn from it directly.<sup>98</sup>

It is argued here that a British MIC - viewed here as a system of public-private interaction on military issues - has very clearly existed historically in the UK defence sector and, considering the on-going public-private dynamics around the MoD's sizable equipment programme, continues to do so today. For the avoidance of doubt, this analysis on the character of the 'industrial-complex' in the UK CT sector does not suggest that the British MIC has disappeared or has necessarily been superseded - the MoD still clearly interacts with industry - rather it makes the case that the private-public dynamics which now exist in such non-military security sectors as CT need to be considered in their own right, and that they differ quite considerably. The distinct characteristics of the MIC, and how have they been treated in scholarly debates, are examined below; this establishes a baseline understanding from which existing characterisations of 'the SIC' can be examined.

Literary coverage of British military-industrial interaction (and the MIC more generally) echoes many US treatments - and in one case is compared to them directly.<sup>99</sup> However, it is fair to say that far fewer treatments exist of the British MIC as a distinctly national phenomenon.<sup>100</sup> As introduced above, the British system has also attracted much less *theoretical* scrutiny; writing on UK arrangements, Edgerton explains that 'Political science, strategic studies, and the like have been surprisingly silent on the subject, as have historians, including military historians.'<sup>101</sup> Indeed, there was a 'Post-war silence'<sup>102</sup> in

---

<sup>98</sup> This is notwithstanding the difficulties - identified by Levine and noted in Chapter 1 - associated with measuring the *existence* of any such system.

<sup>99</sup> Keith Hayward, "'I have seen the future and it works": The US Defence Industry Transformation - Lessons for the UK Defence Industrial Base', *Defence and Peace Economics*, Vol. 16:2 (2005), pp.127-141

<sup>100</sup> Exceptions include the treatment of the British MIC in Edgerton, 'The British military-industrial complex in history', and in Dunne and Sköns, 'The Changing Military Industrial Complex'.

<sup>101</sup> Edgerton, 'The British military-industrial complex in history', p.5

<sup>102</sup> *Ibid.* p.7



scrutiny of the British MIC and analysis of the arms industry was ‘never particularly strong’ before its revival in the 1970s.<sup>103</sup>

That being said, considerable scholarly attention has been afforded to the character of the interface between the UK Government and industry on military issues in three main areas. Firstly, the political-economy of warfare has been a major focus; Edgerton considers this ‘[p]robably the most important tradition of enquiry into the British military-industrial complex[.]’<sup>104</sup> This ‘political economic approach’<sup>105</sup> is less preoccupied with the implications of the MIC’s influence on strategic policy, therefore, and more an examination into the (often negative<sup>106</sup>) economic impact of defence expenditure. The emphasis of this angle of inquiry is, in Dunne’s words, ‘to evaluate the effects of the changes in military expenditure on the economy’<sup>107</sup>, rather than necessarily to examine or measure any significant impact of the MIC on policy. Through its examination of three major CT-related public sector security contracts, and other wider areas of concern, this examines any economic impact of such public-private dynamics in the contemporary UK CT context.

The management of defence procurement is a second major field of inquiry on the British MIC; it could even be argued that public-private interaction on defence procurement, rather than the MIC per se, is most frequently the lens through which UK military-industrial issues have been examined. Defence procurement literature (and,

---

<sup>103</sup> Ibid. Fallows also argues that the MIC has been considered in different ways throughout history, arguing; ‘[w]hen people warned about the influence of the military-industrial complex in the 1960s, they usually were talking about an increased risk of actually going to war’ before explaining that ‘During the Vietnam era, the military-industrial complex was a shorthand reference to the interests that presumably kept profiting from the war.’ Fallows, ‘The Dustbin of History’, p.46

<sup>104</sup> Edgerton, ‘The British military-industrial complex in history’, p.5

<sup>105</sup> Ibid. p.8

<sup>106</sup> Edgerton observes that ‘...this literature has at its core the observation that Britain spent considerably more on defense as a proportion of GDP than did most of continental European countries and the argument that this defense expenditure negatively affected the economy.’ Ibid.

p.7

<sup>107</sup> Dunne, ‘The Changing Military Industrial Complex in the UK’, p.92

indeed, wider policy discussions on this subject) generally focuses on how the MoD and industry interact, rather than on whether or not (or the extent to which) they should. A seemingly dry management issue invites fiercely contested debate which draws contributions from industry, academia, non-governmental organisations and even Government officials.<sup>108</sup> Through its analysis of CT-related procurements, and non-military security acquisition more generally, this study contributes to this literature in the wider security field.

A third area of literature relating to the British MIC is on the matter of 'arms exports'. Here, the political significance of international military sales is addressed even in primarily economic-focused literature.<sup>109</sup> In this area, the idea of a close (and potentially damaging) character of the military-industrial system is even more widely accepted; Smith and Smith argue, for example, that '[e]xporters and importers alike are locked into a system which each feeds off the other'<sup>110</sup> leading to 'a ceaseless search for new markets.'<sup>111</sup> Chalmers et. al. have identified the 'considerable ethical and political controversy'<sup>112</sup> around defence exports, with Smith summarising that '...the arms trade does have an unsavoury reputation[.]'<sup>113</sup> Within this body of literature, several accounts seek to explain *why* Governments support defence industries around this priority. Smith suggests, for example, that exporting countries like the UK 'use arms exports to maintain their DIB in the face of fluctuating demand'<sup>114</sup>; Martin agrees that 'exports can help

---

<sup>108</sup> See, for example, a former senior MoD civil servant's forceful article on how the department would implement its approach to defence acquisition. Bill Jeffrey 'Implementing the Defence Industrial Strategy', *RUSI Defence Systems*, Vol. 9:1 (2006), Via: [http://www.rusi.org/downloads/assets/020-025\\_The\\_Debate1.pdf](http://www.rusi.org/downloads/assets/020-025_The_Debate1.pdf) (accessed 01.06.11)

<sup>109</sup> See, for example, Chalmers et al. 'The Economic Costs and Benefits of UK Exports'

<sup>110</sup> Smith and Smith, *The Economics of Militarism*, p.79

<sup>111</sup> Ibid.

<sup>112</sup> Chalmers et al, 'The Economic Costs and Benefits of UK Exports', p.343

<sup>113</sup> Ron Smith, *Military Economics: The Interaction of Money and Power* (Basingstoke: Palgrave Macmillan, 2009), p.138

<sup>114</sup> Ibid. p.146

maintain a strong indigenous industrial base.<sup>115</sup> Furthermore, Chalmers highlights the ‘constant pressure on Government’<sup>116</sup> to maintain such a policy for industrial reasons, criticizing the endeavour as inefficient and as contributory to the ‘rapid militarization of the Third World.’<sup>117</sup> A related debate examines the potential impacts of terminating a country’s pursuit of defence exports.<sup>118</sup> Chapter 7 examines the extent to which these dynamics now appear in the CT field.

Within all this literature, the character of the British MIC is only rarely explored at the theoretical level; the system of interaction is rarely analysed as a concept and questions over its membership and potential impact have not stimulated much scholarly debate. Indeed, ‘national’ economic and industrial considerations have often been seen as playing a fundamentally legitimate (if not ineffective) role in major procurement decisions<sup>119</sup>, and any influence exerted by the MIC is rarely considered significant; perhaps the comparable size of the British defence budget and associated industry has limited any feelings that the British MIC poses any actual danger.

## **2.6 Changing character of the British MIC**

Whilst few conceptual accounts on the British MIC exist, there has been a growing appreciation that significant changes have recently been underway within the UK defence policy context, and Britain’s associated DIB. Firstly, the evolving character of the types of ‘industrial’ capabilities that have increasingly been provided to (or in support of) the British military has been clearly recognised. Indeed, it is widely acknowledged that the MoD is no

---

<sup>115</sup> Martin, ‘The subsidy savings’, p.22

<sup>116</sup> Malcolm Chalmers, *Paying for Defence: Military Spending and British Decline* (London: Pluto Press, 1985), p.124

<sup>117</sup> Ibid.

<sup>118</sup> A lively debate exists around the potential value of reducing defence exports, with Chalmers et. al. arguing, for example, that ‘the economic costs of reducing defence exports are relatively small and largely one-off.’ Chalmers et. al., ‘The Economic Costs’, p.366. Smith identifies the ‘dispute about the costs and benefits of arms exports to the economy.’ Smith, *Military Economics*, p.146

<sup>119</sup> Exceptions exist, including Lewis Page, *Lions, Donkeys and Dinosaurs: Waste and Blundering in the Military* (London: Random House, 2006); and Feuchtwanger, *The Best Kit*.

longer solely acquiring military equipment and hi-tech industrial capability for the Armed Forces; the provision of services by the private sector in overseas conflict has become an increasingly 'ubiquitous'<sup>120</sup> feature of British military capability. Indeed, Heidenkamp has recently concluded that 'contractor support to operations (CSO) has become an essential component of the ability to both deploy and sustain the UK's military instrument'<sup>121</sup> and that this area of capability 'accounted for at least 60 per cent of the UK's overseas operational defence sustainment effort in 2010.'<sup>122</sup> Whilst the use of contractors in support of military operations has had a long heritage, numerous scholars have documented the UK Government's increasing use of PMSCs in recent decades.<sup>123</sup>

Secondly, international trends have had a significant effect on the character of the UK's DIB. As Mabee records in his comprehensive account of the effect of globalization on the arms industry, there was during the 1980s and 1990s 'a trend in the arms industry to embrace a globalized model of industrial production'<sup>124</sup> whereby major programmes would be developed across national boundaries. In short, this combined with related developments including 'increased civilianization'<sup>125</sup> and the arms industry 'becoming increasingly led by firms'<sup>126</sup> resulted in 'the development of an increasingly globalized and transnationalized arms industry'<sup>127</sup>. Other authors have noted the considerable effects that globalisation has had on the UK defence sector; Taylor has also identified that 'defence industries, traditionally organized on a national basis, are in various ways becoming more internationally-structured.'<sup>128</sup> Furthermore, Markusen has charted in *Foreign Policy* the

---

<sup>120</sup> Abrahamsen and Williams, *Security Beyond the State*, p.30

<sup>121</sup> Heidenkamp, 'Sustaining the UK's Defence Effort', p.1

<sup>122</sup> *Ibid.*, p.2

<sup>123</sup> Important accounts include Kinsey, *Private Contractors*; Krahmman, *States, Citizens*; and Deborah Avant, *The Market for Force: The Consequences of Privatizing Security* (Cambridge: Cambridge University Press, 2005).

<sup>124</sup> Mabee, *The Globalization of Security*, p.88

<sup>125</sup> *Ibid.*, p.93

<sup>126</sup> *Ibid.*

<sup>127</sup> *Ibid.*, p.94

<sup>128</sup> Taylor, 'Defence industries in international relations', p.59 (Emphasis in original)

fact that 'Arms manufacturers are following the lead of their commercial counterparts and going global'<sup>129</sup>, advancing the need for regulation over what she labels a 'transnational defense-industrial base'<sup>130</sup>. Hayward similarly noted the emergence of global supply chains in defence and that '[i]t is increasingly difficult to identify the precise national origins of components.'<sup>131</sup>

It is now widely accepted, therefore, that the UK's defence industrial sector has adopted an increasingly integrated, transnational character. In this context, questions have been raised around the extent to which this supply chain can be legitimately referred to as a 'British industry' as traditionally understood<sup>132</sup>; indeed, developments seem to suggest that it may be more appropriate to refer to the MIC as being 'located in the UK', rather than seeing them as 'British' per se. Whatever its precise character, the reality that the British MIC (and the defence industry within it) has undergone significant changes in recent decades has significant implications for how public-private cooperation should be properly understood in a contemporary setting.

## **2.7 Towards a theory on the 'industrial-complex' in the CT sector, and beyond**

This thesis will argue that in the context of the changes that have occurred in the strategic security environment after 9/11 a system of public-private cooperation that looks different to the 'MIC' has emerged in the domestic UK CT sector, if not potentially also in other non-military fields of national security strategy. As well as resetting the direction, priorities and spending associated with national security strategy, the UK Government's appreciation of a wider risk environment has also resulted in a re-orientation of the way in which the State now interacts with 'industry' on security issues. Previously, the principal method of 'industrial engagement' was thought of as the military sector interacting with the DIB

---

<sup>129</sup> Ann Markusen, 'The Rise of World Weapons', *Foreign Policy*, No.114 (Spring 1999), p.40

<sup>130</sup> *Ibid.*, pp.48-49

<sup>131</sup> Keith Hayward, 'The Globalisation of Defence Industries', pp.126-7

<sup>132</sup> Dover, 'Britain, Europe and Defense in the Post-Industrial Age'

around the development of capability along the lines discussed above; in other words, the system labelled the MIC. This naturally remains an important aspect of UK security policy but, as indicated in Section 1.3, 'private sector engagement' extends beyond the military sector and includes a much broader spectrum of corporate actors.<sup>133</sup> In short, as Governments have become increasingly aware of the wider strategic landscape and the need to develop capabilities in different areas of 'national security', so they have fostered new relationships with different corporate entities.

Only a limited number of scholars have explored, as the author and others have done recently, the idea that the private sector now plays a 'multiplicity' of roles in the provision of UK national security.<sup>134</sup> Against this backdrop, a better understanding is needed of what is meant by the 'private security industry' and of the different types of roles played by a 'variety of private actors'<sup>135</sup> in UK national security strategy. Whilst useful taxonomies of the private military services sector have been formulated since 9/11<sup>136</sup>, the scope of 'the security industry' in a modern day UK domestic context has hitherto received little attention in the literature. In fairness, the difficulty of defining what constitutes the 'security industry' has been acknowledged<sup>137</sup> and at least two authors have sought to address this issue by suggesting new research agendas for further study on this issue.<sup>138</sup> A failure to do so to date may have arisen as a result of a lack of awareness around (and/or interest in) the full scope of companies' involvement in this sector, but the larger problem may be that scrutiny of the private sector's involvement in national security has continued to focus on defence matters. The ever-growing complexity of the landscape means that

---

<sup>133</sup> Rosemont, 'Private security engagement'

<sup>134</sup> See, for example, Neville-Jones and Fisher, 'Homeland Security and the Role of Business', p.170; Rosemont, 'Private sector engagement'; and Rosemont, 'Getting Down to Business', p.81

<sup>135</sup> Krahnemann, 'Conceptualizing Security Governance', p.11

<sup>136</sup> See especially Singer, *Corporate Warriors*, pp.88-100 and Avant, *The Market for Force*, pp.16-22

<sup>137</sup> Rosemont, 'Private sector engagement'

<sup>138</sup> See especially Adam White, 'The new political economy of private security', *Theoretical Criminology*, Vol.16:1 (2011) and Sempere, 'The European Security Industry'.

greater clarity is much needed on the character of the private sector's involvement in the non-military aspects of security such as CT.

At the risk of repetition, this thesis proposes that an 'industrial-complex' of a different character to the MIC now exists in the CT aspects of UK national security strategy, and potentially beyond, and that this has important implications for policymakers and the research community. This system has some similarities with, but substantially differs in character from, what has been described above as the MIC; in short, the system of public-private interaction on defence issues whose effects have almost invariably been presented in negative terms. The analysis shows with specific reference to the CT sector that as security risks have evolved and 'broadened' away from military issues after 9/11, the Government has developed new security strategies (such as CONTEST) within which an extensive network of relationships has been formed with private sector actors, both within and outside the traditional defence sector. As mentioned above, and previously (very briefly) suggested by Dunne and Sköns, the 'British MIC' has evolved in the sense that some of its dynamics operate beyond the defence sector and around other contemporary, non-military security issues.<sup>139</sup> The problem is that, prior to this thesis, bold assertions had been made around the character of 'the SIC', but no one had actually examined the detail of the proposed changes now underway.

It is against this backdrop that the dissertation examines at the micro level the origins, characteristics and consequences of various examples of public-private interaction in CONTEST; it examines three individual CT-related contracts and other public-private interactions which have caused concern after 9/11. Having done so, it proposes that, whilst some existing MIC theory still has utility in analysing trends and characteristics in and beyond the defence sector, it is not appropriate to simply conclude that its dynamics have

---

<sup>139</sup> Dunne and Sköns, 'The Changing Military Industrial Complex'

linearly transferred to the non-military security field. In short, on the basis of the evidence in the CT sector, the character of the private sector's involvement in the non-military security field is considerably more complex; the apparent suggestion of critics that the negative dynamics associated with the MIC having merely transferred in to the contemporary UK CT arena is overly simplistic.

### *Core argument*

Ultimately, the thesis will argue that any fleeting application of 'industrial-complex'-type terminology to the non-military arena of national security is likely to be an incomplete reading of the situation. Such applications have complicated matters because they invite the reader to (incorrectly) think that the dynamics of the non-military sector - the so-called 'SIC' - are exactly the same as the MIC; this thesis's examination of the CT sector dispels this idea. Such terminology should therefore be used cautiously and, it is recommended, applied initially only on a sector-by-sector basis, having considered and analysed the data and evidence.

As introduced in Chapter 1, the matter of theorising on the existence of the MIC - or, in this case, a structure of public-private coordination within the non-military CT aspects of contemporary security strategy - is troublesome in the sense that such an idea is not itself a hypothesis or statement which possesses a distinct and measurable output variable.<sup>140</sup> It is for this reason that micro-level analysis will be completed which can analyse the character of the private sector's involvement in the non-military aspects of security. Supporting the justifications for the research presented in Section 1.2, this author believes that whilst the main message of Eisenhower's Farewell Address has been misinterpreted by some authors, his warning about the potential dangers posed by the emerging interests within what he then-called the MIC remain as true and important today

---

<sup>140</sup> See footnote 109 (Chapter 1)



as ever. It is vital, therefore, to systematically examine whether a new 'industrial-complex' has emerged in the contemporary security arena, and consider whether any such system threatens to breach his principle that it should not exert 'unwarranted influence'.

Even if only some of the dynamics which have traditionally been associated with the MIC are found to have established themselves within the non-military security context, as this thesis asserts, it is vital that they are properly assessed and that an alert citizenry is in a position to understand and assess the consequences of such a system. In presenting the characteristics of a network of public-private cooperation in the CT sector, and analysing its impact, it can be hoped that policy-makers, scholars and the public more generally can be encouraged to engage in more informed discussions. An important debate could then follow on whether any 'industrial-complex' is operating more broadly than in CT, and, even more controversially, if any such system may in fact be necessary.

## Chapter 3: Emergency Preparedness

### Introduction

Examples abound of the bravery of emergency service personnel, and of the general public, during, or in the immediate aftermath of, recent major terrorist atrocities. The celebrated image of US fire-fighters raising the Star-Spangled Banner upon the ruins of the World Trade Center after 9/11, for example, or of the young British man who was photographed carefully escorting the injured 'woman in the mask' away from a temporary emergency centre directly following 7/7<sup>1</sup>, are particularly powerful examples. The security authorities would naturally aim to prevent such events from ever occurring; within the UK, the small number of 'successful' attacks that have actually taken place since 9/11 suggests that they have largely achieved this primary objective. In *Securing Freedom*, the former Director of MI5, Eliza Manningham-Buller, reinforces this point: '...from 9/11 until I retired in 2007, we faced fifteen serious terrorist plots and many, many smaller ones.'<sup>2</sup> Notwithstanding the subsequent murder of Gunner Lee Rigby in May 2013, it is difficult to argue with her assessment that '[o]nly the four suicide bombers of 7/7 succeeded[.]'<sup>3</sup>

Whilst the UK authorities should be proud about their record in *preventing* so many substantial plots, enormous efforts have been made to *prepare for* and *respond to* the occurrence of any such events. Indeed, whatever one's attitude towards the proportionality of CONTEST, the authorities were clearly prudent after 9/11 to 'prepare for the worst' on the basis that it would be unlikely that all potential attacks could be successfully thwarted. One former head of London's Metropolitan Police Service (MPS)

---

<sup>1</sup> An image and an account of this story appear in 'Images of 7 July: Reluctant hero', *BBC Website*, 2 July 2006, Via: <http://news.bbc.co.uk/2/hi/5105750.stm> (accessed 19.07.13)

<sup>2</sup> Eliza Manningham-Buller, *Securing Freedom* (London: Profile Books Limited, 2012), p.52

<sup>3</sup> *Ibid.*

captured this when he ‘notoriously said to the media that it was a question of *when*, not *if*.’<sup>4</sup>

The policies and procedures put in place to handle such incidents did not happen accidentally. Indeed, the manner in which the Government has worked (and continues to work) with partners ‘to prepare for, respond to, and recover from emergencies’<sup>5</sup> - to quote the Cabinet Office’s longstanding aim for the UK’s national emergency management procedures - has long been recognised as an important aspect of CONTEST; one of its four guiding pillars, ‘Prepare’, is specifically concerned with how ‘to mitigate the impact of a terrorist attack.’<sup>6</sup> The introduction of a new approach incorporating how to *manage the consequences of an event* in the new security environment is not limited to CT strategy; as London bid to host the 2012 Olympic Games, for example, it was even decided that planning for all types of emergencies - what the UK’s official ‘Bid Book’ called ‘consequence management’ - would comprise one of the ‘three key functions’ that would be delivered by those responsible for the Games’ security preparations.<sup>7</sup>

Before analysing specific examples of corporate involvement in UK emergency preparedness, it is worth recalling that this thesis is concerned with examining the ‘industrial-complex’ in the CT sector; it is relevant, therefore, to consider how terrorism itself has driven the structural reforms in this sector since 9/11. In a major 2004 speech, David Omand (then the UK’s Security and Intelligence Coordinator in the Cabinet Office) explained that ‘it is terrorism that poses the major – although clearly not the only – risk to

---

<sup>4</sup> Omand, ‘The Terrorist Threat to the UK in the Post-9/11 Decade’ (Emphasis added)

<sup>5</sup> Cabinet Office, ‘Improving the UK’s ability to absorb, respond to, and recover from emergencies’, Gov.uk Website, Via: <https://www.gov.uk/government/policies/improving-the-uks-ability-to-absorb-respond-to-and-recover-from-emergencies> (accessed 19.07.13)

<sup>6</sup> HM Government, ‘CONTEST: The United Kingdom’s Strategy for Countering Terrorism’ (2011), p.10

<sup>7</sup> London 2012, *Candidature File: Volume 3 - Theme 12* (2004), p.35

the security of the UK<sup>8</sup>, and that it was this threat ‘that drives most of the programmes of improvement we need’<sup>9</sup>. Coaffee similarly highlights that 9/11 ‘significantly speeded up’ the process of emergency planning reform<sup>10</sup>; Richards has also noted that whilst the Government’s decision to establish a Civil Contingencies Secretariat (CCS) in 2001 was initially made ‘in response to the fuel protests, the foot and mouth disease outbreak, and flooding in 2000’<sup>11</sup>, this was ‘given a whole new impetus’<sup>12</sup> following 9/11. A former Director of the CCS, Bruce Mann, has described the 9/11 attacks as a ‘further, substantial stimulus towards reform’<sup>13</sup>.

It is clear, therefore, that terrorism was a significant driver in the development of the UK’s emergency preparedness activities after 9/11. In this context, the role that the private sector has played in UK emergency preparedness has received some analytical attention<sup>14</sup>, but, like with other security topics, any interest has tended to be ‘siloes’ or seen to be of secondary importance; limited to rather general statements around the importance of the activities of individual business sectors, or seen largely through a

---

<sup>8</sup> David Omand, ‘National Resilience Priorities for UK Government’, Speech given at RUSI at the launch of the Homeland Security and Resilience Department, 1 July 2004, Via: <http://www.rusi.org/analysis/commentary/ref:C40AB913E66BA2/> (accessed 19.07.13). This speech formed the basis of David Omand, ‘Emergency Planning, Security and Business Continuity’, *RUSI Journal*, Vol.149:4 (2004), pp.26-33

<sup>9</sup> Ibid.

<sup>10</sup> Jon Coaffee, ‘From Counterterrorism to Resilience’, *The European Legacy*, Vol.11:4 (2006), p.398

<sup>11</sup> Anthony Richards, ‘The emergency response: Progress and problems’ in Wilkinson, *Homeland Security in the UK*, p.344

<sup>12</sup> Ibid.

<sup>13</sup> Bruce Mann, ‘The UK civil contingencies framework – building common endeavour’, in Paul Cornish (Ed.) *Britain and Security* (London: Smith Institute, 2007), Via: <http://www.smith-institute.org.uk/file/BritainandSecurity.pdf> (accessed 29.07.13), p.46. There was recognition prior to 9/11 that the UK Government’s national emergency management structures needed reform to be able to address all the relevant security risks facing modern society. See, for example, Geoff O’Brien and Paul Read, ‘Future UK emergency management: new wine, old skin?’, *Disaster Prevention and Management*, Vol.14:3 (2005), p.354

<sup>14</sup> See especially Omand, *Securing the State*, pp.80-83. The author has also noted that ‘[f]rom an emergency preparedness perspective, (...) a thorough awareness of the extensive role played by the private sector has been developed; Veness (2003), Stewart (2005) and Gregory (2007), for example, have all articulated the requirement for business sectors of all varieties to work with Government to ensure their resilience against terrorism.’ Rosemont, ‘Private sector engagement’, pp.148-149

corporate security and resilience lens.<sup>15</sup> In view of the potential sizeable effects of major emergencies on parts the UK business community, and the role many companies now play in their mitigation, a greater understanding is needed, drawn from a broader perspective, of the character of the public-private relationships in this sector. Before doing so, the next section details the structures developed by the UK Government to enhance emergency preparedness after 9/11, and the ways in which the role of the ‘private sector’ has been considered within that framework.

### **3.1 Government policy approach and governance arrangements**

The UK Government’s policy framework for emergency preparedness underwent radical changes throughout the 2000s; a greater degree of central direction and a fuller appreciation of the wide variety of risks facing the UK characterized the reforms. On the former, the move towards ‘greater emphasis on cross-departmental and extra-departmental coordination’<sup>16</sup> has been expertly covered by Smith whilst, referring to the plans to establish the CCS at the start of the decade, Feakin summarises how ‘...[i]t became clear that the UK required a body with the authority to prepare, respond and recover from any kind of emergency, be it man made or natural.’<sup>17</sup> Omand has similarly explained; ‘Public protection (...) requires that there are effective emergency responses against the widest range of major threats and hazards.’<sup>18</sup> Reflecting this, ‘there has been a *broadening of the emergency planning agenda*’<sup>19</sup> in the UK after 9/11. In short, the revised framework

---

<sup>15</sup> The main research focus on this topic to date has been around the steps businesses should take to protect themselves from the consequences of terrorism. See cited authors in footnote 14.

<sup>16</sup> James Smith, ‘Civil Contingency Planning in Government’, *Parliamentary Affairs*, Vol.56:3 (2003), p.412

<sup>17</sup> Tobias Feakin, ‘UK Perspectives on Security in an age of ‘Shock and Aftershock’ in Klaus Thoma (Ed.) *European Perspectives on Security Research* (Berlin: Springer-Verlag, 2011), p.47

<sup>18</sup> Omand, ‘The Terrorist Threat to the UK’

<sup>19</sup> Coaffee, ‘From Counterterrorism to Resilience’, p.397 (Emphasis in original)

adopted an ‘all-hazards approach’<sup>20</sup>, or what has perhaps been more appropriately described as ‘multi-hazard management’<sup>21</sup>. The significance of the new approach should not be underestimated; the reforms introduced a completely new policy framework for handling UK emergencies.

Supporting this radical new posture was the introduction of ‘national resilience’ as a central driving concept behind the UK’s post-9/11 emergency preparedness framework. The ‘interesting choice’<sup>22</sup> of phraseology has received much analytical attention; O’Brien and Read, for example, have argued that resilience ‘...is increasingly used in the disaster management sphere and reflects a trend towards a holistic and proactive approach that has the community, and its ability to resist and recover, as its focus’<sup>23</sup>. Analysing policy developments in this field, Coaffee explains that ‘it is now common to talk of minimising the terrorist risk by developing *resilience*.’<sup>24</sup> He continues:

Post 9/11 metaphors of resilience have been used to describe how cities and nations attempt to “bounce-back” from disaster, and to describe the embedding of security and contingency features into planning systems.<sup>25</sup>

In *Securing the State*, Omand presents an interpretation of ‘national resilience’ as ‘...strengthening the overall ability of society to bounce back as quickly as practicable into the patterns of normal life after a major disruption.’<sup>26</sup> An important feature of the UK’s recent approach to (and thus policy framework for) emergency preparedness, therefore, is that, despite enormous determination and every best effort being made to *prevent* any atrocities, it has never pretended to be able to completely *remove* the risk of something

---

<sup>20</sup> Feakin describes the ‘all-hazards approach’ as ‘...meaning preparations should be sufficiently flexible to cover both natural and man-made threats.’ Feakin, ‘UK Perspectives on Security’, pp.47-48

<sup>21</sup> Coaffee, ‘From Counterterrorism to Resilience’, p.396

<sup>22</sup> O’Brien and Read, ‘Future UK emergency management’, p.354

<sup>23</sup> Ibid.

<sup>24</sup> Coaffee, ‘From Counterterrorism to Resilience’, p.396 (Emphasis in original)

<sup>25</sup> Ibid.

<sup>26</sup> Omand, *Securing the State*, p.60

untoward happening. In a separate article, Omand stresses the centrality of this idea within CONTEST:

The CONTEST strategic aim reflects the risk management approach by having the objective ‘to reduce the risk’ from terrorism so that people can go about their normal business, freely (that is, without having to interfere with individual freedoms and liberties) and with confidence (that is, with people still travelling by air and on the underground, visitors coming to the UK, confidence in the markets and so on).<sup>27</sup>

Different conceptualisations of ‘resilience’ may exist internationally, however the concept was cleverly chosen for the UK in view of the realistic (if not slightly pessimistic) assumption that, despite every best effort to prevent them, it would only be prudent to assume that some security events (such as terrorist attacks) would occur. CONTEST has always been clear in this context that capabilities would be developed to ‘deal with disaster’<sup>28</sup>, should ever it strike.

What specific, practical policies did the UK Government pursue in this area after 9/11, and how has the governance framework for UK emergency preparedness evolved? It is not a straightforward matter to generalise about the development of the character of what Gregory has called the ‘National governance structures to manage the response to terrorist threats and attacks’<sup>29</sup>, but reference to the Government’s own policy documentation and other material helps to identify the main elements of the approach. Importantly, it can be noted that despite the new reforms the manner of actually *handling* major emergencies has remained broadly similar for decades. As Hills put it:

---

<sup>27</sup> Omand, ‘The Terrorist Threat to the UK’

<sup>28</sup> Even prior to 9/11, ‘Dealing with Disaster’ was the title of a Home Office document (published in 1992, 1994, and 1997) designed ‘to provide a framework for integrated emergency management’. Roger Miles, ‘Empowering Emergency Responders’ in Simon Bennett (Ed.) *Innovative Thinking in Risk, Crisis, and Disaster Management* (Farnham: Gower Publishing Ltd, 2012), p.32

<sup>29</sup> Frank Gregory, ‘National governance structures to manage the response to terrorist threats and attacks: A cross-national comparative analysis with special reference to the UK ‘lead department’ response structure and UK counter-terrorism strategy’ in Wilkinson (Ed.) *Homeland Security in the UK*, pp.117-140

...there has never been one man or one organization charged with managing the national response to disasters, and successive administrations have consistently maintained that control in such matters must be exercised locally: assistance may be needed from neighbouring areas and organizations, from the national government and from international organizations such as the EC [European Commission], but the responsibility to plan for and deal with a disaster has remained a local responsibility.<sup>30</sup>

Whilst more central coordination, new statutory requirements and numerous central programmes were introduced after 9/11, as described below, O'Brien and Read's argument is widely accepted: 'the overall structure will remain largely the same; that is, government fulfilling the role of co-ordinator and offering guidance and with local agencies left to get on with the task.'<sup>31</sup>

Smith concurs that 'the guiding principles behind contingency planning remain largely unchanged.'<sup>32</sup> Whilst he explains how after 9/11 there would be a greater requirement for 'partnership bodies' to deliver the response (i.e. rather than primarily 'empowering local authorities in emergency planning'<sup>33</sup>), there would be little overall change to the allocation of operational responsibilities following the reforms: 'The centre may thus be seen as providing strategic advice and coordination on contingency planning while actual implementation is left to the localities.'<sup>34</sup> The result, according to Hills, is that the 'organizational arrangements for disaster response in the United Kingdom are extremely complex.'<sup>35</sup> Immediately, the character of these arrangements appears very different to those within defence, or what is labelled the MIC; within the latter system, the MoD clearly possesses more streamlined control over policy, and indeed operational direction in the sector.

---

<sup>30</sup> Alice E. Hills, 'Co-ordination and Disaster Response in the United Kingdom', *Disaster Prevention and Management*, Vol.3:1 (1994), p.66

<sup>31</sup> O'Brien and Read, 'Future UK emergency management', p.358

<sup>32</sup> Smith, 'Civil Contingency Planning in Government', p.421

<sup>33</sup> *Ibid.* p.415

<sup>34</sup> *Ibid.* p.413

<sup>35</sup> Hills, 'Co-ordination and Disaster Response', p.66



Considerable changes were made, however. As the legal cornerstone of the revised approach, a new statutory basis was established; '[t]he changes to the legislative base underpinning civil protection' were 'wholesale'<sup>36</sup>. The Government passed the Civil Contingencies Act 2004 (CCA) and this 'was the first wholesale revision of UK emergency legislation since the 1920s.'<sup>37</sup> It was indeed hardly insignificant: Omand explained that '[t]he Bill provides us with a complete modern legislative framework for dealing with civil contingencies replacing the present inadequate patchwork of historic law.'<sup>38</sup> Under the CCA, which came into force in April 2005, a series of 'functional and collaborative duties' were placed upon '(“category 1”) responders at the core of emergency response (such as the emergency services and local authorities)<sup>39</sup>; these included 'risk assessment', 'emergency planning', 'business continuity management' and 'information sharing' amongst other activities.<sup>40</sup> Thus a substantially revised set of official responsibilities was created.

Significant changes to the machinery and operation of central Government were also made after 9/11; the establishment in 2001 of the CCS was a substantial decision that aimed to introduce greater coordination. Writing in 2007, Gregory explained how '[t]he principal objectives of the CCS are horizon scanning and overseeing the departmental responses to the threat assessments produced by the Joint Terrorism Analysis Centre'<sup>41</sup>, and how its additional responsibilities included '...policy development, ensuring that those responsible for crisis management and operational matters properly discharge their duties and promulgating doctrine, development of key skills and issue awareness through the

---

<sup>36</sup> O'Brien and Read, 'Future UK emergency management', p.356

<sup>37</sup> Richards, 'The emergency response: Progress and problems', p.344

<sup>38</sup> Omand, 'National Resilience Priorities for UK Government'

<sup>39</sup> Mann, 'The UK civil contingencies framework', p.47

<sup>40</sup> Ibid.

<sup>41</sup> Gregory, 'National governance structures', p.118

Emergency Planning College.<sup>42</sup> The current responsibilities of the CCS appear on a Government website; '[i]ts work concentrates on 4 main areas: risk assessment, preparation and planning, response and recovery, and building a resilient society.'<sup>43</sup> As shown below, the CCS also interacts with the private sector in this context.

Reflecting the Government's responsibilities, several new public guidance documents on emergency preparedness were produced. Richards notes that an updated iteration of *Dealing with Disasters* was published in parallel to the production of the original Civil Contingencies Bill in 2003<sup>44</sup> and, according to a letter from the then head of CCS to colleagues, this document provided 'the Government's core guidance to emergency planners and local responders' and reflected 'the many changes that have taken place since the third edition was published by the Home Office in 1998.'<sup>45</sup> Gregory also notes 'the issuing of two guidance documents by the Cabinet Office CCS: *Emergency Preparedness* and *Emergency Response and Recovery*.'<sup>46</sup> Separately, Feakin has explained the significance of the introduction of a 'National Risk Register'<sup>47</sup> (NRR) which '...sets out the government assessment of the likelihood and potential impact of risks that will directly impact the UK.'<sup>48</sup> Structural changes were therefore accompanied by a substantial proliferation of documentation aimed at all parties involved in UK emergency preparedness, including the public.

---

<sup>42</sup> Ibid. pp.118-119

<sup>43</sup> Cabinet Office, 'Improving the UK's ability to absorb, respond to, and recover from emergencies'

<sup>44</sup> Richards, 'The emergency response: Progress and problems', p.344

<sup>45</sup> Susan Scholefield, Head of the CCS, letter, 19 June 2003, Via:

<http://webarchive.nationalarchives.gov.uk/20050523205851/http://ukresilience.info/contingencies/dwd/scholefield.pdf> (accessed 30.07.13) Letter originally cited in Ibid.

<sup>46</sup> Frank Gregory, 'UK draft Civil Contingencies Bill 2003 and the subsequent Act: Building block for homeland security?' in Wilkinson (Ed.) *Homeland Security in the UK*, p.340 (Emphasis in original)

<sup>47</sup> The NRR has been made publicly available by the Government since 2008 and has consistently looked upon terrorism as amongst the most serious national security risks to the UK; the 2013 edition of NRR, for example, assesses that 'catastrophic terrorist attacks' remain one of the highest priority risks facing the country. Cabinet Office, 'National Risk Register of Civil Emergencies – 2013 Edition', Via:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/211867/National\\_RiskRegister2013\\_amended.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/National_RiskRegister2013_amended.pdf) (accessed 29.12.14), p.7

<sup>48</sup> Feakin, 'UK Perspectives on Security', p.48

Several other efforts were made throughout the 2000s to either update previous guidance or develop new policy on UK emergency preparedness; the introduction of the Government's *Concept of Operations* and the *Strategic National Framework on Community Resilience* were perhaps the most significant policy shifts. The first of these 'sets out the flexible arrangements for coordinating the response to and recovery from emergencies within the UK'<sup>49</sup>; outlining in 80 pages the framework that central government will adopt in the event of an emergency.<sup>50</sup> Amongst the most important functions this document performs is, firstly, to describe;

...how the UK central government response will be organised, and the relationship between the central, regional and local tiers in England, as well as the relationship between the UK central government and the devolved administrations in Scotland, Wales and Northern Ireland.<sup>51</sup>

Secondly, the COP also outlines how emergencies will be handled at the political level, when appropriate, through a detailed section that outlines 'The Role and Organisation of the Cabinet Office Briefing Rooms (COBR)'<sup>52</sup>. New resources were allocated to these structures, and a debate emerged around the effectiveness of them.<sup>53</sup>

The role of non-governmental partners in emergency preparedness (including communities and the private sector) was also addressed in the new material. According to *The Strategic National Framework on Community Resilience* document, for example, '[t]he framework is intended to provide the national statement for how individual and

---

<sup>49</sup> Ibid., p.5

<sup>50</sup> Cabinet Office, 'The central government's concept of operations', Via: <https://www.gov.uk/government/publications/the-central-government-s-concept-of-operations> (accessed 30.07.13)

<sup>51</sup> Ibid.

<sup>52</sup> Cabinet Office, 'Responding to Emergencies, The UK Central Government Response, Concept of Operations', 23 April 2013, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/192425/CONOPs\\_incl\\_revised\\_chapter\\_24\\_Apr-13.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192425/CONOPs_incl_revised_chapter_24_Apr-13.pdf) (accessed 30.07.13), pp.21-43

<sup>53</sup> A former MPS officer, Andy Hayman, has been the most vocal critic of COBR, describing it as possessing 'no bite'. Andy Hayman and Margaret Gilmore, *The Terrorist Hunters* (London: Bantam Press, 2009), pp.304-317

community resilience can work'<sup>54</sup>, and aims to act 'as a set of guiding principles which encourage and enable people to take steps to be prepared for an emergency.'<sup>55</sup> Alongside this document, the Cabinet Office recognised the benefit of even wider engagement, as its website almost patronisingly explains: 'The wider UK society - public and private sector, communities and businesses - will find it useful to know how their work fits into a wider framework on resilience for their sector.'<sup>56</sup> Closely connected to the work developed under the 'community resilience' label, the Government has developed a substantial suite of dedicated advisory material for the private sector. This includes the publication annually of 'Sector Resilience Plans'<sup>57</sup>, for example, and, more recently, the development of a 'Corporate Resilience Strategy' designed '...to promote effective but inexpensive ways to enable SMEs to build resilience to all kinds of hazards and threats.'<sup>58</sup> Such documents clearly illustrate the Government's view of the important role played by the private sector in UK emergency preparedness.

To support the emerging policy objectives, new programmes were developed by various agencies. Most significant amongst these, according to Richards, was the creation by CCS of a new 'Capabilities Programme'. The current aim of the National Resilience Capabilities Programme is:

...to increase the capability of the United Kingdom to respond to and recover from civil emergencies. It does this by building capability to deal with the consequences that are common to most types of emergency,

---

<sup>54</sup> Cabinet Office, 'Strategic National Framework on Community Resilience', March 2011, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/60922/Strategic-National-Framework-on-Community-Resilience\\_0.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60922/Strategic-National-Framework-on-Community-Resilience_0.pdf) (accessed 31.07.13), p.3

<sup>55</sup> Ibid., p.5

<sup>56</sup> Cabinet Office, 'Resilience in society: infrastructure, communities and businesses', Via: <https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses> (accessed 30.07.13)

<sup>57</sup> Cabinet Office, 'Sector resilience plans', Via: <https://www.gov.uk/government/publications/sector-resilience-plans> (accessed 30.07.13)

<sup>58</sup> Cabinet Office, 'Resilience in society'

regardless of whether those emergencies are caused by accidents, natural hazards or man-made threats.<sup>59</sup>

Capabilities within this programme varied and included ‘...a number of interdependent and interrelated factors including appropriate numbers and types of personnel, the right types of equipment and supplies, relevant and sufficient training and exercising, clear plans etc.’<sup>60</sup> This included the procurement of new equipment for the emergency services through the ‘New Dimension’ programme; enhanced ‘Cabinet Office-approved emergency planning and crisis management training’<sup>61</sup> also emerged as a core, centrally-driven capability through the (now privately-operated) Emergency Planning College.

The Government has consistently recognised the private sector’s central role in ensuring UK national resilience; the original provisions of the CCA even stated that a number of private sector organisations would be designated as ‘Category 2’ responders – what Mann describes as ‘co-operating bodies’<sup>62</sup> – thus encouraged to meet various requirements directly. In his dedicated chapter on this subject, Gregory highlights the categories succinctly:

In part, this public-private sector inter-relationship in emergency response is reflected in the new civil contingencies legislation with its listing of Category One Responders – the public sector – and Category Two Responders – mainly those private sector bodies with critical national infrastructure responsibilities.<sup>63</sup>

Mann’s account of the CCA also shows how the Government recognised the need to take account of the role of the private sector, and the tensions inherent in doing so:

---

<sup>59</sup> Cabinet Office, ‘Preparation and planning for emergencies: the National Resilience Capabilities Programme’, Via: <https://www.gov.uk/preparation-and-planning-for-emergencies-the-capabilities-programme> (accessed 30.07.13)

<sup>60</sup> Ibid.

<sup>61</sup> ‘About Us’, Emergency Planning College Website, Via: <http://www.epcollege.com/epc/about-us/> (accessed 30.07.13)

<sup>62</sup> Mann, The ‘UK civil contingencies framework’, p.47

<sup>63</sup> Frank Gregory, ‘Private sector roles in counter-terrorism’ in Wilkinson (Ed.) *Homeland Security in the UK*, p.321

As far as the business sector was concerned, policy making around the act had carefully to consider the impact of market pressures – whether positive, in providing firms that engage in relevant planning with a competitive edge, or negative, in placing burdens on firms that do so. It thus had to find the right balance between, on the one hand, placing preparedness duties in law on the business sector that mirror those placed on public-sector bodies, and, on the other, the strong desire to reduce the burden of regulation on business.<sup>64</sup>

Private sector involvement in emergency preparedness is not limited to its statutory responsibilities. Whilst the involvement of the security suppliers' community has not been well documented within this field, it is evident that this part of 'industry' has seen a clear role for itself in the UK; the full, unabbreviated name of the leading representative security industry alliance (examined in Chapter 6) is the 'UK Security *and Resilience* Industry Suppliers' Community'. Equally, it is apparent that at the strategic level the security industry is currently seeking to develop new, joint policy initiatives with government on both security and 'resilience related'<sup>65</sup> matters: whilst one industry executive stated that he had not 'discerned that anyone or anywhere else had picked up the resilience mantle'<sup>66</sup> after Bruce Mann had left office, RISC's interaction has developing more broadly than on CT issues through the recent development of a *Security and Resilience* Growth Partnership.<sup>67</sup>

Prior to this thesis, no study had sought to examine in detail such a wide interpretation of the private sector's involvement within UK emergency preparedness, let alone seek to assess its potential consequences. This chapter examines the character of the involvement, exploring the extent to which the dynamics of the MIC as historically understood may have transferred into the CT sector. Before conducting such analysis, an indication is provided of the levels of expenditure that have been allocated to the UK Government's post 9/11 emergency preparedness priorities.

---

<sup>64</sup> Mann, The 'UK civil contingencies framework', p.47

<sup>65</sup> This useful expression appears in Charlie Edwards, *Resilient Nation* (London: Demos, 2009), p.15

<sup>66</sup> Interview, Industry Executive

<sup>67</sup> *Ibid.*

### 3.2 Security expenditure

The complexity of the UK's post-9/11 governance arrangements for emergency preparedness is now apparent. The combination of such a disaggregated structure with the fact that some budgetary material is of a security-sensitive nature makes it difficult to obtain a full picture of 'resilience' expenditure within the sector; the further complicating lack of coordination around the UK's national security expenditure more broadly has also been covered in one high profile study.<sup>68</sup> However, an indication can be provided of the size and growth of UK emergency preparedness budget. Whilst it would be futile to seek to establish a *complete* picture of post-9/11 UK resilience expenditure, a better understanding of UK resilience spending can be achieved through the analysis of official documents, parliamentary exchanges, and other scholarly literature.

As this thesis is concerned with *national* security strategy, the investment that central UK Government has allocated towards meeting its emergency preparedness or 'resilience' objectives is important to grasp. In response to a parliamentary question tabled in 2011 on the budget of the CCS since 2005, the Minister of the Cabinet Office, Francis Maude MP, replied that the budget 'for each financial year between 2008-09 and 2011-12 was/is'<sup>69</sup>:

**Figure 3. CCS Spending 2008-2012**

	£
2008-09	9,641,750
2009-10	9,646,750
2010-11	9,615,758
2011 -12	10,514,000

<sup>68</sup> IPPR, 'Shared Responsibilities', pp.99-100

<sup>69</sup> Hansard, Francis Maude, Parliamentary Question Reply, 10 Nov 2011: Column 452W, Via: <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm111110/text/111110w0003.htm#11111097001723> (accessed 01.08.13) Table adapted from Parliamentary information licensed under the Open Parliament Licence v3.0.

CCS budgetary figures for the years 2001-2008 were not as readily available; however, the Cabinet Office's Annual Reports and the UK Parliament's 'Hansard' publication provide more detail on centrally-funded, post-9/11 UK resilience spending. Whilst the initial 'start-up' funding apportioned to the CCS following its creation are not clear<sup>70</sup>, £53.4 million was allocated in 2002-03 towards the overall stated objective '[t]o co-ordinate security, intelligence and civil contingencies matters to protect the UK against disruptive challenges'<sup>71</sup>. An early official breakdown of the overall funding provided by the Government states that a smaller, specific figure of '£39.5 million was allocated to the CCS in February 2003, for example, including the £10 million administration and capital costs of the Secretariat, the £19 million Local Authority Grant and £10 million to the Met Office.'<sup>72</sup> Whilst figures are difficult to obtain, on the available information it seems that the costs for the CCS have remained broadly consistent - around £10m per annum - since 9/11.

The CCS budget is not the only indicator of centrally-funded UK emergency preparedness expenditure, however, as records of Government grants issued to enhance regional capabilities indicate. A closer examination into the investment allocated to enhance London's arrangements illustrates how funding has been made up of a mixture of contributions from *both* central and local Government. The 'resilience' page of the London Fire Brigade (LFB) states:

In recent years, we have made substantial investment, supported by the government and the Mayor of London, in additional vehicles, equipment and training for our firefighters to manage major incidents.<sup>73</sup>

---

<sup>70</sup> The Cabinet Office's Department Reports of 2001 and 2002 are silent on this.

<sup>71</sup> Cabinet Office, *Departmental Report 2003*, Cm5926, Via: [http://webarchive.nationalarchives.gov.uk/20100416132449/http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/annualreport/co\\_report2003.pdf](http://webarchive.nationalarchives.gov.uk/20100416132449/http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/annualreport/co_report2003.pdf) (accessed 30.10.13), p.28

<sup>72</sup> Hansard, Douglas Alexander, Parliamentary Question Reply, 21 March 2003: Column 958W, Via: [http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030321/text/30321w01.htm#30321w01.html\\_wqn7](http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030321/text/30321w01.htm#30321w01.html_wqn7) (accessed 02.08.13)

<sup>73</sup> London Fire Brigade, 'Resilience', Via: <http://www.london-fire.gov.uk/Resilience.asp> (accessed 04.08.13)



Reflecting this approach, the London Fire and Emergency Planning Authority (LFEPA) has regularly received a 'Fire and Rescue Service capital grant' from the Department of Communities and Local Government (DCLG); this amounted to £2,195,000 in 2009/10 and £3,674,000 in 2010/11<sup>74</sup>, for example. Whilst it is important to recognise that this grant is both London-specific and has not solely been concerned with the development of capabilities relating to the preparation for (and management of) major *terrorist emergencies* - this allocation is for *all* aspects of the LFB's operations - the accounts clearly illustrate the strong emphasis that the additional funding has placed on investing into the LFB's capital programmes; these are marked against line items such as 'Resilience', accommodation for the 'new dimensions programme' and investment into the service's 'control and communications project'<sup>75</sup>. Furthermore, the contribution that central Government has allocated to the LFB's capital programmes reflects the decentralised character of the governance (and funding) framework for UK emergency preparedness; again, this contrasts with the defence sector where arrangements are more centralised.

Funding was not solely allocated towards enhancing *London's* resilience capabilities; several centrally-coordinated, national programmes were pursued after 9/11. Most notably, the 'New Dimension' programme was a DCLG flagship enterprise. A report completed in 2008 by the National Audit Office (NAO) explains the purpose of the scheme:

...to rapidly, effectively and flexibly tackle the consequences of terrorist and other large-scale catastrophic incidents, such as flooding, by: providing appropriate specialist vehicles and equipment; funding training for

---

<sup>74</sup> London Fire and Emergency Planning Authority, 'Budget 2009/10', FEP 1321, March 2009, Via: <http://www.london-fire.gov.uk/Documents/FEP1321.pdf> (accessed 04.08.13), p.5

<sup>75</sup> These three items accounted for £22,552,000 (respectively: £4,115,000, £1,022,000, £17,415,000) or 39% of the LFB's capital investment programme worth £57,224,000 in 2007/08. London Fire and Emergency Planning Authority, 'Budget 2008/09', FEP1195, March 2008, Via: <http://www.london-fire.gov.uk/Documents/FEP1195.pdf> (accessed 04.08.13), pp.67-68

firefighters to use the new equipment; and supporting planning for deployment of the equipment in the case of an emergency.<sup>76</sup>

Helpfully, the scope (and effectiveness) of the DCLG's procurement activities under this programme have been analysed by the NAO - the acquired capabilities range from 73 'incident response units' for mass decontamination through to training for 20 'Urban Search and Rescue teams'<sup>77</sup>. Even more usefully, the report also outlines how the DCLG:

...has committed some £330 million to the programme: £190 million on vehicles and equipment, £85 million on training and crewing, and an estimated £55 million on programme administration[.]<sup>78</sup>

Whilst in terms of its overall size New Dimension is smaller than many MoD procurement projects, it clearly constitutes one of the UK's largest new, non-military CT equipment programmes after 9/11. That it is considered to have been both a necessary and a highly successful programme would seem to challenge some of the more strident accusations to have been levelled at 'the SIC'.

'New Dimension' was not the only CT-related procurement programme that had the aim of enhancing emergency preparedness after 9/11. As a separate NAO paper explains, the 'Fire and Resilience Programme' established within the department as a consequence of those events 'comprises three separate but interdependent projects'<sup>79</sup>; the two others being Firelink ('a £350 million project to upgrade each Fire and Rescue Service's current main radio-communication system'<sup>80</sup>) and FiRecontrol ('a £423 million project to provide a resilient network of nine regional control centres'<sup>81</sup>). As it was always intended that the information technology (IT) component of this latter project would

---

<sup>76</sup> National Audit Office, 'New Dimension – Enhancing the Fire and Rescue Services' capacity to respond to terrorist and other large-scale incidents', Report by the Comptroller and Auditor General, HC 1050, Session 2007-2008, 31 October 2008, p.4

<sup>77</sup> Ibid., p.5

<sup>78</sup> Ibid., p.11

<sup>79</sup> National Audit Office, 'FiReControl Project', Memorandum for the House of Commons Communities and Local Government Select Committee, February 2010, p.7

<sup>80</sup> Ibid.

<sup>81</sup> Ibid.

constitute the largest single contract of any of these projects<sup>82</sup>, it is selected as the primary case study for further examination into the dynamics of the private sector's involvement in this sub-sector (see Section 3.3).

Whilst it is difficult to determine an *exact* overall figure for UK resilience spending after 9/11, the NAO found in 2010 that central government in the form of DCLG invested 'over £1 billion with the aim of improving their [local Fire and Rescue Authorities] capacity to respond to incidents including large-scale disasters caused by terrorists, accident or nature.'<sup>83</sup> Therefore, as the basis for this chapter's examination, a substantial amount of 'new' public expenditure was allocated to this aspect of CT after 9/11; this can be said to be largely attributable to the Government's increasing desire to address non-military security threats (such as terrorism) alongside classic 'defence' issues in the new context. In view of this sizable additional investment, the ways in which the private sector has been engaged in that endeavour warrant further attention.

### **3.3 Public-private security interactions**

This section examines an extensive and varied network of public-private security interaction in the UK emergency preparedness sector, supporting the notion that an 'industrial-complex' of a different character to the MIC exists in the CT aspects of UK national security strategy. After introducing more details on the involvement of security suppliers in this sector, the section analyses the dynamics that emerged between the public and private sectors in the FiReControl programme, and more broadly.

#### ***Security Suppliers***

---

<sup>82</sup> The NAO states that DCLG's IT contract for FiReControl 'was originally valued at 200 million.' Ibid., p.21

<sup>83</sup> *ibid.* p.7

In contrast to the other sub-sectors of CONTEST considered in this thesis, it is clear that, at least in its public pronouncements, the UK Government has seen a limited strategic role for the security suppliers' community in helping it to fulfil its resilience objectives. Instead, it has focused on developing relationships with the 'business community' considered in the wider sense as being an operational actor that should prepare itself for significant emergencies. Whilst the need to harness technologies developed by the DIB for resilience purposes has been viewed as an 'increasingly important' aspect of the response<sup>84</sup>, the CCS does not appear to have resourced itself to embrace the same outlook. In reality, the emergence of a self-standing 'resilience industry' has not materialised; such a thing is rarely considered separately from the wider 'security industry'<sup>85</sup>.

This is not to suggest that suppliers have not seen a role for themselves in this sub-sector of CONTEST; perhaps the most explicit 'pitch' in this respect is found in a chapter written by a (now former) Director of the security company, G4S. Ian Horseman-Sewell advocates the need for 'partnership with the private sector' to enhance UK resilience, claiming that: '...we have been seeking to lead a vibrant debate about increasing the role of the private security industry in planning for and responding to natural and man-made emergencies in the UK[.]'<sup>86</sup> Promoting the idea that '[t]he private sector has specific 'resilience-building' and 'response' capabilities to offer'<sup>87</sup>, Horseman-Sewell insists that 'the motivation for private security providers to plan for and handle disasters is *not* purely

---

<sup>84</sup> Omand, *Securing the State*, p.82

<sup>85</sup> The government-funded organisation responsible for promoting companies in Scotland, Scottish Enterprise, has referred to the 'Security and resilience industry in Scotland', for example. Scottish Enterprise, 'Security and resilience industry in Scotland', Via: <http://www.scottish-enterprise.com/your-sector/aerospace-defence-and-marine/adm-strategy/adm-facts/security-facts.aspx> (accessed 06.08.13)

<sup>86</sup> Ian Horseman-Sewell, 'Augmenting resilience and response: in partnership with the private sector' in Jennifer Cole (Ed.) *Emergency Response and Civil Defence: Report of the workshop held at the Royal United Services Institute on 11 December 2007* (RUSI: London, 2008), p.26

<sup>87</sup> *Ibid.* p.27

profit'<sup>88</sup>. Without specifying details, he claims that 'every year G4S provides *ad hoc* emergency support to governments around the world without charge.'<sup>89</sup>

The validity of these claims are difficult to ascertain but, even if it is accepted that the profit motive is not the *sole* reason for companies seeking involvement in UK resilience, interviews confirmed that it *is* a strong (and not necessarily illegitimate) factor which drives companies' involvement in the sector. When asked about the character of public-private security engagement generally, the Director for Security Industry Engagement at the Home Office responded:

I think there are different motives and different objectives between the public and the private sectors. So in the public sector there's a great deal of focus on the real mission to protect society, quite rightly so, and really to the exclusion of all else. (...) And I think if you then move over to the private sector - different motives. I mean we're there for profit motives, shareholder value, those sorts of things. A little bit of a suspicion from the public sector that that's their motive[.]<sup>90</sup>

It would certainly be naïve to think that commercial suppliers are not interested in seeking profits. It is also apparent that, in addition to its consistently stated desire to work with the private sector on emergency preparedness issues, the Government has not been opposed to working with the suppliers' community in this sector. It is apparent, for example, that in seeking to fulfil its objectives, the Government has awarded several sizeable contracts with suppliers in the 'resilience' space. One such example was the development of the FiReControl project from 2004; the public-private dynamics around the contract are now examined to examine the character of the 'industrial-complex' in this sector.

### **Case Study: FiReControl**

DCLG's FiReControl project consistently received media attention for all the wrong reasons. The title of one *Daily Telegraph* opinion piece - 'FiReControl Project: silly name,

---

<sup>88</sup> Ibid. (Emphasis added)

<sup>89</sup> Ibid. p.28 (Emphasis in original)

<sup>90</sup> Interview, Stephen Phipson

stupid idea – but you and I will pay for the fiasco<sup>91</sup> - sums it up aptly; the piece fiercely criticises the project, lamenting that no one had been held accountable for the failure described as both a ‘disaster’ and a ‘sorry saga.’<sup>92</sup> The article is not the only such assessment; according to a recent ‘update report’ on FiReControl by the UK Parliament’s Committee on Public Accounts (PAC), the project ‘was one of the worst cases of project failure that the Committee had seen’<sup>93</sup>. It is certainly difficult to describe FiReControl as anything other than a monumental failure. After efforts had consistently been made to ‘soldier on’ with the scheme, the main IT contract for the project was eventually cancelled in December 2010. Announcing that the Government was ‘calling time’ on the agreement with its prime contractor, Cassidian (formerly EADS Defence and Security, now Airbus Defence and Space), the then Fire Minister stated: ‘Following extensive discussion with Cassidian, we have jointly concluded, with regret, that the requirements of the project cannot be delivered to an acceptable timeframe.’<sup>94</sup>

In monetary terms, the project was an unmitigated disaster. As the NAO made clear in its critical review of the project after its cancellation: ‘FiReControl will have wasted a minimum of £469 million[.]’<sup>95</sup> Whilst fortunately the losses did not amount to the total cost of ‘£986 million over fifteen years’<sup>96</sup> that had once been anticipated by the Parliamentary Communities and Local Government Committee (CLG), the loss of almost half a billion pounds was a very regrettable waste of taxpayers’ money. Indeed, such is the

---

<sup>91</sup> Alasdair Palmer, ‘FiReControl Project: silly name, stupid idea – but you and I will pay for the fiasco’, *Daily Telegraph*, 24 Sept. 2011, Via: <http://www.telegraph.co.uk/news/politics/8786524/FiReControl-Project-silly-name-stupid-idea-but-you-and-I-will-pay-for-the-fiasco.html> (accessed 08.08.13)

<sup>92</sup> Ibid.

<sup>93</sup> Committee of Public Accounts, ‘FiReControl: Update report’, Sixteenth Report of Session 2013-14, HC 110, June 2013, p.3

<sup>94</sup> Department for Communities and Local Government, ‘Fire Minister Bob Neill calls time on FiReControl’, Gov.uk. 20 Dec. 2010, Via: <https://www.gov.uk/government/news/fire-minister-bob-neill-calls-time-on-firecontrol> (accessed 08.08.13)

<sup>95</sup> National Audit Office, ‘The failure of the FiReControl project’, Report by the Comptroller and Auditor General, HC 1272, Session 2010-2012, 1 July 2011, p.9

<sup>96</sup> Communities and Local Government Committee, ‘Fire and Rescue Service’, Fourth Report of Session 2005-06, Volume 1, HC 872-1, July 2006, p.14

high profile character of this significant debacle that FiReControl appeared as a case study in one recent account of UK Government blunders.<sup>97</sup>

It was not only the commercial outcome of the project that received condemnation from critics; the failures it exhibited in the area of project management have also been highlighted. In one particularly damning statement made during an evidence session for a PAC inquiry into the project, one Committee member revealed that the UK-based Association for Project Management had indicated to him that it uses FiReControl 'as a textbook example of how *not* to do a project.'<sup>98</sup> Whatever budding project practitioners might learn as a result of the contract failure, it would be a stretch to suggest that FiReControl ever intended to serve such a potentially useful purpose.

It would be equally misleading, however, to suggest that any or all of those individuals responsible for developing the scheme *intended* that such a large amount of taxpayers' money would be wasted, however. Before analysing the dynamics, it is important to understand the basic concept, origins and rationale of the project. 'What is FiReControl?' is the question posed within an overview document published by the DCLG in 2009; the answer now is 'not much', but it was then argued:

The FiReControl project will develop a network of nine, purpose-built Regional Control Centres (RCCs) to handle all emergency calls made to FRs [Fire and Rescue Services], using a single national operating system.<sup>99</sup>

In short, the pre-existing 49 control centres were to be replaced. The document continues:

The RCCs will be fully interconnected. Control room operators will have world-class equipment and technology so, for example, when a call can not

---

<sup>97</sup> Anthony King and Ivor Crewe, *The Blunders of our Governments* (London: Oneworld Publications, 2013), pp.193-194

<sup>98</sup> Committee of Public Accounts, 'The failure of the FiReControl project', Fiftieth Report of Session 2010-12, HC 1397, September 2011, Ev 8, p.24 (Emphasis Added)

<sup>99</sup> Department for Communities and Local Government, 'FiReControl – An Overview', 20 May 2009, Via: <http://webarchive.nationalarchives.gov.uk/20120919132719/http://www.communities.gov.uk/documents/fire/pdf/firecontroloverview.pdf> (08.08.13)

be answered by one RCC it will be handed on, with the same information available at the next RCC.<sup>100</sup>

This naturally invites the question as to why the Government sought to pursue this project; in short, differing views existed over the specific original aim(s) of FiReControl, not to mention the varying levels of support for it. It is clear from policy documentation and archive material, however, that the (then) Labour Government's desire to seek to both improve efficiency and enhance UK 'resilience' in the context of the terrorism threat were major drivers for all the projects developed under its 'Fire and Resilience Programme'.

The Government's 2003 White Paper, *Our Fire and Rescue Service*, captures the twin dynamic concisely. Outlining 'the case for moving towards regional-scale control rooms'<sup>101</sup> on the basis that the existing operation of control rooms at the local level 'is inefficient'<sup>102</sup>, it also argued that '[t]he events of 11 September 2001 have given further new impetus to the need to rationalise the way in which the fire service resources are used.'<sup>103</sup> Indeed, the Government was clear that the events of 9/11, together with the emergence of other risks, meant the Fire Service's capabilities had to be strengthened. In the document's Foreword, the Deputy Prime Minister declared unambiguously; 'That role involves tackling new threats which we are now facing, including terrorism, and threats such as flooding and other environmental disasters.'<sup>104</sup> Together with New Dimension and Firelink, FiReControl would become one of New Labour's flagship CT programmes in this context.

It is the initiation of the project on the grounds that it sought to enhance UK resilience after 9/11 that makes it a relevant case study for this thesis. Indeed, in oral evidence to the CLG the former Fire Minister, Shahid Malik MP, contested the idea that

---

<sup>100</sup> *ibid.*

<sup>101</sup> Office of the Deputy Prime Minister, 'Our Fire and Rescue Service', Cm 5808, (London: HMSO, 2003), p.29

<sup>102</sup> *ibid.* p.28

<sup>103</sup> *ibid.* p.29

<sup>104</sup> *ibid.* p.5



‘efficiency’ (i.e. monetary savings) was even the primary motivation behind FiReControl: ‘As far as I am concerned, this project was never about cost. It was always about the national resilience that FiReControl would provide.’<sup>105</sup> There should therefore be no doubt about the strength with which the ‘national resilience’ angle of the justification for the project gained resonance. The CLG reported its own understanding of the project’s aims:

The Government’s main motivation behind the amalgamation of fire control centres is to increase “resilience” by enabling the FRS to handle large-scale incidents better, from environmental disaster to a terrorist attack.<sup>106</sup>

This rationale is deployed in other project documentation. The Full Business Case for FiReControl, published in May 2009, stated:

The main rationale for FiReControl is to strengthen resilience locally, regionally and nationally – giving the FRS improved call handling and mobilisation capability to respond to incidents of every size and type.<sup>107</sup>

Terrorism might not have been the *sole* reason for the development of FiReControl, but the aim of improving national resilience in a world drastically re-shaped by 9/11 was clearly in the minds of those who developed the project.

Against this backdrop, how was the private sector involved in the FiReControl project and what were the causes of its failure? Could it be argued, as some critics of ‘the SIC’ might have it, that a coalition of vested interests coalesced around the Government’s post 9/11, CT-related resilience priorities, somehow managing to increase Government expenditure in this area to the benefit of a powerful (and profitable) elite? A closer examination of the public-private interactions that existed around the IT aspects of the project paints a different understanding of the situation.

---

<sup>105</sup> Communities and Local Government Committee, ‘Fire and Rescue Service’, Ev 18, p.72

<sup>106</sup> *ibid.*, p.14

<sup>107</sup> Department for Communities and local Government, ‘FiReControl Business Case: Version 1.1’, May 2009,

Via:<http://webarchive.nationalarchives.gov.uk/20120919132719/http://www.communities.gov.uk/documents/fire/pdf/1207425.pdf> (accessed 09.08.13), p.11

The circumstances surrounding the decision in December 2003 to proceed with FiReControl remain controversial; much has been said about the alleged priorities of senior Ministers at the time, and the resultant haste with which the Government decided to proceed. The NAO's analysis on the failure of the project is particularly illuminating; it found that 'neither the project plan nor the business case were finalised before the project's approval.'<sup>108</sup> It continued:

A Gateway Review by the Office of Government Commerce in April 2004 after the project had been approved found that the "extraordinarily fast pace" of the project was introducing new risks to the delivery of the project, and escalating those already identified.<sup>109</sup>

According to this analysis, it would seem FiReControl was moving at such a fast pace - a pace set by political considerations - that it was almost inevitably set up to fail.

It would be too simplistic to entirely blame any hurried desires of Ministers, however, as data arising from Parliament illustrates. The response of the Permanent Secretary of the DCLG to a member's suggestion that the then Deputy Prime Minister was 'this out of control bull in a china shop going round telling you what to do' suggests other factors contributed: 'It would be a convenient cop-out to say this was just down to Ministers' enthusiasm.'<sup>110</sup> Whilst they would have only been acting in their advisory capacity, senior civil servants clearly helped to make the case for the original investment decision (even if it has been suggested privately that, later, one official's advice to Ministers to continue with FiReControl was not heeded.<sup>111</sup>)

Other factors influenced the initiation of FiReControl directly; reports commissioned by the Government to a private consultancy actually helped to justify the project. As the Government outlines in the 'Full Business Case' for the project,

---

<sup>108</sup> National Audit Office, 'The failure of the FiReControl project', p.17

<sup>109</sup> *ibid.*

<sup>110</sup> Committee of Public Accounts, 'The failure of the FiReControl project', Ev 20, Q201

<sup>111</sup> Interview, Industry Executive

'...[i]nvestment in Regional Control Centres (RCCs) is consistent with a wide range of departmental and governmental studies, policies and initiatives.'<sup>112</sup> The seemingly pivotal contribution in this respect was a report completed in 2000 (later updated in 2003) by the company; Mott MacDonald. As FiReControl's Business Case specifically states, these documents were relevant to the creation of FiReControl because they '[c]oncluded that vertical integration best meets the requirements of the FRS, and that regional scale fire and rescue emergency control centres would be optimal.'<sup>113</sup> Thus, according to the Government, FiReControl specifically 'Implements the recommendations of the MMD study in England.'<sup>114</sup> From the outset of the project, therefore, the findings of at least one company clearly influenced the shape and direction of FiReControl.<sup>115</sup> Furthermore, the Government made explicit use of the company's recommendations in its 2003 White Paper<sup>116</sup> - recommendations that helped it to justify (if only in its own mind) the FiReControl concept. That the 2003, updated version of Mott MacDonald's report indicated a preference for the initiation of '...a national strategy to reduce the number of fire and rescue service control rooms by means of Fire-Fire amalgamation to form Regional controls matched to the Government Offices for the Regions'<sup>117</sup> - instead of the previous suggestion to reduce control rooms from 49 to 21 as its earlier report recommended<sup>118</sup> - is further evidence of how its findings were translated into policy. In short, at least one company helped to make the case for substantial reforms to the FRS's control room arrangements and, in the process, helped to justify FiReControl.

---

<sup>112</sup> Department for Communities and local Government, 'FiReControl Business Case: Version 1.1', p.58

<sup>113</sup> *ibid.* p.60

<sup>114</sup> *Ibid.*

<sup>115</sup> This is not to suggest that the Mott MacDonald report was the sole justification, or necessarily responsible for the failure of FiReControl.

<sup>116</sup> Office of the Deputy Prime Minister, 'Our Fire and Rescue Service', pp.28-29

<sup>117</sup> Mott MacDonald, 'The Future of Fire and Rescue Service Control Rooms in England and Wales Update 2003 – Full Report', Via:

[http://www.esfrs.org/document/pdf/fa/membersArea/mott\\_mac\\_report.pdf](http://www.esfrs.org/document/pdf/fa/membersArea/mott_mac_report.pdf) (accessed 12.08.13), p. S-4

<sup>118</sup> *ibid.* p. S-1

What role was it envisaged 'industry' more broadly should play in the implementation of FiReControl? The Government clearly intended to use the private sector and this was evident in the case of the largest individual contract associated with the project - the (estimated) £200 million IT contract awarded to EADS in March 2007. As the NAO's reporting on the project has indicated, the programme would include two main acquisition components; firstly, the delivery (and management) of the new accommodation that would be needed for the fire authorities and, secondly, the supporting IT contract itself.<sup>119</sup> Whilst it is clear that through its financing under the Government's 'Private Finance Initiative' the private sector would also be deeply involved in the first set of accommodation arrangements, this section now devotes its attention to the dynamics around the latter, larger single supply contract.

Having issued a 'call for interest' for the IT aspects of FiReControl in the Official Journal of the European Union in May 2004, the DCLG then invited 'three short-listed bidders for best and final offers'<sup>120</sup>, culminating in the appointment of EADS in 2007. The award of a large, CT-related contract to a company traditionally so closely associated with the defence sector might appear to perfectly reflect the criticism that has been levelled towards 'the SIC'; after 9/11, the MIC has transferred into the CT sector. The award and structure of the contract certainly resembled similar defence projects in important respects. Firstly, it was clear that EADS was considered (and considered itself) as the 'prime contractor' for the integration of the IT aspects of the project, and responsible for managing the overall package in much the same way that it would have been familiar with in the defence sector - as the NAO put it; 'EADS has subcontracted the majority of the work to third parties and its main role is to bring these packages together to form the overall

---

<sup>119</sup> The NAO explains how the DCLG 'organised the FiReControl project into three workstreams', listing: 'Accommodation', 'Business change' and 'IT'. National Audit Office, 'FiReControl Project', p.9

<sup>120</sup> As outlined in a 'Timeline of key events' compiled by the NAO in 2010. *ibid.* p.10

solution.<sup>121</sup> This was never going to be a straightforward task, however - the NAO's detailed overview of EADS's responsibilities clarifies that whilst it was an IT project it consisted of many diverse components<sup>122</sup>. Furthermore, it can be suggested that EADS's previous experience in the defence sector led both the company and the Government into believing that it would be more than suitable for the task. Responding to questioning on the effectiveness of the management of the project, for example, one senior fire officer responded<sup>123</sup>:

At the start of the project the contractors and everybody assumed it would not be complicated. They were a big defence contractor and this was only a little old fire service: "How hard can it be?"

It would be 'business as usual' for EADS, apparently, and, like with its experience of handling contracts in the defence sector, the company would manage the contributions of a wider selection of companies to deliver the contract. Hughes usefully highlights the project's diverse supply chain of '...seven subcontractors: Ericsson, Frequentis (UK), Hewlett-Packard, IMass, Innogistic Software Multitone Electronics and Telent'<sup>124</sup> - whilst challenges arising from the make-up of this supply chain would subsequently emerge (most notably Ericsson was replaced with Intergraph in December 2009), the management of such a structure would certainly not have seemed alien to a defence company of EADS's experience.

---

<sup>121</sup> *ibid.* p.13

<sup>122</sup> The project consisted of 'the procurement and installation of IT hardware in nine Regional Control Centres, 46 Fire and Rescue Service headquarters, 1,400 fire stations and 3,400 fire engines (and other equipment).' In addition, '...[a]s well as designing, developing and installing the core resilient IT systems, EADS is required to supply operational support services, including fault repair, maintenance and data-backups until 2015, with an option for a further three-year extension upto [sic] 2018.' *ibid.*

<sup>123</sup> Committee of Public Accounts, 'The failure of the FiReControl project', Ev 19, Q191

<sup>124</sup> Robert T. Hughes, 'Could Agile Development have prevented the FiReControl project failure', UK Academy for Information Systems Conference Proceedings 2012, Via: <http://www.ukais.org.uk/Documents/Downloads/Conference20124c054606-9517-41d3-96d4-b0dd1913f68.pdf> (accessed 12.08.13), p.10

A further similarity exists between FiReControl and other defence contracts; 'rising costs' is a recognised feature of Government defence projects - and literature of the MIC more broadly - and this was certainly a feature of FiReControl. An analysis of factors potentially accounting for rising costs in this case is provided below, suffice to note here that when the project was first approved (in 2004) it was estimated that it would cost £120 million<sup>125</sup>; as we have already seen, the NAO considered that at least £469 million had been wasted by the FiReControl project upon its termination in 2010. Naturally, this invites the question as to whether a 'conspiracy of optimism' may have emerged in the same way that has been identified within the defence sector.<sup>126</sup> Having considered the main features of the contract, and argued that FiReControl resembled similar contracts in the defence sector, we now turn to an examination of how these cost increases may have come about, and what accounted for the failure of the project.

This thesis benefits from the prior completion of several credible studies covering 'why' FiReControl failed so spectacularly; combining the explanations can only lead to the conclusion that any argument seeking to singularly implicate 'the SIC' for the difficulties would be over-simplistic. According to the PAC, FiReControl failed in large part as a result of a *problem of governance*, rather than as a result of any system pursuing its interests; it concluded that '[t]he project was flawed from the outset'<sup>127</sup> and that the DCLG did not possess 'sufficient mandatory powers (...) to impose a single, national approach on locally accountable Fire and Rescue Services who were reluctant to change the way they operated.'<sup>128</sup> Indeed, the operation of this governance system has been described generously as 'convoluted'<sup>129</sup> and was clearly dysfunctional; the data suggests that the

---

<sup>125</sup> National Audit Office, 'The failure of the FiReControl project', p.6

<sup>126</sup> As Gray has argued: 'Simply put, many participants in the procurement system have a vested interest in optimistically mis-estimating the outcome'. Gray, *Review of Acquisition*, p.19

<sup>127</sup> Committee of Public Accounts, 'The failure of the FiReControl project', p.3

<sup>128</sup> Ibid.

<sup>129</sup> Ibid. p.5

Government declined to properly engage with the FRSs who were supposed to be the main beneficiaries or ‘customers’ of the project. As the NAO put it; ‘FiReControl was flawed from the outset because it did not have the support of the majority of those essential to its success – its users’.<sup>130</sup> The PAC agreed, arguing that the Government actually ‘excluded them [the FRS] from decisions about the design of the regional control centres and the proposed IT solution, even though these decisions would leave local services with potential long-term costs and residual liabilities to which they had not agreed.’<sup>131</sup> This is clearly a fundamental design issue that has nothing to do with the fact that companies such as EADS later became involved, irrespective of their own role and effectiveness in the project.

Other factors contributed to the demise of FiReControl. The role of the leading workers’ union in the sector, for example, was seen as detrimental by one former EADS employee; Richard Fletcher suggested that the Fire Brigades Union (FBU) represented an ‘enormous vested interest’ and that it ‘sought to undermine the scheme throughout the lifecycle of the project.’<sup>132</sup> Whatever level of influence the FBU exerted upon the decision to terminate the contract, there is no doubt of its overall position on FiReControl: it publicly called for the project to be cancelled<sup>133</sup> and, following the publication of the NAO report, the organisation’s Secretary-General was quoted as saying that it had acted as ‘the lone voice highlighting soaring costs, incompetence and delays’<sup>134</sup>, lamenting that that ‘no one listened to what the professional firefighters and fire control staff were saying’<sup>135</sup> throughout the process. Whether any influence being exerted by a public sector union

---

<sup>130</sup> National Audit Office, ‘The failure of the FiReControl project’, p.5

<sup>131</sup> Committee of Public Accounts, ‘The failure of the FiReControl project’, p.3

<sup>132</sup> Interview, Richard Fletcher

<sup>133</sup> ‘FBU calls for regional fire centres to be scrapped’, *BBC News*, 6 Oct. 2010, Via: <http://www.bbc.co.uk/news/uk-11478008> (accessed 28.10.13)

<sup>134</sup> Leo King, ‘FireControl failure blasted by Fire Brigades Union’, *Computerworlduk.com*, 1 July 2011, Via: <http://www.computerworlduk.com/news/public-sector/3289170/firecontrol-failure-blasted-by-fire-brigades-union/> (accessed 25.10.13)

<sup>135</sup> *Ibid.*

could be any more preferable than that exerted by corporate entities will fall within the eye of the beholder.

The explanations offered by officials for the decision to cancel FiReControl should also be taken into account; the oral evidence transcripts included within the PAC's 'update report' on the project are particularly illuminating. Within them, DCLG's Permanent Secretary argued:

I think that it is right to say that one of the reasons why the project struggled was that it did not get buy in at the start, and that is what the NAO said, but it was not the reason why we terminated the contract. The reason we terminated it was because we had no confidence that we would get what we were seeking in a reasonable time scale; it is as simple as that.<sup>136</sup>

For the Government, then, it was the problems it was experiencing with its suppliers in delivering the IT elements of the project that was the key issue; at face value, it seems to have been arguing that it was simply EADS's performance that was the true cause of the problem. Whatever difficulties may have existed, however, we should only cautiously accept that this was the *sole* reason for the cancellation; it can be noted, for example, that civil servants have also been blamed for the fiasco.<sup>137</sup> We could even suggest that the Government's emphasis on the failure being a result of its contractor's 'inability to deliver' suspiciously echoes its explanation of the problems associated with the e-Borders IT contract and the inability to provide sufficient numbers of private security officers in time for the London 2012 Olympics (examined in Chapters 4 and 5 respectively).

---

<sup>136</sup> Committee of Public Accounts, 'FiReControl: Update report', Sixteenth Report of Session 2013-14, HC 110, July 2013, Ev 3, p.17

<sup>137</sup> The former deputy Prime Minister, for example, has suggested it was the fault of 'The bloody civil servant who is now in Scotland', arguing: 'When I left office that (FiReControl) was a programme that was going to cost £100m. They confirmed it was on budget. Twelve months after I left it went up to this enormous figure.' Quoted in Daniel Wainwright, 'John Prescott: Don't blame me for Wolverhampton fire control centre fiasco', *The Express & Star*, 11 June 2013, Via: <http://www.expressandstar.com/news/politics/2013/06/11/john-prescott%E2%80%88dont-blame-me-for-wolverhampton-fire-control-centre-fiasco/> (accessed 28.11.13)



What of any validity in this case of a main charge labelled against ‘the SIC’; that ‘cosy relationships’ would have existed around the IT contract and that its rising costs arose directly from the greedy, sinister or, at a minimum, commercially self-interested motivations of the contractor and/or any other parties involved in the project? There is certainly evidence that Government and industry collaborated closely together on the project at various stages, and that on occasion this may have exceeded the limits of what could be considered to be appropriate. For example, the NAO was extremely critical of the project’s ‘over-reliance on poorly managed consultants’<sup>138</sup>, highlighting the findings of an (unpublished) report by the Office of Government Commerce (OGC) that ‘consultants were found to hold a disproportionate (and accountability-free) amount of authority.’<sup>139</sup> It is also striking that during one Parliamentary evidence session the Government and its main contractor, EADS, appeared on the same panel together when providing evidence on the circumstances surrounding the project’s problems.<sup>140</sup> The session leaves the impression of the relationship being (at that stage) a very cordial affair, at least at the most senior level. At one stage, for example, the then Fire Minister, Shahid Malik, sitting alongside the CEO of EADS, summarised:

I am not here to blame EADS. I think they were at fault quite a lot. We have been at fault as well. They are very trusted in government circles, with the multimillion pound projects that they have with government etc.<sup>141</sup>

This appearance of a degree of ‘cosiness’ might hardly be comforting to the UK taxpayer, even if it could also be argued that at the senior level there was a realistic acceptance that there was a degree of interdependency between the public and private sectors in successfully delivering this project.

---

<sup>138</sup> National Audit Office, ‘The failure of the FiReControl project’, p.7

<sup>139</sup> Ibid. p.23

<sup>140</sup> Communities and Local Government Committee, ‘FiReControl’, Fifth Report of Session 2009-10, HC 352, April 2010, Ev 10-20

<sup>141</sup> Ibid. Ev 19

Whatever the shared understanding, it seems that deep tensions begin to emerge between the supplier and ‘end user’ in this case; in its landmark report on the project, the NAO even refers to ‘the *absence of a partnership approach* between EADS and the Fire and Rescue Services’<sup>142</sup>. EADS’s relationship with the Government also appeared increasingly strained, especially after the 2010 General Election. The NAO report identifies, for example, that the DCLG had been critical of EADS’s handling of the contract and that ‘there was an absence of cooperation to resolve the issues.’<sup>143</sup> This is supported by a segment of an interview held with one industry executive on the causes of the Government’s decision to cancel the FiReControl in 2010:

Who is accountable for closing the FiReControl? Bob Neill was the Fire Minister and the reason why he ended it was because the decision to end FiReControl was taken a year earlier, when the Conservatives secured the General Election. And they were ‘anti’ the FiReControl project because it was a Prescott regionalisation project; they disagree with regionalisation. The Fire Service, of course, were happy at any opportunity to remain in their personal fiefdoms. And to secure a cheap political victory at the expense of John Prescott they cancelled this programme.<sup>144</sup>

Whether this explanation can be accepted at face value, there is also evidence that the technical requirements of the IT contract were *over-specified* and that, despite its ultimate cancellation, some companies involved in FiReControl still profited from FiReControl. A PAC report highlights, for example, that the DCLG had informed it that ‘the original contract was significantly over-specified and not appropriate to the needs of the country’<sup>145</sup>, inviting the question as to who was responsible for this situation developing. A closer examination of the oral evidence supporting the PAC’s conclusion does not necessarily confirm the existence of any foul play on the part of any ‘industrial-complex’, however. Instead, the strong suggestion is that FiReControl was designed in alignment with the then Government’s priority of regionalisation. When pressed on this matter in

---

<sup>142</sup> National Audit Office, ‘The failure of the FiReControl project’, p.24 (Emphasis added)

<sup>143</sup> Ibid.

<sup>144</sup> Interview, Industry Executive

<sup>145</sup> Committee of Public Accounts, ‘FiReControl: Update report’, p.8

Parliament, Sir Bob Kerslake clarified why the decision was taken to deliver a large-scale, national programme:

I think it is two things. One is that it was based on a regional model, and the other was that it was, in my view, significantly over-specified for what we required by way of resilience. You didn't require a system where you could, in any part of the country, provide the back-up to another part of the country in that way.<sup>146</sup>

Whether anyone within Government or its main supplier - or indeed any potential combination thereof - sought to over-specify the project is not evident from the available material, and the impression left is one of a chaotic 'muddling through' rather than a conspiracy. In its careful examination into the potential causes of the associated over-specification of the RCCs, for example, the CLG highlights the speed with which the procurement was developed, the lack of consultation around it, and the naivety of some of the Government's assumptions as the main contributory factors, rather than any 'unwarranted influence'. It states:

It could be argued that an over-specified project is preferable to an under-specified project, especially where security is concerned. (...) The lack of consultation and collaboration on the project has resulted in buildings that have been designed without adequate consultation on specifications needed by those that will work in the buildings and by those who have statutory duties under the 2004 Fire and Rescue Services Act.<sup>147</sup>

Factors other than the emergence of a malign confluence of interests have therefore been offered by independent authorities as contributing towards over-specification within FiReControl. If any 'industrial-complex' in the CT sector was in any way responsible for over-engineering the required capabilities that it was determined would be needed, it did well to conceal itself. Indeed, it seems that the CLG would also have had to have been involved in such a 'conspiracy'.

---

<sup>146</sup> Ibid, Ev 2, p.16

<sup>147</sup> Communities and Local Government Committee, 'FiReControl', p.35

It is also clear, however, that over the course of several investigations suggestions were made that inappropriate corporate influence was exerted on FiReControl, and that some companies profited from their involvement unduly. For example, the NAO explains how, following the decision to terminate FiReControl, ‘an amicable termination’ took place between EADS and the DCLG, resulting in a payment of £22.5m to the latter, meaning that ‘the resulting overall net payment to EADS was £11.7m.’<sup>148</sup> It is easy to see how outside observers might consider the character of the termination as being ‘amicable’ as inappropriate at worst, undesirable at best.

Perhaps more concerning was the role played, and the monetary benefit received, by the consultancy companies who were involved in the project. The NAO has explained, for example, that ‘PA Consulting was contracted to provide consultancy services at a cost of £42 million to the end of March 2011’<sup>149</sup>; concerns were also expressed in Parliament about the nature of their involvement. The PAC Chairman observed on the company’s involvement: ‘Those of us who have wandered occasionally into this world would know it is in their interest to keep that consultancy going.’<sup>150</sup> That a less-than-helpful approach was adopted by PA Consulting in respect of FiReControl was also suggested in interviews. One industry executive reflected:

They were incentivised... PA were there to help manage the chaos. It was in their interest for there to be chaos.<sup>151</sup>

Another interviewee developed this further; describing PA’s activities towards the end of the contract as ‘evil’ and alleging that the company was deliberately ‘creating work for themselves’.<sup>152</sup> Whilst these are only two viewpoints, the perception that such influential corporate actors were acting so unhelpfully raises questions about the appropriate scope

---

<sup>148</sup> National Audit Office, ‘The failure of the FiReControl project’, p.32

<sup>149</sup> Ibid., p.23

<sup>150</sup> Committee of Public Accounts, ‘The failure of the FiReControl project’, Ev 7, p.23

<sup>151</sup> Interview, Industry Executive

<sup>152</sup> Interview, Industry Executive

and level of involvement of such companies in Government security contracts. Remarkably, the DCLG's Permanent Secretary stated that the consultants were not merely advisers but in fact 'a key part of the actual delivery team'<sup>153</sup>. The National Project Director for FiReControl, Roger Hargreaves, also publicly reflected on the appropriate boundaries; 'I think we over-relied on consultants.'<sup>154</sup>

For the avoidance of doubt, no evidence has been found that PA Consulting or any other company was responsible for any specific inappropriate (not to mention illegal or corrupt) behaviour. The concluding chapter addresses the appropriateness of companies being involved in security projects; before then, we can safely conclude that even if the available evidence does not suggest that any *specific* untoward influence was exerted upon FiReControl, it was an alarming feature of this case that some companies could secure multi-million pound returns from a public sector security contract that was *not* delivered. Whilst other contracts and strategic interactions with the private sector in the UK emergency preparedness sector have been more successful<sup>155</sup>, there is no doubt that the case of FiReControl was an extremely regrettable episode that exhibited several worrying dynamics.

### ***Private Operators***

The private sector's involvement in resilience is not limited to industry's (non)provision of CT-related contracts; the Government's interactions with private sector *operators* on CT-related emergency preparedness issues is an issue which has greatly risen in prominence since 9/11. Indeed, there is now widespread recognition that much of the UK's critical

---

<sup>153</sup> Committee of Public Accounts, 'The failure of the FiReControl project', Ev 8, p.24

<sup>154</sup> Ibid.

<sup>155</sup> In addition to 'New Dimension', the utilisation of the nation-wide platform underpinning the emergency services' communications systems known as 'Airwave' is amongst the most celebrated. 'The Airwave Service', Airwave Solutions Limited, Via: <https://www.airwavesolutions.co.uk/about/the-service/> (accessed 30.12.14)

infrastructure - 85% according to one reliable source<sup>156</sup> - is actually owned and operated by the private sector, and thus the country's security and resilience depends on corporate entities. To ensure that such companies develop appropriate levels of preparedness around their installations and/or systems, the UK Government's Centre for the Protection of National Infrastructure (CPNI) has identified nine sectors upon which it considers UK daily life depends<sup>157</sup>, establishing mechanisms of engagement around them. Omand has analysed in depth the quality and effectiveness of the public-private mechanisms that have been put in place in the UK context. He highlighted when in Government:

Within each of these sectors a dialogue is now under way with the industry or sector bodies, companies or trade associations to discuss vulnerabilities, resilience, and protective security issues.<sup>158</sup>

Whilst the details of such dialogue are rarely published for security reasons, it is clear that the establishment of such practical fora as 'information exchanges'<sup>159</sup>, as the CPNI calls them, are vital for ensuring security through sustained public-private sector cooperation. The complexity arising from the fact that business considerations are a constant feature of the CT agenda should not be underestimated - indeed, Omand was a pioneer in identifying the need for 'the commercial competitive pressures on the Boardrooms that now control most of our national critical infrastructure'<sup>160</sup> to be taken into account in security policy. It is thus now widely acknowledged that public-private cooperation on CNI protection is thus not only desirable, but essential. Asked for an updated view of the effectiveness of such interaction for this thesis, David Omand was positive about the progress that had been made:

---

<sup>156</sup> Edwards, *Resilient Nation*, pp. 25-26

<sup>157</sup> The nine identified sectors are: communications, emergency services, energy, financial services, food, government, health, transport and water. 'The national infrastructure', Centre for the Protection of National Infrastructure Website, Via: <http://www.cpni.gov.uk/about/cni/> (accessed 01.11.13)

<sup>158</sup> Omand, 'National Resilience Priorities for UK Government'

<sup>159</sup> 'Information Exchanges', Centre for the Protection of National Infrastructure Website, Via: <http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/> (accessed 01.11.13)

<sup>160</sup> Omand, 'National Resilience Priorities for UK Government'

And I think in the UK I'm reasonably upbeat about that (...) I mean there may be practical difficulties and it all takes a long time – in some cases it hasn't yet reached the stage of the regulator having legal responsibilities for security as well as safety – but you can see the direction of travel.<sup>161</sup>

It is clearly apparent that from 9/11 until the present day an enormous amount of practical work of an operational nature has been pursued between the State and companies comprising the nine sectors of the CNI. The aim of this section is not to highlight each and every public-private interaction to be developed under the auspices of this priority - revealing such details would be inappropriate - rather, it serves to highlight the operational responsibilities that the private sector 'owns' in the non-military security context. The noteworthy characteristic here is the direct, operational role that is 'owned' by companies; this starkly contrasts with industry's role within the defence sector. The idea that the MIC has linearly transferred to the CT sector is thus questionable.

The Government has developed a series of other non-contractual interactions of an operational nature with the private sector to strengthen UK emergency preparedness. Perhaps the most prominent amongst these has been the steps taken to engage with the manpower-related or guarding sub-sector of the wider 'security industry'. Should the relevance of this part of the industry to CONTEST be doubted, there has long been recognition of the potential for this substantial resource to help to supplement public sector capability in policing<sup>162</sup>; Gregory also identifies 'The private sector's role as a potential contributor of human resources to the counter-terrorism response'<sup>163</sup>. This certainly reflects the outlook of the UK's most senior security authorities; a former UK Government Minister for Security, for example, explained to a luncheon of the British Security Industry Association (BSIA) trade association:

---

<sup>161</sup> Interview, David Omand

<sup>162</sup> White observes that 'private security officers outnumber police officers in most industrial countries', White, *The Politics of Private Security*, p.3

<sup>163</sup> Gregory, 'Private sector roles in counter-terrorism', pp.325-6

Because there is no doubt whatsoever in my mind - if we are to excise this cancer of violent extremism, everyone, all of us in the UK, have to work together. And that means involving industry fully, involving our scientists, involving technology, involving all our people actually.<sup>164</sup>

Interestingly, the Minister also thanked the BSIA during the course of his speech for developing its own document, *CONTEST and the Private Security Industry*, which enables its member companies to demonstrate their support for the strategy.<sup>165</sup> This Ministerial desire and endorsement for close cooperation with this part of the private sector has increasingly permeated both industry's and the Home Office's outlook, with specific initiatives developed with this attitude in mind. One interviewee recalled, for example, that during Lord West's tenure at the Home Office, the OSCT organised an 'industry day' at the Emmanuel Centre opposite the Department's headquarters in Marsham Street, designed to be open to the 200,000 members of the manpower-orientated part of the sector.<sup>166</sup>

Finally, any full discussion on the private sector's increasing operational involvement in UK emergency preparedness should note that growing attention - both policy and scholarly - is being paid to the question of how the public and private sectors interact on cyber-related 'resilience' issues. A recent, thought-provoking examination of this important issue was included within a pioneering article by Herrington and Aldrich, and it can be hoped that it provokes further discussion. The article's recognition that 'growing public-private partnerships' in this sector are making the governance of cyber

---

<sup>164</sup> 'Part 2 of 3 - Admiral the Lord West of Spithead speaking at The BSIA Annual Lunch 2009', BSIA YouTube Channel, Uploaded on Aug 11, 2009, Via: <http://www.youtube.com/watch?v=Qd9gmhSdA6w> (accessed 15.11.13)

<sup>165</sup> 'Part 1 of 3 Admiral the Lord West of Spithead speaking at The BSIA Annual Lunch 2009', BSIA YouTube Channel, Uploaded on Aug 11, 2009, Via: <http://www.youtube.com/watch?v=43RBKV6w2IQ> (accessed 15.11.13). The 'Publications' page on the BSIA's website states that its document *CONTEST and the private security industry* 'is only available to BSIA members', Via: <http://www.bsia.co.uk/publications.php?r=NQ4W5W616041> (accessed 15.11.13)

<sup>166</sup> Interview, Industry Executive



security 'more complex'<sup>167</sup> is worthy of profound reflection, as is their argument - closely connected to the themes explored in this thesis - around who might be to blame if (when?) disaster strikes in the context of greater private sector involvement in security matters:

When the digital tsunami occurs, citizens will hold government to account for the failure of an infrastructure they no longer own and control – and which ministers do not fully understand.<sup>168</sup>

This assertion should provoke deep questions of policymakers regarding the desirability, inevitability and consequences of private entities now possessing operational 'national security' responsibilities. Whatever assessments are made in response to such soul-searching, the end result is clear; the private sector's operational involvement in UK emergency preparedness is undeniably extensive.

### ***Wider Business***

In addition to the supply and operational interactions analysed above, it is evident that, even before 9/11, the UK Government increasingly sought to involve the wider business community in achieving stronger UK emergency preparedness against the backdrop of terrorism; whether through guidance or other new mechanisms of engagement. For example, the Home Office's Communications Department's 1999 guidance document titled *Business as Usual: Maximising business resilience to terrorist bombings*<sup>169</sup> outlined the following 'purpose': '...to show what can be done to help businesses affected by major terrorist bombings in urban areas recover as quickly and effectively as possible.'<sup>170</sup> This was not an isolated initiative; a separate booklet titled *How Resilient is your Business to*

---

<sup>167</sup> Herrington and Aldrich, 'The Future of Cyber-Resilience', p.302

<sup>168</sup> Ibid. p.303

<sup>169</sup> Home Office, *Business as Usual: Maximising business resilience to terrorist bombings, A Handbook for Managers*, Home Office Communications Directorate, February 1999, Via: <http://www.nationalarchives.gov.uk/ERORecords/HO/421/2/P2/oicd/business.pdf> (accessed 01.08.13)

<sup>170</sup> Ibid. p.4

*Disaster*<sup>171</sup> was first developed in the mid-1990s by the Home Office in collaboration with the Confederation of British Industry (CBI). The Foreword of its first published version - co-signed by the then Home Secretary and the Director General of the CBI - stated that the guidelines contained within it 'apply equally to the public or private sector' and that, notably; 'Big or small, private or public sector, the message is the same for all organisations.'<sup>172</sup>

This emphasis on encouraging the private sector to take responsibility for its own preparedness increased rapidly after 9/11. Amongst some of the most important recent initiatives have been the 'tools' that have been produced and disseminated by the CPNI and the National Counter Terrorism Police Office (NaCTSO); indeed, both organisations have seen 'working with the private sector' as a core (if not fundamental) aspect of their remits. In the case of the CPNI, Herrington and Aldrich neatly summarise (albeit in a 'cyber' context) that '[j]ust like everyone else it cannot superintend the UK infrastructure but it does enjoy close relationships with the backbone providers'<sup>173</sup>. Regarding NaCTSO, the former head of the organisation has articulated the attitude of the organisation; outlining the importance that he considers business must play in its own protection, and the projects that were established by the organisation under his leadership (such as 'Project ARGUS' and a 'Vulnerability Self-Assessment Tool') to help them to do so.<sup>174</sup> In addition, both organisations have in recent years produced a substantial suite of written guidance material designed either for specific sectors or more general application. NaCTSO's website explains that each of its guides - these range from the protection of stadia to hotels and

---

<sup>171</sup> Home Office, *How Resilient is your Business to Disaster*, Home Office Communications Directorate, 1998, Via: <http://www.nationalarchives.gov.uk/ERORecords/HO/421/2/P2/EPD/hrib.txt> (accessed 01.08.13)

<sup>172</sup> Ibid.

<sup>173</sup> Herrington and Aldrich, 'The Future of Cyber-Resilience', p.302

<sup>174</sup> Chris Phillips, 'Why we need Counter Terrorism', *Professional Security Magazine*, 5 June 2013, Via: <http://www.professionalsecurity.co.uk/news/interviews/why-we-need-counter-terrorism/> (accessed 15.11.13)

restaurants - 'provides protective security advice to those who own, operate, manage or work in environments that are vulnerable to acts of terrorism.'<sup>175</sup>

Additional dimensions of 'wider business' public-private interaction on CT-related emergency preparedness issues have been identified. Gregory's chapter on this subject is the most comprehensive to date; indeed, he was the first to properly recognise the 'wide spectrum of roles'<sup>176</sup> now conducted by the private sector in this aspect of CT and, perhaps even more importantly, the crucial point that 'these public-private sector relationships are both complex and diverse in character'<sup>177</sup>. For the present purposes, we can recall his analysis of two particularly innovative public-private interactions; firstly, the way in which after 9/11 individual police forces' Counter Terrorism Security Advisers (CTSAs) were increasingly required 'to reach out to the wider business and industrial environment'<sup>178</sup> and, secondly, the development of 'Project Unicorn'. This latter scheme was devised by the MPS to 'address the question of how the private sector could help the police.'<sup>179</sup> According to Gregory, the project 'reflected upon what kind of 'drivers' might help to shape a deeper partnership between the wider business community and government agencies'<sup>180</sup>.

Whilst this chapter has been concerned with examining the Government's interactions with *corporate, profit-making entities* within the CT space, as seen above, the importance of the potential role played by private citizens and non-profitmaking organisations in relation to UK emergency preparedness should not be overlooked; some might even consider them part of what is considered the 'private sector'. Certainly, the UK Government has regularly seen value in communicating directly to the public in this area after 9/11; its decision in 2004 to issue a 'preparing for emergencies' booklet to every

---

<sup>175</sup> 'Publications', NaCTSO Website, Via: <http://www.nactso.gov.uk/publications> (accessed 15.11.13)

<sup>176</sup> Gregory, 'Private sector roles in counter-terrorism', p.321

<sup>177</sup> Ibid. p.322

<sup>178</sup> Ibid. p.324

<sup>179</sup> Ibid. pp.325-327

<sup>180</sup> Ibid. p.326

household in the country<sup>181</sup> serves as an excellent (if not slightly ridiculed) example, as does its more recent work with other external organisations to publish a ‘Business Continuity for Dummies’ guide for small and medium-sized businesses.<sup>182</sup>

Perhaps more importantly, there has been a growing appreciation that ‘community resilience’ should be an essential part of the response; the Cabinet Office has developed a significant programme of work around this policy and its website helpfully clarifies its understanding of the concept: ‘Community Resilience is about communities using local resources and knowledge to help themselves during an emergency in a way that complements the local emergency services.’<sup>183</sup> In addition to the Government placing an emphasis on encouraging communities to ‘help themselves’ in responding to emergencies, it equally recognises the role that non-governmental organisations and charities can play in supporting them. For Edwards, the voluntary sector is a particularly important player as it plays ‘four distinct roles’ in supporting the authorities with emergency preparedness: ‘communications, search and rescue, social and psychological aftercare, and welfare and medical support.’<sup>184</sup> Whilst outside the scope of this thesis, there could be benefit in examining the role and influence that such actors may exert within, and upon, the UK’s national security strategy (or any of its component parts).

### **3.4 Character and impact of the ‘industrial-complex’ in Emergency Preparedness**

This chapter has not sought to examine the dynamics around *all* of the contracts or public-private interactions that have emerged in the UK’s emergency preparedness landscape. It

---

<sup>181</sup> ‘Terror advice pamphlet unveiled’, *BBC News*, 26 July 2004, Via:

[http://news.bbc.co.uk/2/hi/uk\\_news/politics/3923949.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/3923949.stm) (accessed 16.11.13)

<sup>182</sup> HM Government, CONTEST: The United Kingdom’s Strategy for Countering Terrorism - Annual Report (CM 8583). Via:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/170644/28307\\_CM\\_8583\\_v0\\_20.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170644/28307_CM_8583_v0_20.pdf) (accessed 16.11.13), p.31

<sup>183</sup> Cabinet Office, ‘Resilience in society: infrastructure, communities and businesses’, Via:

<https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses> (accessed 16.11.13)

<sup>184</sup> Edwards, *Resilient Nation*, p.52

has, however, clearly illustrated the extensiveness, breadth and variety of private sector involvement in this area of CONTEST since 9/11. It proved the involvement of suppliers, operators and wider business sectors in this space - and showed that the Government and its agencies have actively sought to engage these communities. The second section of the chapter illustrated how substantial additional investment (over £1bn) was allocated to UK emergency preparedness after 9/11 in accordance with the theory under examination.

For the reasons explained in Chapter 1, the chapter examined in particular the public-private dynamics which emerged around a large, non-military, CT-related UK security contract; FiReControl. Prior to its cancellation, this IT contract was shown to have been operated by a traditional defence company, EADS, and to have suffered from many of the same problems (such as rising costs and over-specification) that have traditionally been associated with high profile acquisition failures in the military sector; and the MIC more generally. Furthermore, the analysis revealed the significant involvement of other profit-making commercial consultancies - in particular Mott MacDonald and PA consultancy - who received substantial remuneration despite the failure of the project. All these insights suggest that the suppliers' community traditionally associated with the MIC has transferred into the non-military, CT-related emergency preparedness aspects of the UK national security.

Any idea that any untoward dynamics arising from an SIC (such as threat inflation or over-specification) may have operated in the context of this specific contract is, however, less clear. Whilst it has been shown that the prime contractor for the IT contract, EADS, ultimately received a net profit of £11.7m<sup>185</sup> for its involvement in FiReControl, there is no doubt that, from a financial perspective, the company would have benefited more significantly had the project not been cancelled. The question of why the Government

---

<sup>185</sup> Footnote 148

chose to cancel the scheme, if it was somehow in a 'cosy alliance' with the company, also arises. The causes of the failure have been extensively scrutinized and several official reviews have provided *multiple* credible explanations for the failure. None of these has suggested that an SIC along the lines presented by critics was accountable; the main failure of FiReControl has been repeatedly identified as a failure of engagement between the Government and the Fire Services.

Perhaps more worrying, however, is the finding that one of the consultancy companies most deeply involved in the project, PA Consulting, generated substantial profits from its participation in the failed project. Worse still, it is doubtful whether the level of the company's involvement was scoped, discharged or overseen appropriately. The longer-term adverse reputational damage that PA Consulting may have suffered as a result of the national media coverage following the project's cancellation does not necessarily mean that its level of involvement in and impact upon the project should not have been a matter for concern. This conclusion resonates worryingly with O'Reilly's assertion that something we might call 'state-corporate symbiosis'<sup>186</sup> has arisen in areas of what he calls the 'transnational security consultancy industry'; the potential consequences of this level of involvement are revisited in the final chapter.

Notwithstanding this worrying suggestion, on the basis of the available evidence - including detailed evidence provided to Parliament and interviews conducted for this study - it cannot be concluded that an organised conspiracy along the lines suggested by critics was evident in either the case of FiReControl, or the UK's emergency preparedness sector more broadly; the former project appears to have been much more disorganised, rushed and ill-thought through than could validate such a theory. Any suggestion that the vested interests arising from something resembling an 'SIC' system were the sole or primary

---

<sup>186</sup> Conor O'Reilly, 'The transnational security consultancy industry: A case of state-corporate symbiosis', *Theoretical Criminology*, Vol. 14:2 (2010), pp.183-210

reason for the growth in the level of funding for FiReControl's IT contract - and indeed that any such dynamics were the sole cause for the overall project failure - are cautiously rejected as a result of the multiple additional explanations that can be, and have been offered to explain what might rightly be described as 'yet another fiasco'.

Finally, the latter sections of the chapter revealed a wide range of additional public-private interactions existing within the 'operational' and 'wider business' categories proposed within this thesis. The diversity of these roles stands in stark contrast to how 'industry' has been traditionally involved in the defence sector - and indeed how it has been conceptualised as a singular corner of the MIC - thus questioning the suitability of casually applying 'the SIC' to the CT sector.

## Chapter 4: Border Security

### Introduction

CT objectives have featured prominently within the UK's Government's border security strategy since 9/11. The first published version of CONTEST, for example, immediately identifies the following priority as one of the 'range of issues' of utmost importance:

Strengthening border security - so that terrorists and those who inspire them can be prevented from travelling here and we can get better intelligence about suspects who travel, including improving our identity management, for example by use of biometrics[.]<sup>1</sup>

This focus has regularly featured in CONTEST subsequently; the document's March 2009 iteration clarifies that '[p]rotecting our borders has been a key part of this workstream'<sup>2</sup> and, when considering 'future challenges', states that 'The UK border will remain critical to our security.'<sup>3</sup> In addition to introducing enhanced arrangements for physical security and policing at the border, the Government has prioritized the use of new technology such as biometrics and enhanced radiological detection capabilities to enhance UK border security. As Section 4.2 outlines, significant levels of new financial investment have been allocated in this sector. Border security, like other areas of contemporary national security strategy, warrants further scrutiny.

This chapter is not the first analysis of companies' involvement in border security; the desirability of its role in developing technological solutions in this sector has previously been questioned within the academic community. According to Amoore, for example, the use of algorithms for border control and other applications 'produces a screened geography of suspicion'<sup>4</sup> and 'the feigned impression of an open world[.]'<sup>5</sup> In a critical

---

<sup>1</sup> HM Government, 'Countering International Terrorism: The United Kingdom's Strategy', p.2

<sup>2</sup> HM Government, 'Pursue Prevent Protect Prepare: The United Kingdom's Strategy for Countering International Terrorism', p.104

<sup>3</sup> Ibid. p.117

<sup>4</sup> Louise Amoore, 'Algorithmic War: Everyday Geographies of the War on Terror', *Antipode*, Vol:41:1 (2009), p.52

<sup>5</sup> Ibid. p.63



article of the 'homeland securitization of the war on terror'<sup>6</sup>, the trend towards the increasing use of military capabilities in the border security sector is not viewed positively:

Here we see the targeting of markets and neighbourhoods by military hardware segueing into the targeting of people at border crossings and in the spaces of the airport.<sup>7</sup>

Journalistic coverage has been even more critical. In support of his damning thesis on the emergence of the SIC, Hughes has identified the role that the US-owned company Raytheon has played in the UK Government's border security strategy through the e-borders scheme analysed in this chapter. For him, it is highly undesirable that the company 'worked hard to build more business in the "war on terror"'<sup>8</sup> after 9/11; he attacks the Government for 'being ready to be wooed by Raytheon, ignoring its murky past.'<sup>9</sup> In border security, as in other areas of CT after 9/11, the so-called SIC is characterized by 'a mixture of the sinister and the incompetent.'<sup>10</sup>

If criticism has been directed towards security suppliers' allegedly detrimental impact on the UK's border security strategy after 9/11, the wider private sector's involvement in this sector has surprisingly not attracted much scrutiny. Whilst Gregory's major 2009 paper on UK border security recognises the 'major role in border controls'<sup>11</sup> played by private operators within the transport sector (such as airports and airlines), for example, even his analysis on this aspect is limited to only a few paragraphs, and not in any depth around whether an SIC-type system has emerged; it is perhaps symptomatic of the fact that the business aspects of security are often presented as a secondary matter that a scholar who has covered the importance of the private sector's contribution to CT

---

<sup>6</sup> Ibid. p.49

<sup>7</sup> Ibid. p.63

<sup>8</sup> Hughes, 'Shining A Light On Raytheon'

<sup>9</sup> Ibid.

<sup>10</sup> Ibid.

<sup>11</sup> Frank Gregory, 'UK Border Security: Issues, systems and recent reforms', A submission to the ippr Commission on National Security for the 21<sup>st</sup> Century, 20 March 2009, Via: <http://www.ippr.org/publications/55/1680/uk-border-security-issues-systems-and-recent-reforms> (accessed 20.01.14), p.5

elsewhere<sup>12</sup> declines to elaborate on this matter. Prior to this chapter, there has been a lack of research on the private sector's involvement in contemporary UK border security.

This chapter shows through its examination into the UK's 'e-Borders' (i.e. 'electronic borders') programme that the public-private interactions that exist around the UK's border security strategy include, but are not limited to, those relating to the suppliers of technological or manpower-related capabilities. Border security, like other sub-sectors of CT, exhibits a multitude of public-private dynamics, the combination of which demand further analysis and scrutiny. Before examining the origins, characteristics and consequences of these relationships in more detail, the chapter introduces the policy and governance context for post-9/11 UK border security.

#### **4.1 Government policy approach and government arrangements**

Like the policy and governance arrangements presented in the previous chapter, the development of (and reform to) the UK's border security arrangements after 9/11 were characterized by considerable complexity and significant change. Whilst this thesis is not concerned with any deeper causal factors for such changes outside its main focus on 'the SIC', it is important to briefly outline the broader context for the inquiry into how the private sector is involved in border security.

Perhaps contrary to some perceptions, the Government's aim to improve UK border security after 9/11 was *not* solely justified upon the basis of CT, as its policy documentation at the time (and coverage of it) makes clear. Makarenko has examined the connections made between asylum, immigration and security in the Government's 2002 White Paper, *Secure Borders*, and the 'unprecedented debates' that were emerging more widely around them; her analysis shows that, in addition to CT, the UK's emerging border security strategy was also concerned with 'reducing illegal people-trafficking' and 'to

---

<sup>12</sup> See Gregory, 'Private sector roles in counter-terrorism'.

prevent war criminals from entering the UK'.<sup>13</sup> Furthermore, the Government's five year strategy published in 2005, *Controlling our Borders*, addresses how it intended to ensure 'secure borders' from the perspective of managing *asylum and immigration*, as the document's subheading makes clear.<sup>14</sup> Even where the document addresses 'harder' security issues, it is as much concerned with 'tackling organised crime', for example, as it is with terrorism. Indeed, the strategy clearly recognises the multi-faceted character of how border control would be managed; it expresses a clear desire 'to implement a fully integrated control'<sup>15</sup>.

It can be argued that as a result of 7/7 and the subsequent change in Home Secretary (from Charles Clarke to John Reid in May 2006), the Immigration and Nationality Directorate's (IND) new White Paper of July 2006 placed a much greater emphasis on CT. That being said, the multi-dimensional character of what the Government sought to achieve through this border security strategy continued to be stressed; the Foreword to the document stated the rationale for the Government's planned reforms to UK border management:

Above all, we need a system which protects the security of this country, prevents abuse of our laws, is fair to lawful migrants and the British public, and in which people have confidence.<sup>16</sup>

Examining the extent to which the Government's multiple strategic objectives for border security helped or hindered its efforts to achieve its reforms is less important at this stage than recognizing how its overall approach for border security after 9/11 became both

---

<sup>13</sup> Tamara Makarenko, 'Immigration and asylum issues' in Wilkinson (Ed.), *Homeland Security in the UK*, pp.251-252

<sup>14</sup> HM Government, 'Controlling our borders: Making migration work for Britain', Five year strategy for asylum and immigration, Cm 6472, February 2005.

<sup>15</sup> *Ibid.*, p.25

<sup>16</sup> Home Office, 'Fair, effective, transparent and trusted: Rebuilding confidence in our immigration system', Ref: 275921, July 2006, Via: <http://webarchive.nationalarchives.gov.uk/20080806121433/http://www.ukba.homeoffice.gov.uk/si/tecontent/documents/aboutus/reports/indreview/indreview.pdf?view=Binary> (accessed 22.01.14), p.2

*broad in scope* and connected to a *wide range of contentious political issues*. Like other sub-sectors of UK national security strategy, border security is characterized by complexity and relates to multiple policy objectives.

If it would be wrong to characterize the Government's emerging border security policy agenda as being *solely* concerned with CT, it would equally be misguided to deny the prominence with which it became a major driver for some of the UK's border security reforms and projects after 9/11. At the legislative level, for example, a wide range of new domestic and European Union (EU) measures relating to cross-border transportation activity would be developed; controversial new international agreements were signed between the US and the EU, for example, on sharing passenger data information prior to travel.

To deliver operational security objectives, some new technology-based border security programmes were initiated by the UK Government and reflect the growing emphasis on CT. For example, the creation of 'Programme Cyclamen' - a scheme introduced in 2002 'to deter or detect the illicit importation of radiological materials into the UK that could be used for terrorist purposes'<sup>17</sup> - was developed within the bounds of CONTEST. Similarly, whilst it boasted application to wider priorities including immigration and efforts to tackle organised crime, the introduction of the UK's e-Borders programme was (as shown below) mainly justified and developed on CT grounds. By contrast, some new border security programmes after 9/11 had nothing whatsoever to do with CT; it would be a stretch, for example, to claim that the introduction of a 'points based system' to manage the influx of skilled economic migrants was CT-related. The idea that the introduction of a proposed National Identity Card could ever be genuinely considered as a 'border security' measure - a proposal that nevertheless at one stage was explicitly

---

<sup>17</sup> 'Pursue, Prevent, Protect, Prepare', p.129

connected to the UK's border security arrangements<sup>18</sup> - should also be treated with caution; the flexibility with which the Government sought to justify the scheme has already rightly been considered with scepticism.<sup>19</sup>

Whatever exact proportion of the UK's post-9/11 border security initiatives were CT-focused, an important point for this thesis is that much of the additional 'border security' investment after 9/11 - investment which would underpin the involvement of private security suppliers and other corporate entities - was primarily driven, and specifically justified by, the 'new' terrorism context. As this study seeks to cast new light on the origins, characteristics and the consequences of the private sector's involvement in CT, the private sector's involvement in post-9/11 UK border security is long overdue for further examination.

If the UK's border security policy priorities were extremely varied after 9/11, the character of the governance arrangements established to oversee them reflected the complexity in two main respects. Firstly, as micro-level examination of the e-Borders programme below shows, it is apparent that, like other sub-sectors of CT, the UK's strategy for border security involves a multitude of both public and private sector entities. Regarding the first category, the Cabinet Office's 2007 Review into the UK's border arrangements is particularly revealing of the large number of 'relevant government organisations' that are involved; this includes (amongst others) the Border and Immigration Agency, UKVisas, HM Revenue and Customs, and the Police.<sup>20</sup> Secondly, whilst

---

<sup>18</sup> One document stated that 'Identity management and ID cards will remain one of the essential components in the management of migration.' Home Office, 'Fair, effective, transparent and trusted', p.8

<sup>19</sup> Kampfner argues that 'Ministers adapted their arguments to suit the moment' when seeking to justify the introduction of ID cards in the UK. John Kampfner, *Freedom For Sale* (New York: Basic Books, 2010), p.207

<sup>20</sup> Cabinet Office, 'Security in a Global Hub: Establishing the UK's new border arrangements', Ref: 284440/1107, November 2007, Via: <http://webarchive.nationalarchives.gov.uk/20071204130052/http://cabinetoffice.gov.uk/upload/as>

the Home Office consistently 'owned' the overall policy lead in Government for border security after 9/11, like with 'emergency preparedness' there were also several important machinery of Government changes in this sector. The purpose of this section is not to examine these at length, but to highlight the level of flux in the system that provides essential context for analysis of the public-private dynamics therein.

Most notable amongst the *policy-level* governance changes during this period were the transition of the Home Office's IND into a new Border and Immigration Agency (BIA) in 2007; the merger of the BIA and UKVisas into a single UK Border Agency (UKBA) in 2008; and, most recently, the split of the UKBA into 'two separate operational units' (UK Visas and Immigration, and Immigration Enforcement) in April 2013.<sup>21</sup> Furthermore, new *operational* border security structures were also introduced to implement the Government's new projects in this sector; the creation in January 2005 of the 'Joint Border Operations Centre' at Heathrow Airport to implement the pilot project for the e-Borders programme - the predecessor agency of the 'National Border Targeting Centre' organization that was itself only opened in March 2010<sup>22</sup> - was amongst the most substantial of these. Alongside these major, border security-specific governance changes, the dispersal after the 2010 General Election of the responsibilities of the UK's Transportation Security and Contingencies Directorate known as 'TRANSEC' within the Department of Transport - both within the DFT and outside to the Civil Aviation Authority - was another major change. In short, whilst the volume of reform being made to UK border security was perhaps unsurprising in view of the highly politicized nature of this sector, the

---

[sets/www.cabinetoffice.gov.uk/publications/reports/border\\_review.pdf](https://www.cabinetoffice.gov.uk/publications/reports/border_review.pdf) (accessed 24.01.14), pp.31-37

<sup>21</sup> 'Our Organisation', UK Border Agency Website, Via: <http://www.bia.homeoffice.gov.uk/aboutus/organisation/> (accessed 24.01.14)

<sup>22</sup> 'Government ramps up passenger screening', Home Office Press Release, 12 March 2010, Via: <http://tna.europarchive.org/20100419081706/press.homeoffice.gov.uk/press-releases/government-passenger-screening.html> (accessed 04.02.14)

governance of UK border security policy in the decade after 7/7 was characterized less by consolidation than change.

One aspect of the Government's border security approach has remained fairly consistent, however; its attitude towards working with the private sector to implement its objectives. At the policy level, there has been constant recognition, across political parties, of the need to cooperate closely with industry in this area. For example, the Foreword to the (then) New Labour Government's border security strategy document, *Securing the UK Border*, could not have been clearer that the approach 'requires co-ordinated support of government, international partners and industry to succeed.'<sup>23</sup> Furthermore, whilst as this chapter shows the coalition Government elected in 2010 would take a quite different approach towards its suppliers, it also arguably equally looked upon 'working with the private sector' as an indispensable part of the strategy. As the Conservative Minister for Immigration outlined in March 2012, for example:

Over the coming years we will work hard with European partners, carriers and trade groups to further extend e-borders coverage to provide a genuinely secure, fluid and complete e-border for the United Kingdom.<sup>24</sup>

The need to involve the private sector in UK border security after 9/11 thus appears to have received a cross-party consensus, reflecting Gregory's important (if not rather generalized) observation that border security 'involves a mix of individual, public sector and private sector responsibilities.'<sup>25</sup> As in the other sub-sectors of CONTEST, therefore, the governance arrangements for post-9/11 UK border security management have incorporated a diverse range of public-private interactions, at multiple levels. Analysis of

---

<sup>23</sup> Home Office, 'Securing the UK Border: Our vision and strategy for the future', Ref. 280648, March 2007, Via: [http://dematerialisedid.com/pdfs/Securing\\_the\\_UK\\_Border\\_final.pdf](http://dematerialisedid.com/pdfs/Securing_the_UK_Border_final.pdf) (accessed 04.12.14)

<sup>24</sup> Damian Green, 'Keynote Speech: Damian Green MP', Royal United Services Institute, London, 14 March 2012, Via: [http://www.rusi.org/events/ref:E4EE5DAE74B90C/info:public/infoID:E4F60AD5049495/#.UvDfEfl\\_vD8](http://www.rusi.org/events/ref:E4EE5DAE74B90C/info:public/infoID:E4F60AD5049495/#.UvDfEfl_vD8) (accessed 14.02.14)

<sup>25</sup> Gregory, 'UK Border Security', p.3

the origins and characteristics of such extensive corporate involvement is offered below; before then, an indication of expenditure in this sector is provided.

#### **4.2 Security Expenditure**

The frequency of the Governmental re-organizations indicated above presents challenges for measuring expenditure levels in 'border security' accurately; material contained within official documents nevertheless suggests that UK border security spending grew significantly after 9/11. Whilst no single, comprehensive or even consistent source of data covering a breakdown of *all* contemporary border security spending is available, this section illustrates both that a greater level of resources was allocated to UK border management throughout the 2000s, and that much of the 'spike' in additional *overall* CT spending after 9/11 can actually be attributed to this sector.

To re-cap on the overall, direct impact of 9/11 on UK CT spending, the Government's 2004 'pre-budget report' states the change in priorities:

Since 11 September 2001, the Government has given increased priority to improving the UK's ability to respond to the terrorist threat. In total, annual spending on counterterrorism and resilience across departments will be over £2 billion in 2007-08, compared with £1.5 billion in 2004-05 and less than £1 billion before 11 September 2001.<sup>26</sup>

Whilst for operational reasons the *exact* breakdown of any funding devoted to border security initiatives after 9/11 may never be published, separate figures indicate how additional resources were allocated to border security. The full business case for the e-borders project includes a number of pertinent figures as it explains the economic impact of 9/11 and 7/7, for example; the document explains that the aviation security measures

---

<sup>26</sup> HM Treasury, 'Pre-Budget Report 2004 - Opportunity for all: The strength to take the long-term decisions for Britain', Cm 6408, 2 December 2004, Via: [http://webarchive.nationalarchives.gov.uk/20100407164511/http://www.hm-treasury.gov.uk/d/pbr04\\_chap06\\_256.pdf](http://webarchive.nationalarchives.gov.uk/20100407164511/http://www.hm-treasury.gov.uk/d/pbr04_chap06_256.pdf) (accessed 05.02.14), p.120



which followed the attack had been estimated at costing 'upwards of \$41bn'<sup>27</sup> and that, in the UK, changes in the airport security regime 'required the airport operator BAA to invest £7m in additional X-ray machines and metal detectors and to employ an additional 500 security staff at an annual cost of £16m.'<sup>28</sup>

Reinforcing the upward trajectory of these figures, a speech delivered by the author in 2009 provides a useful indication of the rising cost of aviation security measures after 9/11.<sup>29</sup> It outlines how one airline operator, Virgin Atlantic, stated in response to a Parliamentary inquiry on transport security that following 9/11 European airlines and airports were paying out '€3 billion for additional anti-terrorist security measures imposed by EU governments'<sup>30</sup>. British Airways also stated in a written memorandum for the same inquiry that it was spending in excess of £100 million per annum on aviation security provision.<sup>31</sup> The author also noted the following statistic:

The European Commission recently quoted ACI-Europe figures which suggest that security costs now represent up to 35% of overall airport operating costs instead of 5% to 8% prior to the events of September 2001.<sup>32</sup>

Whilst these figures are obviously not comprehensive, they clearly illustrate the 'direction of travel' in the absence of available or comprehensive official statistics.

---

<sup>27</sup> Home Office, Border & Immigration Agency, 'e-Borders – Full Business Case, V1.0', 12 November 2007, Via: [http://data.parliament.uk/DepositedPapers/Files/DEP2013-1847/20071112\\_FBC\\_v1\\_0\\_doc1\\_agreed\\_redactions.docx](http://data.parliament.uk/DepositedPapers/Files/DEP2013-1847/20071112_FBC_v1_0_doc1_agreed_redactions.docx) (accessed 04.02.14), p.51

<sup>28</sup> Ibid., p.52

<sup>29</sup> Hugo Rosemont, 'Operating a Tighter Ship in 2009', Speech to TRANSEC Annual Security Conference, Via: [http://www.assa-int.org/\\_Uploads/dbsAttachedFiles/Day1-Operatingatightershipin2009-HugoRosemont.pdf](http://www.assa-int.org/_Uploads/dbsAttachedFiles/Day1-Operatingatightershipin2009-HugoRosemont.pdf) (accessed 26.02.14)

<sup>30</sup> Transport Committee, 'Transport Security: Travelling without Fear', Oral and written evidence, HC 191, 12 December 2007, Via: <http://www.publications.parliament.uk/pa/cm200708/cmselect/cmtran/191/191.pdf> (accessed 26.2.14), Ev. 105-6

<sup>31</sup> Ibid. Ev.11

<sup>32</sup> Rosemont, 'Operating a Tighter Ship in 2009', p.5 This statistic appears in other EU publications including a short 'Working Document' completed by Jörg Leichtfried for the Transport Committee at the European Parliament. European Parliament, Committee on Transport and Tourism, 'Working Document on aviation security charges', DT\793269EN.doc, 20 October 2009, Via: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONGML%2BCOMPARL%2BPE-430.335%2B01%2BDOC%2BPDF%2BV0%2F%2FEN> (accessed 26.02.14), p.2

There is further evidence that post-9/11 UK Government spending on border management grew considerably; statistics on spending prior to 9/11 were made available in a 2001 report of the Parliamentary Home Affairs Select Committee (HASC) on 'Border Control'. Located in the seventh annex of the document, the Government provided a breakdown of the funding that was allocated towards the UK Immigration Service (the operational arm of the then IND); this remained fairly consistent at between £86.1m and £99.65m in 1995-96 and 1999-00 respectively.<sup>33</sup> In its 2005 report on the management of the UK's Asylum Process, by contrast, the NAO outlined the 2003-04 budget of the IND, stating that 'the Directorate spent £1.89 billion on its immigration and nationality operations' in that year.<sup>34</sup> By 2008-09 the annual budget of the (now renamed) UK Border Agency had grown to an even more striking £2.44bn.<sup>35</sup> Expenditure on border security would only seem to begin to subside in real terms following the 2010 General Election; this reflected the coalition Government's priority of reducing the public sector deficit, from which the Home Office would not be exempt. The UKBA's most recent business plan explained that it 'will be reducing the cost to the taxpayer (...) by up to 23 per cent over the next four years.'<sup>36</sup>

A substantial proportion of the rising costs associated with border security is accounted for by the larger number of public officials employed to work on border and immigration, but several high profile border security projects also accounted for the

---

<sup>33</sup> Home Affairs Select Committee, 'Border Controls: Minutes of Evidence and Appendices', HC 163-II, Annex 7, Via:

<http://www.publications.parliament.uk/pa/cm200001/cmselect/cmhaff/163/163ap06.htm> (accessed 05.02.14)

<sup>34</sup> National Audit Office, 'Returning failed asylum applicants', Report by the Comptroller and Auditor General, HC 76 Session 2005-2006, 14 July 2005, Via: <http://www.nao.org.uk/wp-content/uploads/2005/07/050676.pdf> (accessed 04.02.14), p.1

<sup>35</sup> National Audit Office, 'The UK Border Agency and Border Force: Progress in cutting costs and improving performance', Report by the Comptroller and Auditor General, HC 467, Session 2012-13, 17 July 2012, Via: <http://www.nao.org.uk/wp-content/uploads/2012/07/1213467es.pdf> (accessed 04.02.14), p.4

<sup>36</sup> Home Office, UK Border Agency, 'UK Border Agency Business Plan: April 2011-March 2015', 13 May 2011, Via: <http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/uk-border-agency-business-plan/business-plan/ukba-business-plan?view=Binary> (accessed 05.02.14), p.27

additional expenditure. For example, Programme Cyclamen - the project designed to screen material entering the UK border for illicit radiological substances - constituted a £100million, ten-year contract between the Home Office and the Serco Group.<sup>37</sup> Even more significantly, the Government committed £1.3bn of public money over ten years towards the implementation of its high profile e-Borders programme. Whilst even this sizeable new programme pales in comparison to many contracts let by the MoD in the defence sector, this section has shown a general trend towards increasing levels of public sector expenditure on UK border security since 9/11. To explore the origins, character and the potential consequences of the public-private dynamics that have emerged in this context, the chapter turns to an examination of the e-Borders IT project - a project which prior to its cancellation represented the Home Office's largest single procurement by a considerable margin.<sup>38</sup>

### **4.3 Public-private security interactions**

As the involvement of the 'wider business' category of private sector entities introduced in Chapter 1 was found to be limited within the UK border security arena, this section has selected to focus its micro-level analysis on the 'supply' and 'operational' public-private dynamics which arose in the context of the Home Office's largest single CT-related security contract after 9/11. The section supports the main argument of this thesis; the e-Borders IT contract proves that whilst existing presentations of 'the SIC' may be seductive, they do not fully explain the complexity of the public-private dynamics at play; the private sector's involvement in within the 'wider security' arena is more complex than has hitherto been

---

<sup>37</sup> FE Investigate, 'Serco Group PLC Contract Award', 12 Oct. 2005, Via:

<http://www.investigate.co.uk/article.aspx?id=20051012092509PCC89> (accessed 30.12.14)

<sup>38</sup> The HASC recently stated that the e-Borders programme 'is worth as much as the Home Office's two next largest projects – COMPASS and the Disclosure and Barring Service Programme - combined.' Home Affairs Select Committee, 'The work of the Permanent Secretary', Thirteenth Report of Session 2013-14, HC 233, Via:

<http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/233/233.pdf> (accessed 05.02.14), p.6

understood. Furthermore, the serious (and costly) difficulties that arose with the contract resemble something much more like a blunder than a conspiracy of the type often presented as being associated with 'the SIC'.

Part of the reason for this complexity may be the dependence that Government has on the private sector to deliver the security technology it needs. As noted above, technology has become increasingly relied upon in the UK Government's border security strategy; this attitude is captured from the outset of its 2007 White Paper, *Securing the UK Border*. Having recognised (and criticized) the limits of the 'twentieth century concept' of 'a single, staffed physical frontier, where travellers show paper-based identity documents', the document states the following vision:

We believe a new doctrine is demanded, where controls begin off-shore and where we use information, intelligence and identity systems to allow scrutiny at key checkpoints on the journey to and from the UK.<sup>39</sup>

Whilst the use of hi-tech systems for border security has not been universally embraced<sup>40</sup>, it is now in large part the private sector, not Government, who develops the security capabilities used in this sector. This was apparent in the most complex UK border security project ever to be developed by the UK Government.

### **Case Study: e-Borders**

No serious appraisal of the Home Office's 'e-Borders' programme would claim that it resembled anything like a model of best practice in project management. On the contrary, unflattering depictions of the project have appeared regularly; one IT industry media commentator has referred to the scheme as 'a public policy failing reminiscent of Margaret

---

<sup>39</sup> Home Office, 'Securing the UK Border', p.3

<sup>40</sup> Amore, 'Algorithmic War'. The use of technology has also been looked upon negatively in parts of the media; the tone of one article covering the capabilities of the e-borders serves as a good example: Jason Lewis, 'Stasi HQ UK... where details of all your journeys are secretly logged and kept for a decade', *Mail on Sunday*, 21 March 2009, Via: <http://www.dailymail.co.uk/news/article-1163786/Stasi-HQ-UK---details-journeys-secretly-logged-kept-decade.html> (accessed 05.02.14)

Thatcher's poll tax'<sup>41</sup>, for example, whilst the Parliamentary committee responsible for its oversight, the HASC, has described e-Borders as a 'lamentable saga'.<sup>42</sup>

Several headline points indicate why the project has been, and continues to be viewed so negatively. In August 2014, after almost four years of a behind-closed-doors arbitration procedure between the UK Home Office and its prime contractor Raytheon Systems (following the former's sacking of the company in 2010), the Government's decision was judged to be illegal and so ordered to pay £224m to the company.<sup>43</sup> In the meantime, as a result of the contract termination, the UK's border security strategy currently relies on technology that was developed a decade ago for the pilot project ('Semaphore') pre-dating e-Borders. Whilst a report by the UK's independent chief inspector of borders and immigration has recognised that e-Borders had delivered 'significant benefits for the police'<sup>44</sup> - thus suggesting that the ferocity of the criticism levelled against the project may be over-exaggerated - the implementation of the flagship post-9/11 border security programme was beset by difficulties, as the remainder of this chapter shows. Before exploring the origins and characteristics of e-Borders, and any role that 'an SIC' may have played in its instigation and demise, an analysis is presented of the context and original purpose of the now much-maligned programme.

It is noteworthy that, shortly prior to 9/11, the HASC lamented the lack of 'a single computer system' across different border security agencies. One section of a HASC report devoted to 'Information Technology' recommended:

---

<sup>41</sup> Michael Cross, 'The illegal e-Borders disaster', *theguardian.com*, 18 December 2009, Via: <http://www.theguardian.com/commentisfree/libertycentral/2009/dec/18/illegal-eborders-disaster-it-profession> (accessed 07.02.14)

<sup>42</sup> HASC, 'The work of the Permanent Secretary', p.4

<sup>43</sup> Helen Warrell and Ed Crooks, 'UK ordered to pay Raytheon £224m over eBorders contract', *Financial Times*, 18 August 2014, via: <http://www.ft.com/intl/cms/s/0/68f98f04-23bf-11e4-8e29-00144feabdc0.html#axzz3Bmd5FHsZ> (accessed 31.08.14)

<sup>44</sup> John Vine CBE QPM, "'Exporting the border"? An inspection of e-Borders: October 2012 – March 2013', Ref. HO\_02088\_ICI, 9 October 2013, Via: <http://icinspector.independent.gov.uk/wp-content/uploads/2013/10/An-Inspection-of-eborders.pdf> (accessed 07.02.14), p.2

The lack of sufficient information and communications technology in the Immigration Service should be addressed urgently. The under-investment in such technology has undoubtedly caused difficulties in maintaining effective border controls.<sup>45</sup>

Whilst in its response at that time the Government did not appear to believe that wholesale reform or the development of a specific new programme such as e-Borders would be needed, it explicitly recognised 'the need for effective use of information and communication technology in the Immigration Service'<sup>46</sup>. As shown below, the e-Borders Business Case would invoke in its justification for the project the need for greater integration amongst border agencies, and in particular their handling of intelligence information, through an advanced IT solution. Before then, we can say that, prior to 9/11, an argument was already emerging that new technological solutions would be needed to manage the UK border more effectively.

That CT was used as a specific justification for the development of the e-Borders programme is clear, however. Amoore has correctly contextualized the development of the programme within the context of the 'War on Terror'<sup>47</sup>, and, more recently, Dibb et al. have argued in their valuable research on the effect of the project on the aviation sector that e-Borders should itself be seen as a 'counter-terrorism initiative'<sup>48</sup>. Considering e-Borders as being intimately connected to the CT agenda is supported by data arising from interviews and the Government's own business case for e-Borders. According to a former

---

<sup>45</sup> Home Affairs Select Committee, 'Border Controls: Report and Proceedings of the Committee', First Report from the Home Affairs Committee, Session 2000-01, HC 163-I, Via: <http://www.publications.parliament.uk/pa/cm200001/cmselect/cmhaff/163/16311.htm#a14> (accessed 10.02.14)

<sup>46</sup> Home Affairs Select Committee, 'Border Controls', Fourth Special Report, Government Reply to the First Report from the Home Affairs Committee, Session 2000-01, HC 375, Via: <http://www.publications.parliament.uk/pa/cm200001/cmselect/cmhaff/375/37502.htm> (accessed 10.02.14)

<sup>47</sup> Amoore, 'Algorithmic War'

<sup>48</sup> Sally Dibb, Kirstie Ball, Ana Canhoto, Elizabeth M. Daniel, Maureen Meadows, Keith Spillar, 'Taking responsibility for border security: Commercial interests in the face of e-borders', *Tourism Management*, Vol.24 (2014), p.51

Raytheon employee involved in the company's bid to manage the programme, e-Borders was 'a fairly pivotal, large scale national security programme.'<sup>49</sup> Brading continued:

And it was touted very much as national security. It wasn't about human immigration, organised crime really. It was really focused on CONTEST.<sup>50</sup>

The stated purpose and objectives of the programme within the Full Business Case for e-Borders supports this notion; whilst it also aimed to realize other benefits such as greater efficiency and integration amongst immigration agencies, it was principally designed for, and driven in substantial part by, the need to fulfil the Government's CT objectives. Indeed, the document includes multiple references to the programme's direct, central connection to CONTEST; its introduction explicitly states that '[e]ffective border security is critical to the counter-terrorism effort.'<sup>51</sup> Furthermore, the listed advantage of e-Borders given most prominence in the presentation of a 'benefits' section within the Business Case is 'national security'. Paragraph 2.4.3.2 of the document states:

e-Borders will improve security by providing the security and intelligence agencies with the ability to identify, track and analyse the activities of potential terrorists and other national security targets across the border, prevent them travelling, or intervening where appropriate.<sup>52</sup>

A further indication of e-Borders's CT-focus is found within the 'economic appraisal' contained in the Business Case. Whilst alongside the growing emphasis within the research community on the need to apply cost-benefit analysis methodology to CT spending<sup>53</sup> there has been a greater emphasis in Government to ensure that any new procurement programmes achieve 'value for money', any potential economic benefits to be had from e-Borders obviously took on a secondary importance. The document actually even declined to complete a 'quantification in monetary terms of as many of the costs and benefits as feasible', arguing:

---

<sup>49</sup> Interview, John Brading

<sup>50</sup> Ibid.

<sup>51</sup> Home Office, 'e-Borders – Full Business Case, V1.0', p.5

<sup>52</sup> Ibid. p.20

<sup>53</sup> See especially Mueller and Stewart, *Terror, Security, and Money*

In this case, however, given that the key benefits relate to enhancing national security and operational effectiveness, it is not possible to quantify a financial value for these directly[.]<sup>54</sup>

Whilst a brief, broad estimation of the costs of e-Borders was made within the document, these would increase dramatically over the course of the project's lifecycle. Whether the absence of earlier, more detailed thinking on the realistic costs of e-Borders contributed to the failure of the contract - or whether they may have been the result of more complex factors and/or potentially dubious motivations - are important considerations.

If the renewed focus on CT informed e-Borders' development, and helps to explain its justification, what comprised the programme's main elements? Helpfully, its technical components have been outlined within several documents covering the project; its basic motivation was, in the words of the independent reviewer of UK border security, to develop '...a programme of work designed to deliver a modernized immigration control that would be more effective, efficient and secure.'<sup>55</sup> To achieve this, the purpose of the programme was, according to the HASC:

The e-Borders programme provides for electronic collection and analysis of information on all passengers entering or leaving the UK from carriers (including airlines, ferries and rail companies).<sup>56</sup>

According to the Government's March 2007 White Paper, *Securing the UK Border*, the aspiration was to establish a 'new offshore border control' through technological means<sup>57</sup>.

The following procedures would enable this:

The process will involve carriers sending us passport data prior to travel, both inbound and outbound. The data will be analysed (...) and alerts will be issued to the partner agencies on individuals of interest.<sup>58</sup>

---

<sup>54</sup> Home Office, 'e-Borders – Full Business Case, V1.0', p.48

<sup>55</sup> John Vine, "'Exporting the border"?'', p.11

<sup>56</sup> Home Affairs Select Committee, 'The E-Borders Programme', Third Report of Session 2009-10, HC 170, 15 December 2009, Via: <http://www.publications.parliament.uk/pa/cm200910/cmselect/cmhaff/170/170.pdf> (accessed 10.04.14), p.5

<sup>57</sup> Home Office, 'Securing the UK Border', p.16

<sup>58</sup> Ibid.



In effect, the Government planned to introduce a system capable of collecting a large amount of passenger data, in advance of their journeys to and from the UK, sourced via third-party transport operators who would be required to provide it, and subject such data to analysis and comparison with various security-related databases. A briefing paper by the UK Parliament's Research Library neatly summarizes how the data would be handled:

Once a passenger checks in, their data will be sent electronically to an e-Borders operations centre and will be compared to information held on databases there. Decisions will be made against determined criteria and, if necessary, the carrier (the airline, for example) will be alerted that some kind of intervention is needed.<sup>59</sup>

In such a way the UK Government would be able to 'export the border', at least in theory, a proposition the 2009 report by John Vine on e-Borders would later examine.

According to the original proposal, the timescale for delivery would be aggressive; e-Borders' Business Case included a 'Delivery timeline' which stated that 95% of international passenger and crew details would be collected and checked by December 2010, and that 'Full Operating Capability' would be reached by March 2014.<sup>60</sup> Unfortunately, the proposed timescale suffered from considerable delays and became increasingly politicized. In October 2013, for example, a significant controversy emerged around the failure to implement e-Borders fully; the Government was criticized when the Vine Report reported that only 65% of total passenger movements into the UK were actually being covered. This resulted in the then Immigration Minister seeking to reassure the public, explaining on BBC television that '...everybody that turns up in Britain is of course checked at the border.'<sup>61</sup> In the Government's attempts to contain the political fall-out of the delays in the programme, the fact that one of the main aims of the e-Borders

---

<sup>59</sup> Gabrielle Grimwood, 'E-borders and Operation Semaphore', Standard Note: SN/HA/3960, 7 November 2008, Via: <http://www.parliament.uk/briefing-papers/SN03980/eborders-and-operation-semicolon> (accessed 14.02.14), p.9

<sup>60</sup> Home Office, 'e-Borders – Full Business Case, V1.0', p.112

<sup>61</sup> Video interview available within report by Danny Shaw, 'E-borders system "failing on passenger checks"', *BBC News*, 9 October 2013, Via: <http://www.bbc.co.uk/news/uk-24453677> (accessed 11.02.14)

programme was to 'export the border' seemed to have been at least temporarily forgotten.

It is worth briefly comparing and contrasting several additional key characteristics of e-Borders with the previous chapter's FiReControl case study, lest it appear that the thesis is covering identical ground. Firstly, it can be observed that, in addition to their CT justifications, both programmes incorporated significant IT components for which, in both cases, the Government decided to appoint an industrial 'prime contractor' to deliver the work. Secondly, it was shown how the (estimated and actual) costs of FiReControl grew substantially over the lifecycle of the project; the same can be said of e-Borders. The original Business Case's only attempt at a financial assessment estimated that '...the net additional cost to Government of e-Borders in the region of £382m'<sup>62</sup> whereas, in the event, the cost breakdown for e-Borders within the period 2007/08 to 2013/14 alone was £472m.<sup>63</sup> That the Government stated that it anticipated the programme to cost an additional £655m between 2015/16 and 2021/22<sup>64</sup>, and the HASC has referred to e-Borders as having lifetime costs of £1.3bn<sup>65</sup>, might lead us to naturally question how and why the original assessment was determined. Finally, whilst the FiReControl project was scrapped in its entirety, and at least some parts of e-Borders continue to be pursued at the time of writing (albeit under a different name), both contracts were cancelled by the coalition Government not long after its formation in 2010. The previous chapter explored its perceived motivations for doing so with FiReControl; with regards to e-Borders, the Government similarly announced on 22 July 2010 that contract was terminated because

---

<sup>62</sup> Home Office, 'e-Borders – Full Business Case, V1.0', p.7

<sup>63</sup> John Vine, "'Exporting the border'?", p.15

<sup>64</sup> Ibid.

<sup>65</sup> HASC, 'The work of the Permanent Secretary', p.6

‘...the Home Secretary has no confidence in the prime supplier of the e-borders contract, Raytheon, which since July 2009 has been in breach of contract.’<sup>66</sup>

The two projects differed in important respects, however, and a failure to take these into account might create the mistaken impression that the problems they encountered were identical. Firstly, whilst FiReControl and e-Borders were both undeniably UK ‘security’ programmes, it should be noted that their ‘host’ Government departments were different ones entirely; DCLG was responsible for the former, whilst it was the Home Office (and in particular the UKBA within its purview) that developed e-Borders. The consequences of what many interviewees described as a ‘diverse’ security sector are revisited in later chapters; suffice to say here that, unlike in defence, these examples illustrate how no single ministry has been responsible for all CT-related public sector procurement projects after 9/11. Secondly, whereas in the case of FiReControl the business case and the decision to proceed with the project were allowed to develop out of sequence, the programme management and ‘sign-off’ for e-Borders was much more orderly; crucially, the Business Case for the project was completed *before* any contracts were issued. Furthermore, prior to the appointment of Raytheon Systems in December 2007<sup>67</sup>, it has been revealed that no less than five official OGC ‘Gateway Reviews’ were completed.<sup>68</sup> It was notwithstanding the adoption of this more sensible approach to managing major public sector projects that considerable difficulties emerged. Finally, in so far as *delivering* the projects was concerned, each consisted of a very different set of (public and private sector) stakeholders. Whilst in both cases the Government engaged a private company to supply the IT components of the project - and both were well known companies possessing a longstanding record of operating in defence - they relied on very

---

<sup>66</sup> Home Office, ‘E-borders contract terminated’, Home Office Press Release, 22 July 2010, Via: <https://www.gov.uk/government/news/e-borders-contract-terminated> (accessed 11.02.14)

<sup>67</sup> Home Office, ‘e-Borders – Full Business Case, V1.0’, p.108

<sup>68</sup> The ‘Gateway Review’ process is one of the UK Government’s main ways of independently assessing the performance of major projects at various identified stages of their lifecycle.

different external actors for their successful implementation. In the case of FiReControl, serious difficulties emerged as a result of the main 'end user' constituency not being sufficiently engaged in the project. In the case of e-Borders, by contrast, it would be private companies - transport operators such as airlines and ferry companies - upon whom the Government would rely for interacting with its prime contractor, and indeed programme delivery. This crucial difference reflects the varying character and operation of the different sub-sectors that comprise the CT sector; these important differences do not exist to the same extent within the military sector, thus reinforcing the notion that the character of the 'industrial complex' in the CT aspects of UK national security strategy is of a very different order.

A deeper examination into the development of e-Borders and its difficulties helps to reveal the character of the sector's public-private dynamics, and their impact. Notwithstanding the publication of the Government's account of the proceedings relating to the concluded arbitration process<sup>69</sup>, however, there remains a degree of secrecy around the dispute that took place between the Home Office and Raytheon, presenting challenges for analysis. Nevertheless, this thesis has benefitted from the recent publication of several reports on e-Borders, and conversations with interviewees who were willing to provide data under the condition of anonymity.

On the surface, Raytheon was sacked as the prime contractor for e-Borders because it was considered by the Government to be in 'breach of contract'; a written statement by the then Minister for Immigration detailed the position:

Over recent weeks we have been examining the progress of the [e-Borders] programme and it has been extremely disappointing. While some elements have been delivered, they have not been delivered on time. Delivery on the next critical parts of the programme are already running at

---

<sup>69</sup> Home Office, 'Home Secretary letter on the e-Borders programme arbitration', 18 August 2014, Via: <https://www.gov.uk/government/news/home-secretary-letter-on-the-e-borders-programme-arbitration> (accessed 18.08.14)

least 12 months late. On top of this there remain risks of further delays, and there is no confidence in the current prime contractor – Raytheon Systems Limited – being able to address this situation.<sup>70</sup>

Against this backdrop, the Government held that it was because ‘the supplier’s performance to date has not been compliant with their contractual obligations’<sup>71</sup> that it was relieved of its duties; implicit in this position is the suggestion that no other factors played a significant part. Clearly, the court disagreed with this particular viewpoint in its August 2014 ruling.

Several additional issues appear to have contributed to e-Borders’ delivery problems, despite the Government’s insistence that its former prime contractor was to blame. Most significantly, a substantial legal question arose around the extent to which the Home Office was actually ever authorized to collect data on passengers travelling to and from the UK within the EU; a serious doubt emerged in 2009 that e-Borders actually violated EU rules.<sup>72</sup> The fact that consideration of the implications of the EU’s underlying principle of free movement was overlooked by those in Government responsible for designing the project was noted in the Vine Report:

A significant barrier to the achievement of the e-Borders data collection targets was the view taken by the European Commission that it was incompatible with EU free movement rights to impose a mandatory requirement on EEA nationals and family members to provide passenger data to e-Borders in advance of travel.<sup>73</sup>

The Vine Report was not alone in criticizing the failure to identify the risks associated with the scheme’s compatibility with EU rules on free movement and wider data protection procedures; the HASC concluded earlier that the e-Borders programme ‘is (...) likely to be

---

<sup>70</sup> Damian Green, ‘e-Borders Programme’, Written Ministerial Statement, 22 July 2010, Via: <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100722/wmstext/100722m0001.htm#10072238000035> (accessed 14.02.14)

<sup>71</sup> Ibid.

<sup>72</sup> John Leyden, ‘UK e-Borders scheme thrown into confusion by EU rules’, *The Register*, 18 December 2009, Via: [http://www.theregister.co.uk/2009/12/18/e\\_borders\\_confusion/](http://www.theregister.co.uk/2009/12/18/e_borders_confusion/) (accessed 26.02.14)

<sup>73</sup> John Vine, “‘Exporting the border’?”, p.18

illegal under the EU Treaty.<sup>74</sup> Additionally, one commentator pondered; ‘...how did anyone ever think e-Borders within Europe would be acceptable or legal?’<sup>75</sup> The author would then question the commercial suppliers’ role in this major oversight:

...we deserve to know if anyone in Trusted Borders, the commercial consortium contracted to implement the scheme, at a cost of £1.2bn, sounded a warning. (...) These firms were specifically charged to “work as an open, honest and collaborative team”. Did none of this open honesty involve pointing out that e-Borders within Europe risked being unworkable and illegal?<sup>76</sup>

Whilst Cross poses an interesting question, the problem with this argument is that it overlooks how the e-Borders Full Business Case correctly placed a strong emphasis on the role that Government, not the supplier, would have to play as an ‘Intelligent customer’<sup>77</sup>. Whilst it would clearly have an operational impact, the matter of weighing up the effects of EU legislation on any major UK programme such as e-Borders must be seen as fundamentally a *policy consideration*. In this case, the Business Case did not include such an assessment at the same time as arguing that one of the responsibilities of the Government would be to ‘Provide overall strategy formulation, policy and standard-setting to the Service Provider.’<sup>78</sup> Furthermore, it is important to ask - in the context of this thesis’s interest in the potential impact of ‘the SIC’ on national security strategy - whether it would ever be desirable to hand the responsibility for determining such policy matters to profit-making security suppliers. Unfortunately in this case, the (ultimately costly) risks associated with e-Borders’s compatibility with EU law appear to have been completely overlooked; this should be seen as primarily an oversight arising from Government, not any company.

A second issue that obviously contributed to e-Borders’ failure was the quality and effectiveness of the programme’s *engagement with the travel industry*; a constituency

---

<sup>74</sup> Home Affairs Select Committee, ‘The E-Borders Programme’, p.66

<sup>75</sup> Cross, ‘The illegal e-Borders disaster’

<sup>76</sup> Ibid.

<sup>77</sup> Home Office, ‘e-Borders – Full Business Case, V1.0’, pp.100-102

<sup>78</sup> Ibid. p.101

whose support, in the words of the project's original Senior Responsible Owner (SRO) within the Foreword to the e-Borders business case, '...is crucial to the successful delivery of the project.'<sup>79</sup> It is important to recognise that, in the recent history of the UK's strategy to improve border control, e-Borders would not be the first time where the Government's record on engaging private sector stakeholders effectively would be questioned; the HASC's 2001 report into Border Controls included, for example, the observation that 'Port operators and carriers have told us that they are not consulted sufficiently by the border agencies.'<sup>80</sup> However, an even weaker approach to 'industry engagement' appears to have developed on e-Borders. Whilst there is a suggestion that *some parts* of the travel industry were consulted even before the contract was let - the Business Case states that 'the Programme is now involved in a series of workshops designed to explore and resolve specific issues and concerns' and that 'Engagement with carriers and ports will continue throughout the implementation'<sup>81</sup> - it has become apparent that, whether deliberately or inadvertently, some travel sectors were not engaged effectively in the consultation process. The HASC's 2009 report on e-Border is particularly illuminating in this regard; within a 12-page section titled 'Problems faced by carriers' the Committee highlights that whilst 'the maritime sector was engaged in discussions at an early stage of the process', an unfortunate situation emerged where;

...the overwhelming sense we received from our maritime witnesses was that, far from laying strong foundations on which they would be able quickly to build a practical system, the talks had made little progress and, indeed, had in some respects gone backwards.<sup>82</sup>

The question of whether some commercial travel companies (or even sectors) may have resisted, or perhaps sought to limit, the additional requirements arising from e-Borders is important and one that may have played into this sentiment. However, the sense of a lack

---

<sup>79</sup> Ibid. p.4

<sup>80</sup> HASC, 'Border Controls: Report and Proceedings of the Committee'

<sup>81</sup> Home Office, 'e-Borders – Full Business Case, V1.0', p.24

<sup>82</sup> HASC, 'The E-Borders Programme', p.13

of effective consultation and engagement is supported by the 2013 Vine Report; this listed ‘the lack of alignment between the e-Borders and the business models employed in the maritime and rail sectors’<sup>83</sup> as one of three main issues listed within a section titled ‘Barriers to achievement of data collection targets’<sup>84</sup>. Whereas some innovative models of engagement were developed in particular with the aviation sector - the HASC identifies that this sector’s involvement extended ‘even to the point of being included in meetings with prospective suppliers as part of the procurement process’<sup>85</sup> - it cannot be said that this was replicated across the entire travel industry. This appears to be a significant failure in project design, particularly in view of e-Borders’ inevitably heavy dependence on these industries.

Whilst this thesis is reluctant to engage in any ‘blame game’ type of discussion, this shortcoming in ‘industry engagement’ inevitably invites the question as to who was (or indeed should have been) responsible for engaging the travel industry; the Government or its prime contractor? Whilst the actual contract signed between the Government and the Raytheon-led Trusted Borders consortium is not publicly available - thus the contractually-agreed separation of responsibilities cannot be validated - the Business Case for e-Borders clearly identifies both how the obvious complexities around this particular issue were recognised at an early stage, and how the Government envisaged they would be managed. Indeed, it is striking to see a caveat contained within one of the ‘responsibilities’ falling upon the supplier in the ‘commercial approach’ section of the document; ‘The Service Provider will be responsible for ensuring that carriers provide data to e-Borders (*subject to certain limits*)[.]’<sup>86</sup> Indeed, such was the recognition that ‘certain limits’ existed around ensuring the participation of the travel operators that the Business case also establishes a

---

<sup>83</sup> John Vine, “Exporting the border”?, p.18

<sup>84</sup> Ibid. pp.17-18

<sup>85</sup> HASC, ‘The E-Borders Programme’, p.13

<sup>86</sup> Home Office, ‘e-Borders – Full Business Case, V1.0’, p.87 (Emphasis added)



three-stage process to be followed ‘if carriers and ports refuse to work with the Service Provider’<sup>87</sup>. In short, the dedicated process allowed the Service Provider to inform the UKBA around incidences of non-compliance on the part of an operator, opening the possibility that, subject to the implementation of an agreed ‘industry stakeholder action plan’, it may be ‘given relief/compensation (as appropriate) from its obligations under the contract.’<sup>88</sup>

Whilst judging by the Business Case the primary *operational* responsibility would therefore appear to have been placed on the Service Provider for acquiring data from the travel operators, it can now be asked whether what seems to have been such a ‘hands off’ strategy on the part of the Government was sensible in view of the large number of transport operators that had to be engaged. Asked whether the requirement upon Raytheon to engage with such a multiplicity of private transport operators contributed to the difficulties that ultimately developed, one former employee of Raytheon responded:

Yes, it has an enormous impact that a lot of the stakeholders, who are not paying for the programme, are private individuals or private industries.<sup>89</sup>

Revealingly, a separate conversation held on the condition of anonymity with an industry executive with knowledge of Raytheon’s contract questioned the effectiveness of how the transport sector engaged on e-Borders, suggesting a lack of enthusiasm to participate contributed in the difficulties; ‘of course you’re going to stand up and say “count me out, I’m not being part of this because it’s too bloody complicated, it’s going to cost me money.”’<sup>90</sup> The same executive offered a view of the dynamics that developed between the Government, Raytheon and the operators as follows:

...we were in no position to control a third party. We had no leverage over them whatsoever. We couldn’t negotiate. They held all the cards. We had

---

<sup>87</sup> Ibid. p.94

<sup>88</sup> Ibid.

<sup>89</sup> Interview, John Brading

<sup>90</sup> Interview, Industry Executive

to rely on the government to do something for us, and the government were; 'not our problem, it's your risk'. So it does complicate things when you... when the risk is in your area... is an area that you can't control.<sup>91</sup>

The notion that private sector operators might be hesitant to pay additional costs arising from a new security programme like e-Borders is not new and has been identified elsewhere<sup>92</sup>; indeed this ever-present, thorny issue appears to have been recognised from the outset of this project. In hindsight, it is obvious that a contractor like Raytheon might find it difficult to obtain data from private transport operators. Processes may have existed on paper to tackle any arising issues, but the events that transpired suggest that it is doubtful whether the overall (policy) framework for engaging end-users - a framework which was designed and 'owned' by the Government - was ever sufficiently robust in its approach towards ensuring effective 'industry cooperation'.

Whilst in contractual terms the emphasis might have been upon Raytheon to collect the desired passenger data from transport operators, and thus the 'risk' lay with the company if things went wrong, it is clear that the Government had a clear stake in the outcome of the company's endeavors; not least from a security perspective. Furthermore, the e-Borders Full Business Case states the need for a *shared approach* to be maintained in the development of e-Borders, including in the specific area of stakeholder engagement, both within and outside Government:

The Service Provider will be fully involved with the programme in the *joint management and governance arrangements* both with agencies and with carriers and ports.<sup>93</sup>

Unfortunately, events clearly indicate that cooperation between the Government and Raytheon on engaging the transport industry completely fell apart. It may be some time before details of the most contentious issues arising from the arbitration procedure are revealed but, in light of the available evidence, it would be extremely surprising if a

---

<sup>91</sup> Ibid.

<sup>92</sup> Neville-Jones and Fisher, 'Homeland Security and the Role of Business', p.170

<sup>93</sup> Home Office, 'e-Borders – Full Business Case, V1.0', p.99 (Emphasis Added)

disagreement over responsibilities in this area was not one of them. It is clearer that the relationship between the Government and Raytheon suffered particularly in respect to how the project should be managed. As an unnamed industry official apparently associated with one of the companies within the Trusted Borders consortium relayed to the *Financial Times* upon the cancellation of the project; 'This is about a falling-out between Raytheon and the Home Office and about project management.'<sup>94</sup>

Finally, it is now evident, following the arbitration ruling, that the Government's case for sacking Raytheon was not as clear cut as its statements at the time of the contract termination suggested. Interestingly, in advance of the decision, the delay on the ruling was lamented by both the Home Office and the HASC; when asked about the anticipated date of the legal judgment on e-Borders, the Permanent Secretary at the Home Office stated; 'To my frustration, I don't know when we can expect a decision'<sup>95</sup>. In response, the HASC concluded in no uncertain terms:

We are appalled at the handling of this matter post-termination of the contract; and that 3½ years later it is still not resolved. Neither the company nor the Government are in a position to explain more. The confidentiality means we do not know [sic.] what went wrong and are losing the opportunity to ensure this does not happen again. To avoid conspiracy theories there has to be full transparency and lessons need to be learnt.<sup>96</sup>

The considerable length of the process does appear to be unusual; the website of the London Court of International Arbitration (LCIA) - the institution tasked with handling the e-Borders case - states that;

...around half of all cases referred to the LCIA that run their course from Request for Arbitration to Final Award are typically concluded in 12 months or less, and more than three quarters in 18 months or less.<sup>97</sup>

---

<sup>94</sup> James Boxell, 'May sacks Raytheon from e-borders contract', *Financial Times*, 22 July 2010

<sup>95</sup> HASC, 'The work of the Permanent Secretary', Ev16, Q102

<sup>96</sup> Ibid. p.7

<sup>97</sup> 'Frequently Asked Questions', LCIA Website, Via:

[http://www.lcia.org/Frequently\\_Asked\\_Questions.aspx#Length](http://www.lcia.org/Frequently_Asked_Questions.aspx#Length) (accessed 28.01.14)

Whilst the precise causes of the delay can only be speculated upon, it can be observed that Raytheon always strongly contested the Government's suggestion; a letter submitted to the HASC in August 2011 by the UK CEO of Raytheon, Robert Delorge, read as follows;

...our contract was terminated by the Home Secretary in July 2010 on the grounds that Raytheon was allegedly in material default of its contractual obligations. We vigorously refute that contention. We maintain that the purported termination was unlawful and that Raytheon is entitled to recover substantial damages for wrongful termination.<sup>98</sup>

One industry figure with a close understanding of the dispute suggested on the condition of anonymity that any impression that the company should be held entirely to blame for the difficulties encountered would be incorrect. Reflecting on the findings of the October 2013 Vine report, the individual stated: 'It was a wonderful statement of Raytheon's case.'<sup>99</sup> It is now clear that Raytheon was not judged to be entirely at fault for the events which led to the Government's decision to terminate its e-Borders IT contract; it is also now apparent that factors other than any sinister motivations on the part of 'the SIC' contributed towards the whole affair.

What weight might be assigned, in considering both the project and the difficulties that transpired, to the strength of any influence exerted by those private sector companies who were involved in the project, and/or any alliance they may have formed with the public officials overseeing the programme? In particular, was there any evidence of a dynamic within the system towards overstating the necessary requirements - the practice known in the sector as 'gold-plating' - as it has been suggested occurs in the defence sector? Whilst in its 2009 report on e-Borders the HASC suggested that the significant number of changes in senior staff at the UKBA over the lifecycle of the programme could '...have led to the perception that UKBA had been 'captured' by its chosen provider and

---

<sup>98</sup> Letter from Robert M Delorge to Keith Vaz MP, 3 August 2011

<sup>99</sup> Interview, Industry Executive

lost sight of what was reasonable and practicable<sup>100</sup>, there appears to be no specific evidence of any occurrence of impropriety. Indeed the impression left is extremely far from the notion that some form of ‘cosy conspiracy’ was in operation; the UKBA and Raytheon appear to have been at complete loggerheads with each other. According to Raytheon’s CEO, for example, ‘...the Government’s targets and objectives changed repeatedly throughout the course of the Programme.’<sup>101</sup> Even if the Government was consistent that it was Raytheon who was in breach of contract, this point is validated through the Minister for Immigration’s statement that ‘[t]here were 58 changes to the specifications for the contract’<sup>102</sup>.

Furthermore, it would be fanciful to suggest that Raytheon deliberately entered into the IT contract with a view to ultimately seeking a substantial financial return gained through a legal challenge - one ultimately based on an argument of loss of earnings, having been sacked from the project. Having said this, it is hardly surprising that the outcome whereby a contractor receives substantial payment (paid for by the taxpayer) for work not completed might raise some criticism, if not outright suspicion. It is to be hoped that the Government’s commitment to share with Parliament ‘much fuller detail once the case has concluded’<sup>103</sup> is upheld. Before then, as noted above, the lack of transparency around the e-Borders arbitration process is worrisome. That the LCIA is transparent about the rules it sets for confidentiality in its arbitration proceedings<sup>104</sup> is of little consolation to analysts and researchers of e-Borders, not to mention the wider public. It could also be enormously

---

<sup>100</sup> HASC, ‘The E-Borders Programme’, p.13

<sup>101</sup> Letter from Robert M Delorge to Rt Hon Keith Vaz MP, 3 August 2011.

<sup>102</sup> Hansard, Damian Green, Parliamentary Question Reply, 15 Sep 2010 : Column 1073W, Via: <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100915/text/100915w0002.htm#10091521000116> (accessed 05.02.14)

<sup>103</sup> Committee of Public Accounts, ‘The Border Force: securing the border’, Thirty-first Report of Session 2013-14, HC 663, 2 December 2013, Ev 19, Q186

<sup>104</sup> According to the LCIA, ‘Confidentiality is still generally regarded as one of the primary underpinnings of arbitration. Nobody who is not a proper party to an arbitration, or a legal representative of a party, may obtain information about pending or completed arbitrations from the LCIA.’ ‘Frequently Asked Questions’, LCIA Website

problematic - not least for all parties' reputations - if it was decided that this type of process should be routinely pursued in the future. As the HASC has astutely noted, a lack of transparency does nothing to dissuade the development of conspiracy theories in this area.<sup>105</sup>

It has also become apparent that, in addition to Raytheon's own remuneration, a significant amount of public expenditure was allocated to various consultancy firms for the work they conducted on e-Borders. A response to a Parliamentary question has clarified, for example, that, between 2006-07 and the first three months of 2010-11, the cost of consultants and independent contractors to the e-Borders programme was £45.1m.<sup>106</sup> Whilst there is no suggestion of any untoward behavior being conducted by such firms in the case of e-Borders, it can be noted that, like FiReControl, the provision of such expertise did not succeed in averting the cancellation of what has been cited as an important Government contract. Whilst there would not appear to have been the level of 'bad blood' that existed between consultants and the prime contractor on FiReControl - with e-Borders the most serious antipathy appears to have been reserved for the Home Office-Raytheon relationship - we can question whether it is appropriate that upwards of £40m taxpayers' money was spent on employing 'experts' that ultimately failed to prevent a contract cancellation.

Finally, as noted above, the success of the e-Borders IT contract relied on the provision of passenger data by the transport industry. In this context, it is important not to overlook how schemes such as e-Borders might be affected by the commercial interests of such operators, and the role that new Government requirements may play in influencing their behaviour. Recent research by Dibb et. al. has expertly examined these under-

---

<sup>105</sup> HASC, 'The work of the Permanent Secretary', p.7

<sup>106</sup> Hansard, Damian Green, Parliamentary Question Reply, 15 Sep 2010 : Column 1074W, Via: <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100915/text/100915w0002.htm#10091521000116> (accessed 05.02.14)

researched interactions; usefully specifically in the case of e-Borders. Importantly, their article provides an assessment of the potential impact that Government regulation may have (or be seen to have) on the commercial interests of the carriers:

For carriers, e-borders has the potential to threaten these interests because of the operational costs involved in implementing the initiative and its potential to damage customer relationships.<sup>107</sup>

The findings of their research - drawn from 24 original semi-structured interviews - supports the damaging evidence provided by transport operators to the Parliamentary inquiries referred to above, and casts new light on how transport operators considered e-Borders negatively. Additionally, it further questions the effectiveness of engagement that was established with them. In a striking statement relating to the premise of the whole scheme, the authors conclude:

Compliance with e-Borders was seen as conflicting with the commercial interests of travel firms due to the costs and other resources involved, disruption caused to existing operations and ways of working, and negative effects on customers and on service quality.<sup>108</sup>

That Raytheon might struggle to overcome the (commercially-driven) resistance inherent in the above conclusion should, perhaps, not be very surprising; it can be noted in our analysis of the contemporary characteristics of the industrial-complex within the CT sector, however, that this dynamic does not exist in the defence sector. Furthermore, according to one industry executive, the secondary legislation that was designed and put in place to ensure that the carriers complied with the service provider's requests for data 'just didn't cut it'<sup>109</sup>. A failure on the part of Raytheon to fully appreciate the constraints that would arise from this dynamic - the natural logic of private operators' clear desire to protect their own commercial interests - was considered as being part of Raytheon's 'naivety'.<sup>110</sup> One of

---

<sup>107</sup> Dobb et. al., 'Taking responsibility for border security', p.51

<sup>108</sup> Ibid. p.55

<sup>109</sup> Interview, Industry Executive

<sup>110</sup> Ibid.

the consequences of this case, revisited in the concluding chapter, is that Government and its suppliers must do more to take account of such interests in the future.

Before then, it is worth noting that Dibb et. al. raise further questions about the quality of the Government's industrial engagement on e-Borders. They conclude that '[i]n general, there was a feeling among respondents that the government had not taken into account how the industry already worked'<sup>111</sup>, citing the response of one airline representative as follows:

They were having conversations with system suppliers rather than carriers. The obligation falls on the carrier but the system supplier had to do the development work.<sup>112</sup>

That the Government focused on 'getting its own house in order' - seeing its role primarily as a coordinator of the multiple *government agencies* involved in e-Borders - and that, ultimately, it appeared to rely on its supplier to engage with operational side of industry (laden with its own commercial interests) is clearly evident from the Full Business Case. In a striking indication of the lack of the imagination it exhibited to the question of how to structure public-private cooperation around e-Borders effectively, neither 'Carriers and Ports' nor the 'Travel Industry' were even included as a 'main partner' of the programme in the Government's identified list of 'Key stakeholders'<sup>113</sup>. Furthermore, a diagram contained within the Business Case to illustrate the process of obtaining data from carriers is extremely simplistic and arguably indicative of the Government's complete lack of interest in *how* the data would be collected. The diagram below presents the image of data flowing naturally in and out of a central hub:

---

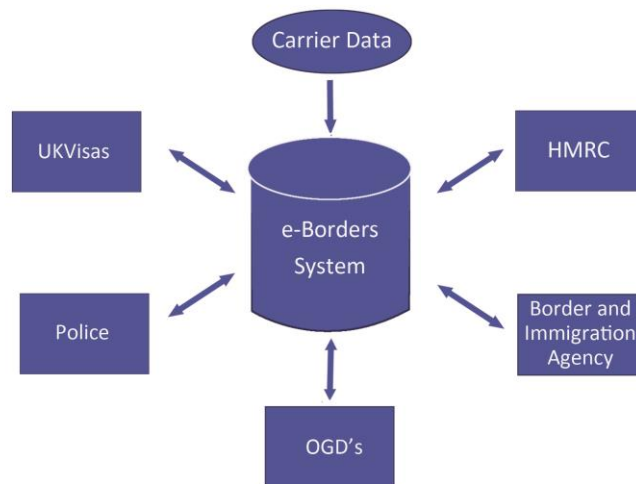
<sup>111</sup> Dibb et. al., 'Taking responsibility for border security', p.56

<sup>112</sup> Ibid.

<sup>113</sup> Home Office, 'e-Borders – Full Business Case, V1.0', p.35



**Figure 4. The exchange of data in the e-Borders programme<sup>114</sup>**



Whilst this approach was possibly convincing on paper at the time, it is now doubtful that the flow of data could ever have been so straightforward; particularly given the reality of the complex governance structure and public-private dynamics analysed above.

#### **4.4 Character and impact of the industrial-complex in Border Security**

The Government's approach to industrial engagement on e-Borders reflects a lack of an appreciation on the part of policy-makers that, under the commercial structure that was selected, a key requisite for e-Border's success would always have been the effective engagement by its contracted security supplier of the operational side of industry; ideally all under the watchful eye of an 'Intelligent customer'. As addressed in the concluding chapter, the e-Borders case-study appears to show that there is an unfortunate lack of an appreciation - perhaps even a worrying disinterest - in Government around the difficulties associated with reconciling the conflicting commercial interests that exist. How to structure the engagement between the supply and operational sides of industry, and

<sup>114</sup> Home Office, 'e-Borders – Full Business Case – Appendices, V1.0', 12 November 2007, p.102. Diagram adapted and reproduced from Parliamentary information licensed under the Open Parliament Licence v3.0.

define Government's vital role therein, becomes an absolutely core consideration in this context; regrettably, in the case of e-Borders, it appears that it was not seen as such.

As we saw with FiReControl, the IT contract for e-Borders developed serious difficulties and, following the Government's sacking of its prime contractor, Raytheon, became widely seen as nothing short of a disaster. Several factors have been offered as potential contributors to the difficulties that emerged in the programme; the secretive nature of the arbitration procedure between the Government and Raytheon means it is still not yet known what exactly transpired. Nevertheless, it is now clear that the Government's argument that Raytheon was the main (if not sole) cause of the difficulties did not stand up to scrutiny.

The e-Borders case study also usefully illustrates the existence of at least two different sets of commercial outlooks in the UK's border security sector; the chapter has shown how the interests of 'suppliers' and private sector 'operators' do not always perfectly align with each other. Thus the commercial dynamics within this CT sub-sector are varied, and can approach each other from opposite sides of the profit-making spectrum. The extent to which any non-alignment of such interests means that a potentially corrosive 'industrial-complex' of the sort we have considered in past can ever materialize therefore needs serious consideration.

Whilst Raytheon and some consultancies did benefit financially from e-Borders, the case-study suggests that, in the UK's border security sector, the idea that the MIC has transferred into the security sector is an over-simplification; the reality is that - at least in the final few years of the contract - the Government embarked upon a serious (and costly) legal dispute with its prime contractor, challenging the idea that a similar 'confluence' of strategic interests is at play in CT. Instead, it is apparent that the Government actually failed to engage the private sector sufficiently in this case; this was particularly evident in

respect of how the transport operators upon whom the whole programme evidently relied were integrated. Regarding its relationship with Raytheon, the Government's engagement with the company became extremely acrimonious and did not resemble the dynamics that critics have argued characterize 'the SIC'.

Ultimately, the unhappy experience of the e-Borders IT contract shows that the question of how Government should structure public-private cooperation more effectively must be addressed. The chapter suggests that on e-Borders, as with other large-scale IT projects such as FiReControl, the Government failed to engage the private sector properly on this matter. We shall encounter similar dynamics in the next chapter covering the security for the London 2012 Olympic Games.

## Chapter 5: Olympic Security

### Introduction

Securing the London 2012 Olympic and Paralympic Games (London 2012) was always going to be a significant challenge for the UK. Prior to the successful passing of the Games themselves, it had long been recognised that more would be expected of London 2012 in security terms than any previous Olympics<sup>1</sup> and that the security for major events had become a 'spectacle'.<sup>2</sup> Even before 7/7 - an attack which occurred the day after London won its bid thus creating an association between the Games and the potential for insecurity<sup>3</sup> - the level of public interest in the plans for London 2012 promised to be substantial. As the British Prime Minister stated in his 2012 'New Year's message'; 'This will be the year Britain sees the world and the world sees Britain.'<sup>4</sup>

This was the context for the British coalition Government's then Defence Secretary, Philip Hammond, to announce on 15 December 2011 that he expected 13,500 military personnel to be deployed in support of the London 2012 security operation<sup>5</sup>, thus reminding observers that 'government's provision of manpower from the armed forces and the police remains integral to securing most recent Games.'<sup>6</sup> Such an extensive use of military assets would be enhanced even further. On 12 July, just weeks before London 2012, the Home Secretary announced that, as a result of a failure to supply sufficient

---

<sup>1</sup> Alphas Hinds, 'Fortress Olympics: Counting the cost of major event security', *Jane's Intelligence Review*, Vol.19:5 (May 2007), p.25

<sup>2</sup> Philip Boyle and Kevin D. Haggerty, 'Spectacular Security: Mega-Events and the Security Complex', *International Political Sociology*, Vol.3:3 (2009), p.263

<sup>3</sup> Houlihan and Giulianotti argue that '[i]nsecurity became the dominant discourse of the 2012 Games' following the 7/7 attacks. Barrie Houlihan and Richard Giulianotti, 'Politics and the London 2012 Olympics: the (in)security Games', *International Affairs*, Vol.88:4 (2012), p.701

<sup>4</sup> David Cameron, '2012 New Year's Message', Via: <https://www.gov.uk/government/speeches/2012-new-year-message-from-david-cameron> (accessed 08.01.12)

<sup>5</sup> Ministry of Defence, 'Military support to 2012 Olympic Games announced', 15 Dec. 2011, Via: <http://www.mod.uk/DefenceInternet/DefenceNews/MilitaryOperations/MilitarySupportTo2012OlympicGamesAnnounced.htm> (accessed 08.01.12)

<sup>6</sup> Will Jennings, 'Governing the Games in an age of uncertainty: The Olympics and organisational responses to risk in Richards et al, *Terrorism and the Olympics*, p.150

numbers of private security officers at the venues, an additional 3,500 Armed Forces would be deployed.<sup>7</sup> On 24 July, just days before the Opening Ceremony, the Culture Secretary then announced that the Government had decided to deploy a further additional 1,200 Armed Forces personnel (that it had placed on standby the previous week).<sup>8</sup> As reportedly described by a senior military officer, the deployment of over 18,000 military personnel on UK shores was ‘the largest peacetime operation ever performed by the armed forces.’<sup>9</sup>

This chapter examines the Government’s often troublesome interactions with the private sector in achieving its London 2012 security objectives. With one notable exception - which itself only covers the ‘security industry’s’ involvement<sup>10</sup> - the private sector’s involvement in London 2012 security had, prior to the Games, been largely overlooked as a major issue worthy of academic analysis. The G4S contract ‘fiasco’ or ‘debacle’, as it has been variously described<sup>11</sup>, changed this and the matter of the failure of the Games’ primary security contractor failing in its obligations subsequently received extensive media scrutiny. Indeed, during the event - which happily passed safely and was ultimately considered a major success for the UK - G4S received fierce criticism and the military’s resulting extensive involvement in the security operation for the Games was hailed by the

---

<sup>7</sup> Home Office, ‘Home Secretary statement on Olympic security’, 12 July 2012, Via: <http://www.homeoffice.gov.uk/media-centre/news/theresa-may-olympic-security> (accessed 26.08.12)

<sup>8</sup> Department for Culture, Media and Sport (DCMS), ‘Jeremy Hunt statement on Olympic security’, 24 July 2012, Via: <http://goc2012.culture.gov.uk/2012/07/jeremy-hunt-statement-on-olympic-security/> (accessed 26.08.12)

<sup>9</sup> Nick Hopkins, ‘Army warns Olympic Games recovery will take two years’, *The Guardian*, 13 Aug. 2012, Via: <http://www.guardian.co.uk/uk/2012/aug/13/army-olympic-games-recovery-two-years> (accessed 26.08.12)

<sup>10</sup> David Evans, ‘The role of the private security industry’ in Richards et. al., *Terrorism and the Olympics*, pp.163-179

<sup>11</sup> Valentina Soria, ‘G4S and London 2012: Choosing your partners wisely?’, *RUSI Analysis*, 26 July 2012, Via: <http://www.rusi.org/analysis/commentary/ref:C50115986AD337/> (accessed 26.08.12)

Chairman of the London Organising Committee (LOCOG) as one of the 'defining features' of London 2012.<sup>12</sup>

With the Games long since passed, it is timely to reflect upon London 2012's security arrangements and consider important questions about the effectiveness of the public-private cooperative arrangements therein. Until now, the detail of these multiple and extensive interactions have not been fully analysed, and the critical focus has been over the presence of vested corporate interests in Olympic security arrangements.<sup>13</sup> A better understanding of the landscape is needed to assess the validity of any claims which purport to show the negative impact of the private sector's (or, indeed, 'the SIC's') involvement in London 2012 security, and consider the consequences of such public-private cooperation. Additional scholarly attention is justified because, despite the major problems that arose with the G4S contract, a case can be made that the Games could not have been delivered safely without the public-private security cooperation covered below.

This chapter first describes the security policy framework that was established for London 2012, before outlining the scale of, and substantial growth in, the Games' security budget. It then analyses the private sector's involvement in the security preparations for London 2012 through the conceptual framework established for this thesis; particularly close attention is paid to the public-private dynamics and problems which arose around the largest manpower security contract for the Games awarded to G4S - the widely-accepted causes of which are challenged. The chapter shows how the UK Government relied on a wide range and variety of private sector entities in delivering its security

---

<sup>12</sup> 'London 2012: Lord Coe applauds armed forces Olympic efforts', *BBC News*, 16 Jan. 2013, Via: <http://www.bbc.co.uk/news/uk-19182310> (accessed 21.02.13)

<sup>13</sup> Boyle and Haggerty suggest that 'The massive budgets and cultural capital associated with Olympic involvement makes them the security industry equivalent of what Paris or Milan is to the fashion industry', Boyle and Haggerty, 'Spectacular Security', p.269. For criticism of industry's involvement in the Athens 2004 Games, see Mina Samatas, 'Surveilling the 2004 Athens Olympics in the aftermath of 9/11', in Colin J. Bennett and Kevin D. Haggerty, *Security Games: Surveillance and Control at Mega-Events* (Oxford: Routledge, 2011)

objectives, and that the system of public-private interaction which emerged was only one factor amongst many in potentially accounting for the growth in the Olympic security budget. Finally, the extensive involvement of companies in London 2012's security arrangements clearly strengthens the notion that an 'industrial-complex' of a different character to the defence sector exists, and that private sector engagement is now a crucial element of the non-military CT aspects of the UK's national security strategy.

### **5.1 Government policy approach and governance arrangements**

When the UK won the right to host the thirtieth Olympic Games, on 6 July 2005, the Government immediately inherited the responsibility of ensuring a 'safe and secure' London 2012 in accordance with the requirements of the 'Host City Contract' it signed with the International Olympic Committee (IOC). This security policy ownership was clear from the outset - the security chapter within London 2012's original bid document explains, for example, that '[u]ltimate responsibility for security at the Games will belong to the UK Government in the form of the Home Office'<sup>14</sup>; this was later reiterated in the Olympic and Paralympic Safety and Security Strategy.<sup>15</sup> In implementing the strategy, the aim of which was '[t]o deliver a safe and secure Games, in keeping with the Olympic culture and spirit'<sup>16</sup>, the Government was clear that, whilst a wide range of 'key partners'<sup>17</sup> would be involved, it 'owned' ultimate responsibility for Olympic security.

If 'one of the thorniest aspects of security is its governance'<sup>18</sup> under normal circumstances, this was particularly so for London 2012. The challenges of security

---

<sup>14</sup> London 2012, *Candidature File: Volume 3 - Theme 12* (2004), p.31

<sup>15</sup> The 'guarantees' for security that the Government provided to the IOC are outlined in the Olympic security strategy. Home Office, 'London 2012 Olympic and Paralympic Safety and Security Strategy', July 2009, Via: <http://webarchive.nationalarchives.gov.uk/20100407094535/http://security.homeoffice.gov.uk/news-publications/publication-search/olympic-security/olympic-strategy.html> (accessed 23.04.12), p.3

<sup>16</sup> Ibid. p.7

<sup>17</sup> Ibid. p.16

<sup>18</sup> Zedner, *Security*, p.143

coordination around such major events have been well documented<sup>19</sup>, and it is in this context that the Government detailed the roles and responsibilities of the many contributors in its (published) Olympic security strategy.<sup>20</sup> Reflecting (perhaps even increasing) the complexity, London 2012's security governance arrangements underwent significant alterations between 2004 and the actual event. For example, it was decided immediately after London's bid was successful that an 'Olympic Security Directorate' - the main anticipated coordinating mechanism for the Games' security - should no longer reside inside the Organising Committee's structures as proposed by the bid document, and that it should be coordinated by the authorities under the leadership of a new 'Olympic Security Coordinator' lead by a senior police officer.<sup>21</sup> Furthermore, the decision in December 2008 to 'move the OSD [Olympic Security Directorate] from the Metropolitan Police to the OSCT'<sup>22</sup> was arguably even more significant because it clarified that the Government (rather than the police) had responsibility for security policy. Whilst earlier agreement of these governance arrangements would have been preferable, this decision was widely welcomed amongst the UK security policy community, including for example by the HASC.<sup>23</sup> After a period of some uncertainty, there was finally no doubt that the Home Office headed the governance structure for London 2012 security.

---

<sup>19</sup> Keith Weston, 'The challenge of inter-agency coordination' in Richards et al, *Terrorism and the Olympics*, pp.180-207

<sup>20</sup> Home Office, 'London 2012 Olympic and Paralympic Safety and Security Strategy', pp.14-18

<sup>21</sup> The first holder of the position was Assistant Commissioner Tarique Ghaffur, who it was reported subsequently deeply resented losing the role. See, for example, Vikram Dodd, 'Fresh pressure on Met chief Blair as top Asian police officer sues force over alleged racial discrimination', *The Guardian*, 19 August 2008, Via: <http://www.theguardian.com/politics/2008/aug/20/police.race> (accessed 11.08.14)

<sup>22</sup> Home Affairs Select Committee, 'Project CONTEST: The Government's Counter-Terrorism Strategy', Ninth Report of Session 2008-2009, June 2009, Via: <http://www.publications.parliament.uk/pa/cm200809/cmselect/cmhaff/212/212.pdf> (accessed 23.04.12), p.17

<sup>23</sup> *Ibid* p.18



Within this framework, the Government envisaged that the private sector had crucial roles to play in the strategy. It articulated its position within the Olympic security strategy as follows:

The Strategy will require close cooperation with industry and the private security sector across a range of issues. Communicating the Strategy to these sectors, and providing a clear statement of coordinated and consistent capability requirements, will be vital.<sup>24</sup>

Whilst no additional details were provided on *how* it was that industry would so vitally help to secure the Games, the strategy was explicitly clear that it depended to a certain extent on the private sector. After reviewing the growth in Olympic security budget, this chapter analyses the origins and character of the public-private interactions that emerged.

## 5.2 Security expenditure

Controversies around the ‘mushrooming security cost of the Games’<sup>25</sup> have regularly appeared in discussions around the Olympics. Indeed, the security budgets associated with this rising industry have grown strikingly; it has been noted that ‘mega-events offer a bonanza of growth opportunities’<sup>26</sup>, and recorded that whereas for the Sydney Olympic Games \$180million was spent on security operations this rose to an estimated \$1.5billion for Athens 2004.<sup>27</sup> In short, the steady post-9/11 increase in security costs for major events has been expertly documented<sup>28</sup> and it is now widely accepted that ‘the cost burden of providing security at such events has risen dramatically.’<sup>29</sup> Despite this context, sharp criticism was levelled towards the high and growing security costs associated with London

---

<sup>24</sup> Home Office, ‘London 2012 Olympic and Paralympic Safety and Security Strategy’, p.11

<sup>25</sup> Will Jennings, ‘Governing the Games’, p.148

<sup>26</sup> Adam Molnar and Laureen Snider, ‘Mega-events and mega-profits: Unravelling the Vancouver 2010 security-development nexus’ in Bennett and Haggerty, *Security Games*, p.158

<sup>27</sup> Ibid. For a table of Olympic security spending since 1984, see Houlihan and Giulianotti, ‘Politics and the London 2012 Olympics’, p.707

<sup>28</sup> Richard Giulianotti and Francisco Klauser, ‘Security Governance and Sport Mega-events: Toward an Interdisciplinary Research Agenda’, *Journal of Sport and Social Issues*, Vol.34:1 (2010), p.50

<sup>29</sup> Hinds, ‘Fortress Olympics’, p.20

2012.<sup>30</sup> This section provides a short analytical overview of the increasing levels of security funding that were associated with the Games.

Whilst the level of funding that London's original Olympic bid document envisaged for security would later cause consternation as a result of its eventual under-estimation, it was at least quite transparent. In addition to the £20m that London's Candidature File stated would be allocated to security by the Organising Committee<sup>31</sup>, public funding amounting to £190million was earmarked for Olympic security prior to the successful bid's submission.<sup>32</sup> Following London's victory, and 7/7 which immediately followed it, the Government completed a review of the Olympic Budget and announced a revised public sector package in March 2007. This included an additional allocation of £600m for 'wider policing and security' costs (with a further £238m contingency), and a revised Olympic Delivery Authority (ODA) security budget of £301 for 'security for venue construction' (with a further £53m contingency).<sup>33</sup> The reasons for the increases have attracted some speculation.<sup>34</sup>

It is important to clarify (as far as possible) the 'final' status of the Olympic security budget; this is a difficult task as budgets lay in different areas and constantly changed. For example, according to the Department of Culture, Media and Sport's June 2012 'Quarterly

---

<sup>30</sup> See, for example, Simon Jenkins, 'How Londoners can survive the Olympics', *London Evening Standard*, 26 July 2011, Via: <http://www.thisislondon.co.uk/standard/article-23973146-how-londoners-can-survive-the-olympics.do> (accessed 20.01.12)

<sup>31</sup> London 2012, *Candidature File: Volume 1 - Theme 6* (2004), p.103. 'Security' appeared in the bid document's budget as '\$37 million' and has been converted here in approximate historical prices. Conversion completed at: <http://www.x-rates.com/> (accessed 28.08.12)

<sup>32</sup> National Audit Office, 'Preparations for the London 2012 Olympic and Paralympic Games - Risk assessment and management', 2 Feb. 2007, Via: [http://www.nao.org.uk/publications/0607/preparations\\_for\\_the\\_olympics.aspx](http://www.nao.org.uk/publications/0607/preparations_for_the_olympics.aspx) (accessed 24.04.12), p.14

<sup>33</sup> DCMS, 'London 2012 Olympic Games and Paralympic Games Annual Report', January 2008, Via: [http://webarchive.nationalarchives.gov.uk/+http://www.culture.gov.uk/images/publications/dcms\\_goeannualreportjan08vs3update.pdf](http://webarchive.nationalarchives.gov.uk/+http://www.culture.gov.uk/images/publications/dcms_goeannualreportjan08vs3update.pdf) (accessed 24.04.12)

<sup>34</sup> Fussey et. al. suggest that the perception London's bid was going to fail led to a 'decision not to thoroughly cost the security requirements'. They also attribute significance to 'the separation of security costs' from the bid document. Pete Fussey, Jon Coaffee, Gary Armstrong and Dick Hobbs, *Securing and Sustaining the Olympic City: Reconfiguring London for 2012 and Beyond* (Farnham: Ashgate Publishing, 2011), p.118

Report' on the progress of the Games, it was stated that the ODA's security costs amounted to £277m.<sup>35</sup> Furthermore, the Home Office stated in December 2010 that it believed that 'it should be possible to deliver the core cross Government safety and security programme for about £475m.'<sup>36</sup> Whilst this would seem to be an attractive reduction, the Department was equally clear that it would retain the ability to draw on the original £600m figure if necessary, including the associated £238m contingency as appropriate. In addition, the security costs that were separately 'owned' by LOCOG for venue security increased substantially in the course of the project, and were only clarified with the announcement in late 2011 of an anticipated and substantial £553m publicly-funded grant.<sup>37</sup> According to a February 2012 report of the PAC, this sum would cover (amongst other items) the main G4S security contract (originally amounting to £284m) and the costs of the military's contribution to venue security for the Games (£48m).<sup>38</sup> Whilst the subsequent contract failure meant that the military's contribution towards venue security would increase substantially - thereby directing significant additional Olympic Security costs to the MOD budget - no rise in the overall budget would be expected as a result of G4S's acceptance of 'its responsibility for the additional cost of the increased military deployment resulting from the shortfall in workforce delivery.'<sup>39</sup> Furthermore, in

---

<sup>35</sup> This comprised £228m for 'security for park construction' and £49m for 'security screening and operational areas'. DCMS, 'London 2012 Olympic and Paralympic Games - Quarterly Report', June 2012, Via: [http://www.culture.gov.uk/images/publications/DCMS\\_GOE\\_QR\\_JUNE-2012.pdf](http://www.culture.gov.uk/images/publications/DCMS_GOE_QR_JUNE-2012.pdf) (accessed 03.09.12), p.17

<sup>36</sup> Home Office, Written Ministerial Statement, 'Allocation of grants to police authorities in England and Wales', 13 Dec. 2010, Via: <http://www.homeoffice.gov.uk/publications/about-us/parliamentary-business/written-ministerial-statement/allocations-police-england-wales?view=Binary> (accessed 23.04.12)

<sup>37</sup> DCMS, 'London 2012 Olympic and Paralympic Games - Quarterly Report', December 2011, Via: [http://www.culture.gov.uk/images/publications/DCMS\\_GOE\\_QR\\_Dec\\_2011.pdf](http://www.culture.gov.uk/images/publications/DCMS_GOE_QR_Dec_2011.pdf) (accessed 11.01.12), p.11

<sup>38</sup> Committee of Public Accounts, 'Preparations for the London 2012 Olympic Games and Paralympic Games', Seventy-fourth Report of Session 2010-12. 29 Feb. 2012, Via: <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1716/1716.pdf> (accessed 24.04.12)

<sup>39</sup> G4S, 'Statement regarding the Olympic Games Security Contract', 13 July 2012, Via: <http://www.g4s.com/en/Investors/News%20and%20Presentations/Regulatory%20Announcements/2012/07/13/Olympic%20Games%20Security%20Contract/> (accessed 27.08.12)

September 2012, LOCOG explained that the contract had been reduced from £284m to £236m, and that the 'final' sum to be paid to G4S would be subject to negotiation<sup>40</sup>; it was eventually announced in February 2013 that G4S would receive £204m in revenue for its services<sup>41</sup>, and that, overall, it would eventually make a total loss of £88m as a result of the contract.<sup>42</sup>

It may never be possible to accurately state the full, 'final' overall Olympic security budget for London 2012; whilst certain costs have been published, as shown above, the investment made in support of London 2012 by the Intelligence Services and the military, for example, have not been published in full. However, on the basis of the available figures, one can conclude that it easily amounted to around £1.2bn.<sup>43</sup> Having established this context, the following section analyses the private sector's involvement in the strategy and the extent to which any 'industrial-complex' impacted upon London 2012's security arrangements.

### 5.3 Public-private security interactions

Analysis of academic literature, available Government documentation, company press releases, media reports, employment advertisements and trade publications relating to

---

<sup>40</sup> Alan Travis and Owen Gibson, 'G4S failed to understand size of Olympic security job, says Lord Coe', *The Guardian*, 11 Sept. 2012, Via: <http://www.guardian.co.uk/business/2012/sep/11/g4s-failed-olympic-security-lord-coe> (accessed 14.09.12)

<sup>41</sup> 'G4S plc Annual Report and Accounts 2012', Via: [http://www.g4s.com/~media/Files/Annual%20Reports/g4s\\_annual\\_report\\_2012.ashx](http://www.g4s.com/~media/Files/Annual%20Reports/g4s_annual_report_2012.ashx) (accessed 11.08.14), p.83

<sup>42</sup> Gill Plimmer and Jonathan Moules, 'G4S takes £88m hit for Olympics fiasco', *Financial Times*, 12 February 2013, Via: <http://www.ft.com/cms/s/0/73df1bae-74e9-11e2-8bc7-00144feabdc0.html#axzz3A7clDdfN> (accessed 11.08.14)

<sup>43</sup> According to the DCMS's final 'quarterly report' on London 2012, security costs included £455m for the policing and wider security programme and £514m for venue security (this preceded the final, negotiated figure for G4S, which reduced the value of its revenue on the contract by a further £32m). In addition, £272m was spent by the ODA on its security budget; this comprised £224m for 'security for park construction' and £48m for 'security screening and operational areas'. Department of Culture Media and Sport, 'London 2012 Olympic and Paralympic Games - Quarterly Report', October 2012, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/78251/DCMS\\_GO\\_E\\_Quarterly\\_Report\\_Q3.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78251/DCMS_GO_E_Quarterly_Report_Q3.pdf) (accessed 11.08.14)

London 2012 security reveals an extensive network of public-private security relationships, supporting the notion that a system of a different character to the MIC exists in the non-military, CT-related aspects of contemporary UK national security strategy. The major interactions (contracts, engagements, or strategic partnerships) that emerged between the public and private sectors for the Games are detailed below; particular attention is first given in the 'security suppliers' category to the example of the G4S security contract.

### **Case Study: G4S Olympic Security Contract**

London's Olympic bid document, submitted to the IOC in November 2004, always envisaged that manpower-related security services provided by the private sector would be utilised to protect visitors, participants and London 2012 venues at the Games.<sup>44</sup> Nearly six years later, in March 2011, it was announced that G4S Secure Systems had been appointed as the London 2012 Games Organisers' 'Official Security Services Partner', and that the company would thus take responsibility 'for recruiting, training and managing the 10,000-strong security workforce that will be tasked with securing the Games.'<sup>45</sup> At the time, the Chairman of LOCOG, Lord Coe, proudly announced that this 'partnership' with G4S built on the earlier contract the company had signed with the ODA to secure the Olympic Park site during the construction phase of the project.<sup>46</sup> There certainly seemed to be confidence at the highest level that G4S was suitable for the task.

The evolution in the monetary value of G4S's contract has proven to be difficult to ascertain; after all, neither LOCOG's (publicly-subsidised) security service contract nor many of its specific details have ever been published. Nevertheless, prior to the contract

---

<sup>44</sup> The London 2012 Olympic Bid estimated that '6,500 private security staff would be required'. London 2012, *Theme 12, London 2012 Candidature File*, p.39

<sup>45</sup> London 2012, 'London 2012 secures G4S as Games Sponsor', 21 March 2011, Via: <http://www.london2012.com/press/media-releases/2011/03/london-2012-secures-g4s-as-sponsor.php> (accessed 11.01.12)

<sup>46</sup> G4S plc, 'G4S - Delivering the Games', G4S Corporate Video, 21 October 2011, Via: <http://www.youtube.com/watch?NR=1&v=6sgDdPDLOTQ&feature=endscreen> (accessed 11.01.12)

unravelling, LOCOG's Chief Executive indicated to the PAC in December 2011 that he expected G4S would receive just over £300m for the deal.<sup>47</sup> As is now well documented, it was also revealed during the same month that at peak times around 23,700 security guards (instead of the 10,000) would in fact be required<sup>48</sup>, resulting in LOCOG having to re-write the requirement of its original contract (which G4S subsequently agreed to) and, of course, more extensive military involvement.<sup>49</sup> Notwithstanding the £50m loss that in August 2012 G4S announced it expected to make because of its inability to meet the upgraded requirement<sup>50</sup>, and the eventual reduction of the value in revenues of the contract to £204m as stated above, this remained the largest private security service contract for London 2012. Despite the contract failure, G4S would later state that it provided around 8,000 officers at peak times<sup>51</sup>; this speaks volumes of the extent to which the State was content for a core element of the Games' security provision to be outsourced.

The question of who was 'to blame' for the failure to provide the required number of security guards was subject to considerable media speculation in the lead up to London 2012, and subsequently after the Games. G4S accepted failure on its part with a public

---

<sup>47</sup> Committee of Public Accounts, 'Uncorrected transcript of oral evidence taken before the Public Accounts Committee on Managing Preparations for the Olympics'. 14 Dec. 2011, Via: <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/uc1716-i/uc171601.htm> (accessed 11.01.12). As indicated above, it was subsequently twice confirmed that the size of contract would be revised downwards to £284m and £236m respectively.

<sup>48</sup> Owen Gibson, 'London 2012 organisers: security estimate was a 'finger in the air exercise'', *The Guardian*, 14 Dec. 2011, Via: <http://www.guardian.co.uk/sport/2011/dec/14/london-2012-security-estimate-cost> (accessed 11.01.12)

<sup>49</sup> This was explained by a speaker at a seminar titled 'Military Aid to the Private Authorities?', hosted by the Private Military and Security Research Group (PMSRG) at King's College, London, on 3 May 2012.

<sup>50</sup> G4S plc, 'G4S H1 2012 results', 28 Aug. 2012, Via: <http://www.g4s.com/en/Investors/News%20and%20Presentations/Regulatory%20Announcements/2012/08/28/G4S%20H1%202012%20results/> (accessed 29.08.12)

<sup>51</sup> G4S plc, 'Half yearly results announcement for the six months ended 30 June 2012', 28 Aug. 2012, Via: <http://www.g4s.com/~media/Files/Investor%20Relations%20documents/Results%20Announcements/2012%20interims%20announcement%20combined%20Final.ashx> (accessed 29.08.12), p.5

apology<sup>52</sup>, and notoriously when its Chief Executive, Nick Buckles, stated when providing evidence to the HASC that he ‘could not disagree’ that the episode represented a ‘humiliating shambles’ for the company.<sup>53</sup> Subsequently, G4S received the lion’s share of the criticism, even if it has been argued (including by the present author) that the Government was not a marginal player in the affair.<sup>54</sup> Whilst it is tempting to further examine the causes and seek to identify the ‘culprits’ (as some journalistic accounts have done<sup>55</sup>), a more sensible question for this thesis in the context of its inquiry into the existence of any dynamics associated with the MIC in the CT sector, however, is around what accounted for the character, size, and growth of the contract. To answer this, a greater understanding is needed of how an additional 8,400 security officers came to be needed and why the size of the contract grew so substantially from £86m in 2010 to £284m in 2011.<sup>56</sup>

Whilst there has never been any suggestion that G4S played a direct role in formulating the revised, larger requirement, it can be observed that the contractor was appointed as LOCOG’s ‘Official Security Services Provider’ ten months before the revision and, indeed, that LOCOG was the first Olympic organiser in history to offer a sponsorship arrangement in this new, bespoke ‘security service’ category; a relationship obviously existed between the supplier and its client. However, unlike the ‘category exclusivity’<sup>57</sup>

---

<sup>52</sup> ‘G4S Security boss: “We are sorry and bitterly disappointed”’, *BBC News*, 14 June 2012, Via: <http://www.bbc.co.uk/news/uk-18840185> (accessed 06.09.12)

<sup>53</sup> ‘MPs: G4S Olympics security is a “humiliating shambles”’, *Channel 4 News*, 17 July 2012, Via: <http://www.channel4.com/news/mps-g4s-olympics-security-is-a-humiliating-shambles> (accessed 29.08.12)

<sup>54</sup> Hugo Rosemont, ‘Reassessing the G4S Olympic security affair’, *Defencemanagement.com*, 3 Oct. 2012, Via: [http://www.defencemanagement.com/feature\\_story.asp?id=20939](http://www.defencemanagement.com/feature_story.asp?id=20939) (accessed 05.10.12)

<sup>55</sup> See, for example, Nick Hopkins and Owen Gibson, ‘Olympics security bill: how it soared to more than £1bn’, *The Guardian*, 9 March 2012 Via: <http://www.guardian.co.uk/sport/2012/mar/09/olympics-security-bill-how-it-soared> (accessed 07.05.12)

<sup>56</sup> Committee of Public Accounts, ‘Preparations for the London 2012 Olympic Games and Paralympic Games’, p.3

<sup>57</sup> IOC, ‘The Worldwide Top Partners’, IOC Website, Via: <http://www.olympic.org/sponsors> (accessed 23.09.12)

provisions that are contained in the most valuable Games sponsorship categories - i.e. those which both allow company sponsors to market themselves exclusively within their service area and, if they so wish, benefit from a 'first right' to supply requirements emerging in their sponsorship category - the CEO of LOCOG explained to the HASC in September 2012 that the (nearly) £5m that G4S paid for sponsorship was for 'marketing rights'<sup>58</sup> and that the deal was treated *separately* to the supply contract.<sup>59</sup> Whilst these arrangements were consistent with the rights associated with any other deal of such value within an Organising Committee's domestic sponsorship programme<sup>60</sup>, the complicating factor in the case of the G4S contract is that (as shown above) it was the Government, not LOCOG, who provided the funding for it. That there was a complicated system of public-private interaction around the G4S contract cannot be disputed.<sup>61</sup>

This is not to suggest that, following its appointment by LOCOG, G4S was in any way involved in the shaping of the revised, larger requirement; no evidence was found in the course of this thesis that it did. By contrast, one industry executive suggested on the condition of anonymity that G4S may actually have been reluctant to agree to deliver the late, revised requirement.<sup>62</sup> The idea that the company may have been *pressured* into fulfilling the revised contract at first seems possible in view of the late identification of the additional requirement and the strong view that G4S could have fulfilled the contract; in the words of the Head of Security Operations at LOCOG, Andrew Amery, 'G4S were best

---

<sup>58</sup> Home Affairs Select Committee, 'Olympics Security', Seventh Report of Session 2012–13. 21 Sept. 2012, Via: <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmhaff/531/531.pdf> (accessed 21.09.12), p.4

<sup>59</sup> Travis and Gibson, 'G4S failed to understand'

<sup>60</sup> These rights are explained in Alastair Ruxton, 'Structure of the Olympic Movement, the Paralympic Movement and London 2012' in Adam Lewis and Jonathan Taylor (Eds.), *Sports Law and Practice - 2<sup>nd</sup> Edition* (Haywards Heath: Tottell, 2008)

<sup>61</sup> As noted in Chapter 7, the Home Office also seconded an official into G4S before the Games.

<sup>62</sup> The interviewee suggested; 'G4S came back and said: 'we can't do that'. Government said: 'well, you're going to have to.'" Interview, Industry Executive



placed to deliver this following the increase in requirement<sup>63</sup>. Having said this, Amery also emphasised that the company ultimately entered into the revised contract willingly:

G4S always understood the risks from the outset of the sponsorship process, I do not believe they would have signed unless they were either totally content with the deal or had some form of 'guarantee' from the government... which clearly they did not!<sup>64</sup>

This explanation certainly seems plausible; even if questions remain around how hesitant G4S may have initially been in respect of delivering the revised requirement at such short notice.

The extent to which any system of public-private (and potentially wider) interaction - what has been labelled as 'the SIC' - directly affected or resulted in the growth of the Olympic security budget generally, or indeed the rising costs and failure of the G4S contract itself, is worth further examination; data is available to show how some companies may have contributed towards the plans being established on shaky foundations. In particular, it is surprising that private sector consultancies were so influential in being contracted to both make an early estimate of the 'true' costs of London 2012 security, and to actually assess LOCOG's security personnel requirements. With regards to the former, Jennings explains that a 2002 Arup study on the feasibility of a London Olympic bid estimated the total costs of security to be worth £160.2m<sup>65</sup>; that this figure appears to so closely resemble the stated original budgetary estimate included in the official bid document might suggest that it was considered as 'received wisdom', and accepted with too little scrutiny. Whilst the time pressures associated with submitting an Olympic bid should not be underestimated, the extent to which the financial estimate was 'off target' should raise questions over whether it could ever be appropriate for the findings of a private company to potentially form the statistical basis of such an important

---

<sup>63</sup> Written correspondence, Andrew Amery, August 2014

<sup>64</sup> Ibid.

<sup>65</sup> Jennings, 'Governing the Games', p.156

security budget. The present author's involvement in London's 2012 Olympic bid should not make these observations any more or less prescient.

More significantly, the leading management consultancy firm, Deloitte, publicly associated itself with the development of 'a functional model to help LOCOG fully understand the security personnel (private security and stewarding) requirements across 34 venues'<sup>66</sup>; a corporate brochure available on its website before the Games explained how it identified that 'up to 5,000 private security staff will be needed for in-venue security.'<sup>67</sup> Whilst the full size and scope of the Games' security requirements might not have been understood at the time the assessment was completed, it is evident from the final manpower resourcing figures (cited above) that Deloitte's version of the estimate turned out to be remarkably inaccurate. In light of the late, increased requirement (and thus significant budget growth) so clearly contributing to at least the context for the failure of the G4S contract, it might legitimately be asked whether it was appropriate to task a private sector company with the completion of such an important assessment, and what mechanisms of oversight existed to monitor their work.

Interviews have suggested that other unusual dynamics existed around the approach to assessing the manpower security requirement for London 2012. The Project Lead on Olympic Security for the BSIA trade association recalled, for example, how work on scoping the requirement actually began in collaboration with industry in 2007/8:

We talked about scoping the requirement. And we did. The industry spent time (...) doing that. We developed a template with the concept that as information became available it could be fed into the template. I believe that that was a very sensible thing to do, as it would inform planning and

---

<sup>66</sup> Deloitte, 'The State of Play: our journey to London 2012 and beyond', Issue 1, 2009, Via: <http://www.deloittelondon2012.co.uk/london-2012/the-state-of-play/issue-1-our-journey-to-london-2012-and-beyond> (accessed 12.01.12), p.20

<sup>67</sup> Ibid.

provide a timely specification for numbers and duties. There would have been no surprises.<sup>68</sup>

That such activity was completed for LOCOG free of charge might raise some eyebrows. According to Evans, however, it was the fact that the work was discontinued that was most significant; indeed, it can easily be seen how it contributed to the serious problems that eventually transpired. In a potentially damning revelation of the performance of the consultants operating inside LOCOG, he stated:

The fact that later down the line it [the scoping exercise] was stopped by the consultants within LOCOG (...) removed the only method to deliver the specification in good time and this led to the very late delivery of the requirement.<sup>69</sup>

The idea that the modelling was not adequately completed was suggested by two other individuals interviewed for this thesis. According to one industry executive familiar with the G4S contract:

...they did change the requirement for the Olympics because there was... there was a mistake with the modelling about how many security guards were needed. And so suddenly they had to boost their number of recruits. Suddenly they had to go flying up, and they obviously weren't set up to do it.<sup>70</sup>

Were there to be any doubt that the modelling was mishandled, another industry official identified the problem: '...the models Deloitte used were incorrect'<sup>71</sup>. To date, there appears to have been no public admission - by LOCOG, Deloitte or anyone else - around the possibility that the work conducted around the scoping of the manpower security requirement for London 2012 venues was deficient, and that this shortcoming might have contributed to the subsequent problems.

Whatever the precise roots of the difficulties, and who was to blame for them, the failure to identify an accurate requirement can now be seen as an extremely costly

---

<sup>68</sup> Interview, David Evans

<sup>69</sup> Ibid.

<sup>70</sup> Interview, Industry Executive

<sup>71</sup> Interview, Mark Phillips

mistake, to put it mildly. According to Evans, the need in the manpower sector of the security industry to identify the true requirement at the earliest possible stage is always ‘the most important thing of all’<sup>72</sup>; in this case it ‘was incredibly late being delivered’<sup>73</sup>. It is hard to see how the fact that a ‘final’, more accurate requirement was not identified and resolved at an earlier stage than December 2011 - incredibly, just six months before the actual deployment - could not have contributed to the difficulties which were encountered with the G4S Olympic security contract.

At the risk of repetition, there is no dispute that G4S entered into the revised contract (i.e. including the additional requirement) freely; it can even be suggested (as it was in the final report of the HASC<sup>74</sup>) that the company displayed an over-confident, even arrogant attitude towards its ability to deliver what was obviously a challenging requirement in such a short period. It was certainly apparent from his evidence to the HASC that Nick Buckles believed it would not present difficulties; indeed he claimed that ‘...we felt we were the only company able to do it[.]’<sup>75</sup>

From the available information, therefore, the company clearly (mistakenly) felt that it could meet the additional need. This chapter does not seek to excuse G4S for its clear contributions towards the failure: one industry interviewee summarized the situation well as follows:

There was a feeling of unfairness because of the late, larger requirement inflicted upon them by the Home Office. So I feel certain sympathy for G4S. Notwithstanding that, they made some of their own mistakes.<sup>76</sup>

---

<sup>72</sup> Interview, David Evans

<sup>73</sup> Ibid.

<sup>74</sup> The HASC report strongly criticized the public pronouncements of one G4S Director (who subsequently lost his job) in the run up to the Games as follows: ‘...Mr. Horseman-Sewell was boasting recklessly in the press that G4S would have been more than capable of simultaneously delivering multiple Olympic security projects around the world.’ HASC, ‘Olympics Security’, p.9

<sup>75</sup> HASC, ‘Olympics Security’, Volume II, Ev 5

<sup>76</sup> Interview, Shaun Hipgrave

Another industry executive was less sympathetic, suggesting that the company may have been engaged in a ‘conspiracy of optimism’ and that, with regards to its actual inability to deliver, G4S ‘...probably should have come clean about it a lot earlier’<sup>77</sup>. Whatever G4S’s actual outlook and the causes of the late identification of the issue, it is clear that the failure to earlier recognise the shortfall proved to be a low point of an episode that G4S’s CEO obviously clearly regretted.<sup>78</sup>

Whilst engaging in ‘blame games’ is undesirable, it is hard to see, however, how the primary responsibility for identifying the manpower security requirement for London 2012 venues could have fallen to anyone other than LOCOG and/or Government. It is of some concern, therefore, that it has been suggested that this work was outsourced to commercial consultants. The extent to which any such consultants may have been considered as being an integral part of the organising committee’s structures should not distract from a more fundamental point; it would be worrying were it to genuinely emerge that it was neither LOCOG nor the Government, but an embedded consultancy firm who not only made (as seems to have transpired) an under-estimate of the requirement, but who potentially more damagingly may have actually made the decision not to properly complete such important modelling work.

Furthermore, it might also be asked why it was that the authorities decided to only initially contract 2,000 new staff from G4S in light of the earlier, manpower security assessments of 6,500 in the original Olympic bid document<sup>79</sup>, and the 5,000 later publicised by Deloitte (however flawed either of these may have been, and notwithstanding the existence of a recruitment initiative designed to help meet the significant requirement<sup>80</sup>).

---

<sup>77</sup> Interview, Industry Executive

<sup>78</sup> In a stark admission, Nick Buckles explained to the HASC; ‘Clearly we regret signing the contract, but now we have to get on and deliver it.’ HASC, ‘Olympics Security’, Volume II, Ev 10

<sup>79</sup> See footnote 44.

<sup>80</sup> See ‘Wider Business’ section below for details on the ‘Bridging the Gap’ scheme.

Indeed, the apparent decision not to require G4S to recruit more new staff in view of these earlier assessments - and the eventual reality that an additional 8,400 security staff would be needed - can now be seen as a highly questionable decision. In retrospect, much more searching questions perhaps should have been raised over both the Home Office's and LOCOG's effectiveness in developing and overseeing the estimated requirement for, and the implementation of, the contract; it is hard to see how anyone other than these two organisations could have been responsible for doing so. Indeed, against this backdrop it can be suggested that the strength of both LOCOG's and the Home Office's monitoring of the scoping and delivery of the requirement - crucially in the context of (an unusually) high level of public subsidy that it was itself allocated for the contract - was lacking. As one industry official explained in an interview:

So [the] G4S [Olympic Security Contract] is a very good example of poor oversight by LOCOG and culpability coming in at the end as an excuse for Government. And actually there was poor commercial oversight, there was poor planning and there was poor preparation.<sup>81</sup>

It is surprising that in the HASC inquiry the performance of Government and LOCOG did not receive greater scrutiny; they were completely vindicated of any responsibility. Furthermore, the Government and others concerned seemed content to allow G4S to publicly receive the full blame for the contract failure - it is particularly noticeable, for example, that the Government's response to the HASC report declines to specifically address the Committee's finding that G4S was 'solely' to blame, stating its position as follows:

The Government welcomes the Committee's recognition of the hard work and achievements of that community and of the successful contingency planning that was able to deal effectively with problems that arose when G4S said that it was unable to meet its contractual obligations.<sup>82</sup>

---

<sup>81</sup> Interview, Industry Executive

<sup>82</sup> Government response to the seventh report from the Home Affairs Select Committee, Session 2012-13, HC531, Olympics Security, November 2012, Cm 8500, Via:

Whilst these statements are careful not to ‘point the finger’ at G4S directly, there is no doubt where the authorities believed the problems lay. The former Head of Security Operations at LOCOG explained to the author that ‘a better form of words could be used’ than those of the HASC in its assessment that G4S was ‘solely’ to blame, but nonetheless concluded:

The statement is factually true - they failed to deliver the contract that they (in my view/understanding) freely signed understanding the risks. They simply did not have the ‘back office capability’ to manage the workforce. That said, information would come through at last minute and the task was a massive one... but they said they could do it.<sup>83</sup>

There is no doubt that G4S mishandled its contract. However, as seen in regards to the involvement of consultancy firms in the IT contracts for e-Borders and FiReControl, the support provided by Deloitte in the preparation for the Olympic security contract appears to have been overlooked by those scrutinizing the contract, and now seems highly questionable. Having said this, it should be stressed that the company appears to have contributed to an *under-estimation* of the manpower security requirement - a not necessarily straightforward task<sup>84</sup> - rather than make any effort to over-specify or ‘gold plate’ the requirement; it is this latter dynamic which is most often presented as being associated with ‘the SIC’ or dynamics relating to Government contracts of such a large size. Either way, the contribution cannot be said to have been ideal. It is perhaps only slightly ironic that, after the failure of the contract became very publicly debated, G4S later appointed another private sector consultancy, PricewaterhouseCoopers, to review the causes of the contract failure.<sup>85</sup>

*Additional reasons for budgetary increases*

---

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/235984/8500.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/235984/8500.pdf) (accessed 12.08.14), p.1

<sup>83</sup> Written correspondence, Andrew Amery, August 2014

<sup>84</sup> Amery explained; ‘In theory the number of staff required for screening areas should be easy to assess. In reality it is not!’ Ibid.

<sup>85</sup> G4S plc, ‘Half yearly results announcement for the six months ended 30 June 2012’, p.6

In researching for this case study, it became clear that factors other than ‘the SIC’ contributed to both the rising costs and failure to fully deliver the G4S contract. Firstly, the change of Government following the 2010 General Election resulted in the development of a greater emphasis towards, and arguably a more limited appetite for risk around, the security preparations for the Games; including in particular the venue security arrangements. As one of her first acts, the coalition Government’s new Minister for Security, Lady Pauline Neville-Jones, completed an ‘audit and review’ of the Games’ security preparations and this identified the need for more focussed attention in certain areas.<sup>86</sup> The Minister’s special adviser prior to her appointment, Mark Phillips, explained how with respect to the plans for London 2012 ‘the issue at the top of my list was in-venue security numbers’ and that ‘we had known that it was an issue for a long time’<sup>87</sup>. It seems apparent, therefore, that the new Government already possessed an awareness of the difficulties. Its realisation that it would be responsible for overseeing the Games’ security operation - that it would occur ‘on its watch’ so to speak - obviously contributed to its decision to strengthen the arrangements significantly, including by increasing the budget for venue security.

Secondly, it can be suggested that the substantial increase in LOCOG’s security budget to meet the additional requirements for the G4S contract resulted at least partly from a lack of relevant experience existing in that organisation. Whilst the 2009 appointment of the former head of the British Transport Police, Sir Ian Johnston, as LOCOG’s Director of Security and Resilience may have reassured some in view of his stature and seniority, it has been argued by one individual with knowledge of the G4S contract that the retired policemen who were appointed to LOCOG in the latter years of

---

<sup>86</sup> Home Office, ‘Audit & Review of Olympic & Paralympic Safety & Security Planning: Summary’, November 2010, Via: <http://www.homeoffice.gov.uk/publications/counter-terrorism/olympics/audit-olympic-security-nov10> (accessed 07.05.12)

<sup>87</sup> Interview, Mark Phillips



planning had a limited understanding of the requirements of ‘force generation’.<sup>88</sup> Whilst at one stage (as explained in Chapter 7) LOCOG’s security team employed the services of a former G4S employee in order help with the management of the contract, the fact that its security leadership had limited experience of dealing with such contracts simply cannot have helped matters.

Finally, the 7/7 attacks and the wider security risk landscape meant that the threat posed by international terrorism to the UK was already ‘substantial’<sup>89</sup> at the time of the Games. As the Director-General of MI5 explained in speech shortly before London 2012; ‘[t]he Games present an attractive target for our enemies.’<sup>90</sup> The combination of an already heightened threat level with the potential attractiveness of an attack against the Games would, in itself, be a serious consideration for those deciding the security measures (and thus levels of investment) around them. According to Amery, high levels of Olympic security spending arose because:

London was always going to be an expensive Games in terms of security given the environment and threat level it took place in. Indeed the international terrorist threats have continued to grow in recent years which has seen proportionate increases in cost to mitigate this since 2001.<sup>91</sup>

Critics of the SIC might not accept the validity of the threat assessment, and the associated levels of spending therefore needed; it was nevertheless consistently articulated as the basis of the security plans (and expenditure) for London 2012.

---

<sup>88</sup> This was suggested at the PMSRG seminar titled ‘Military Aid to the Private Authorities?’ on 3 May 2012.

<sup>89</sup> A ‘substantial’ threat level in the UK system means that ‘an attack is a strong possibility’. Security Service, ‘What are threat levels?’, Via: <https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels/the-uks-threat-level-system/what-are-threat-levels.html> (accessed 03.09.12). The UK Government stressed repeatedly in advance of London 2012 that the authorities were basing their plans on an even higher threat level (‘severe’) occurring at the time of the Games.

<sup>90</sup> Jonathan Evans, ‘The Olympics and Beyond’, Lord Mayor’s Annual Defence and Security Lecture. 25 June 2012, Via: <https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html> (accessed 27.08.12)

<sup>91</sup> Written correspondence, Andrew Amery, August 2014

It is clear, then, that factors other than any influence exerted by the 'SIC' existed and thus may have contributed to the growth of both the G4S security contract, and the Games' security budget more generally. This is not to suppose that G4S or any other involved company might not have possessed the desire to do so; the evidence suggests, however, that the arrangements around the scoping and delivery of the contract in particular were much more chaotic, and that they suffered from considerable miscalculation, uncertainty and flux.

*A note on scrutiny and oversight*

The resulting failure of the G4S Olympic security contract deserved (and continues to deserve) to raise questions over the level and effectiveness of the regime of (internal and external) oversight around it; this is especially important in view of the apparently total surprise with which the Government and others greeted the last minute problems.<sup>92</sup> In so far as this matter relates to this thesis more broadly, it can be recalled that, in his warning on the MIC, Eisenhower considered that, at least in the US, the 'complex' thought of as a system included a legislative element; he even originally contemplated including the word 'congressional' within the original expression.<sup>93</sup> The argument put forward was that politicians and even Congress comprised a core element of the cosy, elite system which posed such a potentially damaging risk.

Applying this line of thinking to both the UK example - and, indeed, to the argument introduced in the opening chapters that the dynamics associated with the MIC have transferred into the non-military CT aspects of national security - it might be logical to expect that elements within the UK Parliament might have therefore welcomed increasing levels of Olympic security expenditure; perhaps especially when any components would

---

<sup>92</sup> Fussey has argued that the surprise which the Government greeted the failure was 'disingenuous'. Pete Fussey, 'Command, control and contestation: negotiating security at the London 2012 Olympics', *The Geographical Journal* (2013), p.10

<sup>93</sup> Ledbetter, *Unwarranted Influence*, p.107

clearly benefit private companies such as G4S. Whilst it was notably silent in its public commentary on, and scrutiny of, any aspect of the G4S security contract prior to the serious difficulties transpiring in July 2012, the reality is that Parliament was extremely critical of the company's performance once the problems emerged. The HASC in particular offered a devastating critique of G4S's involvement in Olympic security, conducting a swift inquiry into the episode shortly before the Games, and concluding in an associated, high profile report that the company was 'solely' to blame for the issues which transpired with the contract. It concluded in no uncertain terms:

The blame for G4S's failure to deliver on its contract rests firmly and solely with the company. There is no suggestion that LOCOG, the Home Office or anybody else involved in the process contributed to the problem in any way.<sup>94</sup>

At the time, few doubts were expressed over the validity of this conclusion<sup>95</sup>; the HASC report noted that even G4S accepted the verdict.<sup>96</sup> This chapter has already shown, however, that the requirements changed at a late stage, that the overarching governance arrangements for the contract (and Olympic security more generally) were incredibly complex, and that there was also an awareness in policy circles that there was an issue with delivering the requirement. That the HASC did not appear to wish to address the broader governance context for London 2012 security, especially in view of its remit for holding the Home Office to account, is baffling.

Perceptions within the security community were sought through interviews and written correspondence - both in the security industry and more broadly - around the appropriateness of the HASC's scrutiny on the G4S security contract; a number of

---

<sup>94</sup> HASC, 'Olympics Security', p.12

<sup>95</sup> Rosemont, 'Reassessing the G4S Olympic security affair', provides an alternative interpretation.

<sup>96</sup> The HASC stated that 'G4S has already acknowledged that it is solely responsible for its failure to deliver the Contract', *Ibid.* p.11

responses were striking. One senior industrialist welcomed the approach of the HASC and the manner in which Nick Buckles was scrutinised during the inquiry:

It was a great example of understanding where accountability lies. And the fact that the CEO of G4S was sitting there in the public glare, and being hammered, is a tribute to the process and the democratic and commercial engagement.<sup>97</sup>

Contrary views also existed, however. In an enlightening discussion on the HASC's handling of its Olympics Security inquiry, one interviewee was candid about the possible motivations of the Committee, and the manner in which it reached its conclusions:

...the select committee were always going to say it was all Nick Buckles' fault, because, you know, talking about contractual requirements doesn't interest Keith Vaz [the Chairman of the HASC], and it certainly doesn't make for a good media pitch. So I think he was obviously going to get the blame.<sup>98</sup>

Supporting this critical suggestion, Evans also reflected bluntly on the efficacy of the HASC's inquiry: '[That] ...was a disgrace as, in my opinion, it was shared equally between LOCOG and G4S and it was just too easy a route for the HASC to blame the private sector.'<sup>99</sup>

Whilst the politics of parliamentary scrutiny are certainly intriguing, the suggestion in this case that G4S may have been 'on a hiding to nothing' in so far as the Committee's deliberations were concerned is important to this thesis for two reasons. Firstly, it clearly illustrates how, whatever one thinks of the validity of the HASC's conclusions, the Committee felt no sense of duty to defend (as classical MIC theory applied to the 'wider security' arena might have it) the reputation of the UK's largest security company, G4S; any idea that any form of 'cosy' or worrying relationship might exist between the UK Parliament and this company therefore appears to be way off the mark. Secondly, by stark contrast, the fact that in this case the HASC declined to offer any criticism of the

---

<sup>97</sup> Interview, Robin Southwell

<sup>98</sup> Interview, Industry Executive

<sup>99</sup> Interview, David Evans

Government or LOCOG in the course of its inquiry - including up to and including its final report - is surprising in view of this chapter's analysis. Whether deliberately or inadvertently, that the HASC declined to scrutinise some of the other actors and obvious additional factors which may have contributed (if not further upstream) to the G4S security contract failure, as this chapter has sought to do, is worrying. Indeed it may even suggest that whilst G4S's influence on the requirement may have been minimal, representatives at least two corners of the 'classic' confluence of interests under examination in this study may have been too closely aligned for comfort.

### *Other suppliers*

Whilst considerable attention has been devoted to the largest private security contract for the Games, it is important to recognise that many other commercial security suppliers were involved in the London 2012 Olympic security strategy; the Games planners' interaction with equipment manufacturers was another crucial category of interaction. The ODA revealed in October 2009, for example, that to secure the main 'Olympic Park' in East London a 'host of security packages' had been awarded: these included the provision of access control systems by Reliance High-Tech, biometric systems by Human Recognition Systems, a range of screening equipment for pedestrian and vehicle entry by Rapiscan Systems, and CCTV and perimeter security systems by Honeywell Control Systems.<sup>100</sup> In addition, a search conducted on an online ODA 'Suppliers Map'<sup>101</sup> identified 23 dedicated security contracts, including the provision of a high profile perimeter fence that is '3.6 metres high with a power topping section on top'<sup>102</sup> supplied by Zaun Fencing.<sup>103</sup> Whilst

---

<sup>100</sup> London 2012, 'Biometric scanners enhance Olympic Park security as big build ramps up', 16 Oct. 2009, Via: <http://www.london2012.com/press/media-releases/2009/10/biometric-scanners-enhance-olympic-park-security-as-big-build-ramps-up.php> (accessed 11.01.12)

<sup>101</sup> Via: <http://www.london2012.com/get-involved/business-network/oda-suppliers/map.php> (accessed 11.01.12)

<sup>102</sup> London 2012, 'Olympic Park security set to increase as construction intensifies', 4 July 2008, Via: <http://www.london2012.com/press/media-releases/2008/07/olympic-park-security-set-to-increase-as-construction-intensifies.php> (accessed 12.01.12)

such contracts might seem typical of any such infrastructure project, the substantial number of them illustrates the extensive public-private interaction that existed. Indeed, such was the high level of corporate interest in the ODA's security contracts that the body organised an additional 'security industry day' for the large number of companies that were unable to attend the original event.<sup>104</sup>

There were other significant London 2012 security equipment contracts; it was announced in March 2011, for example, that, building on the success of its ODA contract, Rapiscan Systems had become 'Official Security Equipment and Systems Supplier' to LOCOG, and that it would 'provide over 2000 vehicle screening, people screening and baggage and parcel inspection systems to all Olympic venues.'<sup>105</sup> Whilst this might appear as a startling figure in its own right, the supply of capabilities extended beyond physical protective measures. The security of the Games' essential information technology systems was a key consideration, for example; Gilmore identifies that 'Atos Origin has the job of ensuring that results and communications IT is not compromised.'<sup>106</sup> Furthermore, it was announced on 8 July 2011 that Airwave would supply LOCOG with 'Apollo' - a private mobile radio service for over 18,000 staff and volunteers, including the security function - for the duration of the Games.<sup>107</sup> These were all lucrative contracts, illustrating the high level of security expenditure for London 2012 and the extensive network of public-private interactions around it.

---

<sup>103</sup> DCMS, 'First 2012 Cabinet meets at Olympic Park', 9 Jan. 2012, Via: [http://www.culture.gov.uk/news/news\\_stories/8758.aspx](http://www.culture.gov.uk/news/news_stories/8758.aspx) (accessed 14.01.12)

<sup>104</sup> Anthony Hildebrand, 'Olympic concerns', *SMT Online*, 25 Oct. 2007, Via: <http://www.ifsecglobal.com/olympic-concerns/> (accessed 03.09.12)

<sup>105</sup> London 2012, 'London 2012 signs Rapiscan as tier three sponsor', 10 March 2011, Via: <http://www.london2012.com/press/media-releases/2011/03/london-2012-signs-rapiscan-as-tier-three-sponsor.php> (accessed 11.01.12)

<sup>106</sup> Margaret Gilmore, 'Countdown to the Olympics', *RUSI Journal*, Vol.156:2 (2011), p.32

<sup>107</sup> Airwave, 'London 2012's Critical Communications Ready for Service', 8 July 2011, Via: <https://www.airwavesolutions.co.uk/media/news/article/london-2012s-critical-communications-ready-for-service/> (accessed 15.01.12)

A more sensitive private security capability for London 2012 was industry's supply of 'close protection' services to VIPs and athletes. As Evans explains, demand for these services around major events 'is often beyond the capacity of any nation's police force and the police are normally forced to ration such protection to those under the greatest threat[.]'<sup>108</sup> Whilst the full extent to which such private sector capability was utilised for London 2012 is not publicly available, a report by the All-Party Parliamentary Group on Specialist Security published shortly before the Games highlighted a concern around the absence of 'a formal system to monitor client demands for close protection.'<sup>109</sup> Despite one scholar previously suggesting that private military and security companies 'are not likely to be utilised for MES (Major Event Security) in the EU'<sup>110</sup>, a precedent may have been set for London 2012 because, in the run-up to the Games, the BSIA established a Close Protection Co-ordination Unit to put 'visiting dignitaries in touch with suppliers that work to the relevant British Standards for quality'<sup>111</sup>, writing to 'over 150 consulates, Ambassadors and High Commissioners' to advertise the capabilities of the sector.<sup>112</sup> It appears that the private sector's involvement in this area should not have been a surprise; Armstrong documents that Tarique Ghaffur suggested to the 2006 annual conference of the British Association of Private Security Companies that there could be opportunities for them to 'part police' the Games.<sup>113</sup> The supply of close protection services to London 2012 clients is evidence of another 'security industry' sub-sector being involved in the strategy.

---

<sup>108</sup> Evans, 'The role of the private security industry', p.173

<sup>109</sup> All Party Parliamentary Group on Specialist Security, 'VIP Security at the London 2012 Olympic & Paralympic Games', First Report of Session 2011-12. 11 July 2012, Via: <http://appgsecurity.com/downloads/VIPSecurityAtLondon2012OlympicGames.pdf> (accessed 02.09.12), p.5

<sup>110</sup> Frank Gregory, 'The European Union and the promotion of major event security within the EU area' in Richards et. al., *Terrorism and the Olympics*, p.220

<sup>111</sup> BSIA, 'New co-ordination unit matches VIPs with reputable Close Protection suppliers', BSIA Website, 3 July 2012, Via: [http://www.bsia.co.uk/M01W4033507/LY8WLW49550/new-Close-Protection\\_co-ordination-unit?backlinktype=newscentre&src=in\\_t](http://www.bsia.co.uk/M01W4033507/LY8WLW49550/new-Close-Protection_co-ordination-unit?backlinktype=newscentre&src=in_t) (accessed 30.12.14)

<sup>112</sup> 'BSIA launches Close Protection Unit for London 2012', Ifsecglobal.com, 3 July 2012, Via: <http://www.ifsecglobal.com/bsia-launches-close-protection-unit-for-london-2012/> (accessed 03.09.12)

<sup>113</sup> Armstrong, *War plc*, p.184

That so many security industry sub-sectors have been ‘hidden’ and comprise what this thesis looks upon as a much more multi-faceted ‘industrial-complex’ reflects how the concept has hitherto been under-researched.

Security consultancy extended beyond the completion of statistical analysis to include the design aspects of the Olympic Park; the company Buro Happold even received a ‘security excellence award’ in 2007 in part for its work on the ‘Security Master Planning’ for London 2012.<sup>114</sup> Furthermore, even more striking is the work that KPMG completed for the Home Office. The scale of its contract has become increasingly apparent: the department revealed in December 2010, for example, that KPMG was the third largest recipient of its consultancy funding during 2009 and 2010 for the work it was doing both on ‘Olympic Security and Value for Money.’<sup>115</sup> A search of the Home Office’s ‘transparency’ website revealed that the OSCT paid KPMG £294,343 in one month alone (June 2010).<sup>116</sup> Whether this use of private consultancy amounts to what O’Reilly calls ‘state-corporate symbiosis’<sup>117</sup> might be questionable; less debatable, however, is that it was an important component of the programme management for London 2012 security. Whilst the involvement of Deloitte in supporting LOCOG to produce a technical manpower requirement is one thing, the involvement of KPMG in such a prominent role at the Home Office - the Department responsible for overall policy - is arguably an entirely different matter. Following what can be seen as the detrimental involvement of consultants in the cases of e-Borders and FiReControl, it is remarkable how little attention has been paid to such similar dynamics emerging in the case of the security for London 2012. Perhaps it was

---

<sup>114</sup> Buro Happold, ‘SEA Article’, Buro Happold Website, Via:

<http://www.happoldsafesecure.com/CompanyAwards.aspx> (accessed 15.01.12)

<sup>115</sup> Home Affairs Select Committee, ‘Supplementary memorandum submitted by the Permanent Secretary, Home Office’, December 2010, Via:

<http://www.publications.parliament.uk/pa/cm201011/cmselect/cmhaff/626/626we06.htm> (accessed 15.01.12)

<sup>116</sup> Home Office, ‘Transparency Spend over £25,000’, June 2010, Via:

<https://www.gov.uk/government/publications/transparency-spend-over-25-000> (accessed 15.01.12)

<sup>117</sup> O’Reilly, ‘The transnational security consultancy industry’, pp.183-210



because the G4S contract affair did not tarnish the impression of the overall management of the Olympic security programme that the role of KPMG was not more deeply scrutinised. The jury is still out, however, over whether the appointment of such companies is (or should be) desirable.

The Government's intention to utilise existing UK security capabilities to support London 2012 security - to 'lamine' Olympic specific measures over existing national arrangements<sup>118</sup> - was clearly evident. Amongst the most prominent of these was the UK's border security capability<sup>119</sup> including the 'e-borders' programme; indeed, the Senior Responsible Owner of the UKBA's London 2012 programme articulated a strategy to draw on e-borders to deliver 'enhanced business as usual' in support of the Games.<sup>120</sup> The Government's separate major capability in this area, 'Programme Cyclamen', was also in operation at the time of the Games.

Other departments and agencies also invested in new capabilities for the Emergency Services before London 2012. In November 2009, for example, the Home Office announced a £39m investment to boost the capacity of the Airwave radio system in preparation for the Games.<sup>121</sup> Additionally, the MPS upgraded its police command and control capabilities to support the London 2012 security operation.<sup>122</sup> The capabilities of Endeleo and Electrosonic were used to establish a new 'Special Operations Room' for the

---

<sup>118</sup> Jon Coaffee, Pete Fussey and Cerwyn Moore, 'Laminated Security for London 2012: Enhancing Security Infrastructures to Defend Mega Sporting Events', *Urban Studies*, Vol.48:15 (2011), p.3316-3318

<sup>119</sup> Border Security arrangements featured within the PROTECT strand of the security plan. Home Office, 'London 2012 Olympic and Paralympic Safety and Security Strategy', p.20

<sup>120</sup> Defence IQ, 'UK Border Agency Director Says E-borders Is Ready For London 2012 Olympics', Defence IQ Podcast, Via: <http://www.defenceiq.com/army-and-land-forces/podcasts/uk-border-agency-director-says-e-borders-is-ready/> (accessed 15.01.12)

<sup>121</sup> Natasha Lomas, '£39m boost for London Olympics' emergency comms', *ZDNet.com*, 3 Nov. 2009, Via: <http://www.zdnet.com/article/39m-boost-for-london-olympics-emergency-comms/> (accessed 12.01.15)

<sup>122</sup> The Home secretary outlined a wide range of new investments in late 2011. Theresa May, 'Olympic Security Conference Speech', 21 Nov. 2011, Via: <https://www.gov.uk/government/speeches/home-secretarys-olympic-security-conference-speech> (accessed 15.01.12)

MPS<sup>123</sup>; its website states that it doubled its capacity '[t]o cope with the size and scale of the operation in 2012[.]'<sup>124</sup>

Finally, in addition to specific contracts, the Government developed more 'strategic' engagement with the security industry; working in particular with RISC. An analysis of the origins and activity of this body is presented in Chapter 6; suffice to say here that, in so far as London 2012 was concerned, Evans documents the creation of an Industry Advisory Group (IAG) co-chaired by the OSD and RISC, arguing that 'London 2012 is witnessing unprecedented involvement of industry in the planning and review process[.]'<sup>125</sup> This clearly serves as evidence of an exchange at the policy level between the public and private sectors in the Olympic security strategy, adding weight to the notion of the existence of an industrial-complex in the CT arena.

### ***Private Operators***

In addition to engaging the security suppliers' community, the Government also engaged private operators who were involved in London 2012 security. As highlighted by Gilmore, the event organiser (LOCOG) was itself a private company<sup>126</sup> - Evans stresses the importance of this as security was not the organisation's main driver<sup>127</sup> - and the Government's security strategy articulated the organisation's range of 'in-venue' security responsibilities.<sup>128</sup> In short, such was the importance of venue security to the success of the overall Games operation that the Government had an inter-dependent relationship

---

<sup>123</sup> Peter Gumm, 'New London CCTV Control Room designed to thwart terrorists', *SMT Online*, 7 Aug. 2007, Via: <http://www.ifsecglobal.com/new-london-cctv-control-room-designed-to-thwart-terrorists/> (accessed 20.01.12)

<sup>124</sup> Metropolitan Police Service, 'Met Command and Control', MPS Website, Via: <http://content.met.police.uk/Article/Met-Command-and-Control/1400005435512/1400005435512> (accessed 20.01.12)

<sup>125</sup> Evans, 'The role of the private security industry', p.170

<sup>126</sup> Gilmore, 'Countdown to the Olympics', p.28

<sup>127</sup> Evans, 'The role of the private security industry', p.165

<sup>128</sup> These included 'the safety of spectators at venues' and 'securing the field of play', for example. For a full list, see Home Office, 'London 2012 Olympic and Paralympic Safety and Security Strategy', pp.17-18

with LOCOG ever since London was awarded the Games. The allocation of a £553m state-funded grant to LOCOG for venue security can be understood in this context.

The CLM consortium<sup>129</sup> - the ODA's contractor for the delivery of the new Games venues - was also an important private operator of security for London 2012; it protected the Olympic venues during the construction phase of the project, and its Logistics and Security team even received a 'Considerate Constructors' award in 2011.<sup>130</sup> Furthermore, the private company Westfield - the owner and operator of East London's new shopping centre located adjacent to the Olympic Park - was an important contributor to the security plan; not least because it was always anticipated that 70% of spectators attending events in Stratford would pass through its site.<sup>131</sup> Indeed, reflecting its proximity to the main cluster of venues, LOCOG announced plans to operate vehicle screening from the Westfield shopping centre on 5 September 2011<sup>132</sup>; in a further development, Westfield was announced as an 'official sponsor' of the Games two days after this announcement.<sup>133</sup> There is no doubt that the security plan depended on the contributions of both CLM and Westfield, both of whom were private companies.

The significance of the role played by the IOC in any Olympic Games' security arrangements has been disputed - it has both been suggested, for example, that the 'IOC make clear in guidance to potential host cities that it is *their* responsibility to provide a safe environment'<sup>134</sup> and that 'security policy for the organisers of the Olympic Games is

---

<sup>129</sup> CLM comprised the companies CH2MHILL, Lang O'Rourke and Mace.

<sup>130</sup> Details via: <http://www.ccscheme.org.uk/index.php/site-registration/national-site-awards/search-for-award-winners> (accessed 29.12.14)

<sup>131</sup> Gilmore, 'Countdown to the Olympics', p.29

<sup>132</sup> London 2012, 'London 2012 confirms vehicle screening plans for Westfield shopping centre', 5 Sept. 2011, Via: <http://www.london2012.com/news/2011/09/london-2012-confirms-vehicle-screening-plans-for-westfie.php> (accessed 15.01.12)

<sup>133</sup> London 2012, 'London 2012 confirms Westfield as sponsor and hits £700m mark', 7 Sept. 2011, Via: <http://www.london2012.com/news/2011/09/london-2012-confirms-westfield-as-sponsor-and-hits-700m-.php> (accessed 15.01.12)

<sup>134</sup> Coaffee et. al., 'Laminated Security', p.3312 (Emphasis in original)

*dictated* by the IOC.<sup>135</sup> However, it is clearer that it is a private entity, operating in Switzerland, and possessing its own commercial perspective and priorities. Perhaps most significantly, the IOC has consistently ensured through its Olympic bidding requirements that each host Government accepts responsibility for the security of the Games (and in particular the costs of them). This was no different for London 2012, and the importance the IOC placed on security in this case was equally clear as it articulated its confidence in the UK's security preparations.<sup>136</sup> Even after the G4S contract failure, the President of the IOC, Jacques Rogge, explained his satisfaction with the contingency established for the Games; 'The troops are a source of reassurance for the public, I don't see it as a negative thing.'<sup>137</sup> The IOC was therefore clearly an influential stakeholder in respect of London 2012's security arrangements; this should be understood, however, in the context of its insistence that it would be the UK Government who should oversee and be the ultimate guarantor for financing them.

It was not only sporting venue operators with whom the Government interacted on London 2012 security issues; it should be recalled that a large number of additional events were organised by private event companies across the UK during the Games. These were not 'official' events but their association with London 2012 by timing would certainly result in 'a need for extra security.'<sup>138</sup> Whilst the Government indicated that it did not intend to subsidise the security of 'crowded places away from the Olympics', the Director of Olympic Safety and Security in the Home Office, Robert Raine, outlined in a speech to

---

<sup>135</sup> Evans, 'The role of the private security industry', p.164 (Emphasis added)

<sup>136</sup> The IOC's assessment of London's 2012 Olympic bid stated; 'The UK has hosted a large number of sports and other international events, demonstrating it has the experience to cover potential security risks.' International Olympic Committee, 'Report of the IOC Evaluation Commission for the Games of the XXX Olympiad in 2012', 22 March 2005, Via: [http://www.olympic.org/Documents/Host\\_city\\_elections/2012\\_OG-Report\\_of\\_the\\_Evaluation\\_Commission.pdf](http://www.olympic.org/Documents/Host_city_elections/2012_OG-Report_of_the_Evaluation_Commission.pdf) (accessed 06.09.12), p.76

<sup>137</sup> 'London 2012: IOC President 'reassured' by troops presence for Olympic security', *The Telegraph*, 23 July 2012, Via: <http://www.telegraph.co.uk/sport/olympics/olympicsvideo/9421384/London-2012-IOC-President-reassured-by-troops-presence-for-Olympic-security.html> (accessed 06.09.12)

<sup>138</sup> Gilmore, 'Countdown to the Olympics', p.30

the Police Foundation that it would be necessary to continue to ‘work in partnership’ with the events industry on the security of such events<sup>139</sup>; substantial security responsibilities were thus placed in ‘private’ hands. To ensure appropriate coordination around these additional activities, the Greater London Authority developed a ‘London Events Coordination Calendar’: the original vision for the initiative was to appoint resources to generate ‘...a central repository of all ‘events’ of interest’ planned from the 1st May to 31st October 2012 to be used to evaluate the viability of hosting such events from a safety, security and visitor experience perspective.’<sup>140</sup> This reveals that it would be wrong to look upon LOCOG as being the only venue operator of security for London 2012; the reality is that the authorities were engaged with a much wider set of companies on securing events across the UK.

Finally, emergency preparedness training for the Games was delivered by the private sector. Although at least one ‘traditional’ security training contract was supplied to the public sector by the company SCS<sup>141</sup>, that G4S was tasked with training LOCOG’s security officers and volunteers also shows how operational ‘private-to-private’ dynamics were present in the Olympic security strategy.

### ***Wider Business***

Several initiatives were developed between Games security planners and wider sectors of the UK economy. Perhaps the most significant was the ‘Cross-Sector Safety and Security Communications Project’ (CSSC) which was established to ensure the efficiency of safety

---

<sup>139</sup> Robert Raine, ‘Working with the private sector to deliver a safe and secure Olympic Games’, Speech to 2009 Police Foundation annual conference. 7 Sept. 2010, Via: <https://www.youtube.com/watch?v=azR3h9ugcfQ&feature=channel&list=UL> (last accessed 29.12.14)

<sup>140</sup> Greater London Authority, ‘London Events Coordination Calendar – Delivery Support’, Via: <http://www.london.gov.uk/sites/default/files/ODD24%20LECC%20Project%20Support%20PDF.pdf> (accessed 30.12.14)

<sup>141</sup> SCS, ‘SCS helps to deliver safe London 2012 Olympic and Paralympic Games’, 10 Sept. 2012, Via: <http://scs.scs.biz/news/scs-helps-to-deliver-safe-london-2012-olympic-paralympic-games/> (accessed 17.09.12)

and security communications between emergency planners and London's businesses both at the time of the Games and thereafter. The website of the initiative explains:

CSSC was founded in June 2011 by a team of senior security experts, with the aim of building a platform to facilitate communications between private and public sector on issues surrounding security and business resilience. The initial focus of CSSC was to help businesses prepare for business as usual in the lead up to, and during the Olympic and Paralympic Games.<sup>142</sup>

Other details are available of what was pitched as a 'truly cross-sectoral'<sup>143</sup> project including the participation of 'twenty-three business categories from banking, insurance, security and supply chain to retail, tourism, hotels, night-time economy and media'<sup>144</sup> - in essence the project was geared at providing threat and real-time security information to the private sector in an efficient manner.

In an interview for this thesis, the leader of the initiative, Sir David Veness, explained how the failure of the authorities to effectively communicate with the business community at the time of the 2011 riots in London served as a 'bit of a jolt'<sup>145</sup> to the authorities in the context of how to communicate to the private sector on security issues for London 2012. The rationale behind the establishment of the CSSC was further explained:

The one thing that business in all of its dimensions wanted out of the prospect of this largest peacetime security operation ever was communication from the public to the private sector - not classified information, not breaking news, but timely, actionable, authoritative information on which a business of any size could make a decision.<sup>146</sup>

In so far as the costs of the CSSC were concerned, Veness further explained that '...the entire CSSC project was run with zero budget from the public sector and was all funded on

---

<sup>142</sup> CSSC, 'About CSSC', Via: <http://www.vocal.co.uk/cssc/about-cssc/> (accessed 30.12.14)

<sup>143</sup> Valentina Soria, 'Promoting the Concept of 'UK plc': A Public-Private Sector Olympic Challenge', *RUSI Journal*, Vol.157:2 (April/May 2012), p.37

<sup>144</sup> Ibid.

<sup>145</sup> Interview, David Veness

<sup>146</sup> Ibid.

goodwill and secondees from the private sector.<sup>147</sup> Any suggestion that this category of the private sector may have been seeking to appropriate public funds through the establishment of the scheme, in the spirit of the more conspiratorial SIC-type theories, could not be viewed as serious; the ambition appears to have been to simply strengthen the levels of public-private communication around security risks and issues, and enhance the private sector's preparedness in that context. Interestingly, CSSC was not the only effort at seeking to engage the private sector considered as the business community in the widest sense. Alongside this initiative, the Games Organisers, LOCOG, published a planning document for businesses which includes a section outlining safety and security advice for the private sector.<sup>148</sup> Whilst problems transpired in their efforts to work with their own commercial security suppliers, officials clearly placed a high priority on the development of a wider business engagement strategy as a part of the security strategy for London 2012.

The (private) education sector also contributed to the Games' security arrangements; notwithstanding the failure to recruit and train sufficient numbers of security personnel. Most significantly, a scheme called 'Bridging the Gap' was established in collaboration with the security industry with a view to meeting the significant manpower requirements that it was always anticipated would be placed on the private security industry for the Games.<sup>149</sup> This was a 'private' project in more senses than one: whilst suppliers' decisions to participate may not have been entirely altruistic, it was reported that LOCOG '...invested more than GB pound 1 million in Bridging The Gap to assist young people in learning new skills and gaining on-the-job training.'<sup>150</sup> The supposed uniqueness

---

<sup>147</sup> Ibid.

<sup>148</sup> London 2012, 'Preparing your business for the games', Via: <http://www.london2012.com/get-involved/business-network/preparing-your-business.php> (accessed 15.01.12), pp.20-22

<sup>149</sup> Evans explained that the London Games would need 'in excess of 7,000 such people, yet the industry does not have this number available in its normal capacity.' Evans, 'The role of the private security industry', p.175

<sup>150</sup> Amanda Beesley, 'The BSIA Briefing: June 2012', *ifsecglobal.com*, June 2012, Via: <http://www.ifsecglobal.com/the-bsia-briefing-june-2012/> (accessed 30.12.14)

of this initiative was even articulated by the Government; the (then) Security Minister, Pauline Neville-Jones, stated: 'Bridging the Gap is an innovative example of partnership working between the Home Office, LOCOG, further education colleges and the private sector.'<sup>151</sup> The failure to deploy sufficient numbers of security personnel in time for the Games raises questions about the efficacy of the scheme, but it also clearly represents a further intended cooperation between the public and private sectors in the Olympic security strategy.

Several other business sectors were involved in London 2012 security which further illustrates the diversity of the public-private security cooperation that emerged. Firstly, as suggested above the 'Sponsor Effect'<sup>152</sup> brought with it 'a significant demand for security'<sup>153</sup> from those (national and global) companies who formed an official association with the Games.<sup>154</sup> Secondly, privately-funded event organisers were involved in hosting conferences to act as platforms for the articulation of London 2012 security preparations; prominent amongst these was the suite of Olympic security-related events organised by CityForum Limited.<sup>155</sup> Finally, as Jennings outlines, the insurance industry plays an important role in the preparation for any Olympics<sup>156</sup>; the IOC and other organisations have increasingly been purchasing 'insurance for cancellation due to terrorism or natural disaster for recent Games.'<sup>157</sup> In the case of London 2012, it proved a significant challenge to find insurance cover around the main security services contract; it has been suggested

---

<sup>151</sup> Bridging the Gap, 'Stakeholders', Via: <http://www.bridging-the-gap.co.uk/Stakeholders.aspx> (accessed 19.01.12)

<sup>152</sup> Evans, 'The role of the private security industry', p.169

<sup>153</sup> Ibid.

<sup>154</sup> A list of London 2012's commercial partners was available at: <http://www.london2012.com/about-us/the-people-delivering-the-games/london-2012-olympic-games-partners.php> (accessed 19.01.12)

<sup>155</sup> See details of its April 2007 event, 'The security and Safety of the 2012 Olympics', Via: [http://www.cityforum.co.uk/index.php?option=com\\_eventlist&func=details&did=4&book=no](http://www.cityforum.co.uk/index.php?option=com_eventlist&func=details&did=4&book=no) (accessed 19.01.12)

<sup>156</sup> Jennings, 'Governing the Games', p.152

<sup>157</sup> Ibid.



that G4S eventually purchased a policy from the US market because it could not find satisfactory UK cover.<sup>158</sup>

#### **5.4 Character and impact of the industrial-complex in Olympic Security**

This chapter suggests that three main characteristics of the 'industrial-complex' in CT were exhibited in this case - firstly, both the IOC and other event organisers including LOCOG appeared to be, like other 'private operators' examined in this thesis, reluctant to allocate their own resources towards security; the Government provided a substantial public subsidy to cover the costs of venue security in this context. Secondly, many 'suppliers' possessed an interest in the emergence of a large number of substantial Olympic security contracts; that there were substantial commercial opportunities, or at least the perception of such opportunities, is not in question. A third dynamic arose which saw wider business sectors of the economy putting in place new measures to enhance (and fund) their own security arrangements.

It is worth briefly elaborating on these dynamics, as they have not been covered by other existing scholarly contributions on London 2012. Firstly, as it was a private company operating for a limited period, LOCOG would have possessed a limited interest in investing a substantial amount of its own resources towards the financing of venue security. It can also be suggested that there was potentially a strong incentive to resist doing so; namely the Government's guarantee to the IOC that it would underwrite the costs for the security of the Games. According to the co-chair of the London 2012 Olympic Security IAG, the significance of these guarantees was never truly understood and may have actually directly contributed to the G4S security contract episode. Reflecting on why the provision of manpower security has so often failed at recent Games, Evans stated:

---

<sup>158</sup> As explained at the 'Military Aid to the Private Authorities?' seminar on 3 May 2012

And so you've got to ask the question - why is that? And foremost in my thinking is the guarantee of safety and security which was required by the IOC in the original bid document, and which was agreed to by our Home Secretary. If you have a Government guarantee to provide a safe and secure Games, then 'why should the IOC worry about private sector delivery and why should the organising committee make their preparations in a way that would meet private sector delivery requirements?' is the thought that occurs to me. They know that the Government is obliged to step in, if the private sector fails to meet its full requirement, with staff from the police and armed forces; and this at no cost to the IOC / Organising Committee. And I don't think we ever understood that and certainly I never saw this element of the guarantee in the register of risks.<sup>159</sup>

Albeit it is offered in retrospect, Evans makes an extremely compelling case; there may well have been an inclination on the part of the private event organiser, LOCOG, to seek to avoid taking on additional costs, particularly in the context of the UK Government's guarantees provided to the IOC. It is worth considering, therefore, whether there may have been an irresistible urge within LOCOG to 'offset' its security costs to others; it can be observed that whilst the IOC was not a factor in that case, a similar dynamic existed with the transport operators in the e-Borders case. Whilst it may never be possible to validate the extent to which it sought to draw on public funding, the Government's decision to allocate a substantial state-funded grant to LOCOG at such a late stage of the Olympic security planning process could be understood from this perspective.

Secondly, whilst it has not been demonstrated that the public-private interactions illustrated above directly impacted upon the growth in the Olympic security budget per se, many commercial security suppliers clearly profited financially from London 2012's security arrangements. However, not all companies benefited as advocates of a more negative account of the 'SIC' system might suggest. In the case of the largest publicly-

---

<sup>159</sup> Written Correspondence, David Evans

funded Olympic security contract, for example, G4S's failure to deliver fully on its contract meant that the company would eventually expect to make a *loss* of £50m.<sup>160</sup>

Finally, the wider business community implemented its own new mechanisms to enhance security communications in preparation for, and in the event of, an emergency situation at the time of the Games (and beyond). A dedicated page on a security trade association website<sup>161</sup> provides clear evidence of a systemic exchange with the public sector as a part of the scheme; the latter regularly provided information to businesses across London. There is no indication, however, that any public funding was allocated towards the project.

In conclusion, the private sector's involvement in the safety and security of London 2012 was extensive, significant, and, particularly in the case of the G4S Olympic security contract, highly problematic.<sup>162</sup> It is because the high level recognition of the role of the private sector in the Olympic security strategy had not previously been comprehensively investigated that this chapter examined its involvement. The research has revealed multiple public-private interactions in London 2012's security preparations; a variety of exchanges took place across the 'Private Supply', 'Private Operator' and 'Wider Business' dimensions, supporting this thesis's argument that a new type of 'industrial-complex' is operating in the UK's CT sector.

Any specific, tangible effect that any 'SIC' may have had on London 2012 security expenditure has not been shown. On the contrary, the research suggests a possible

---

<sup>160</sup> See footnote 50.

<sup>161</sup> BSIA, 'Cross-sector Safety and Security Communications (CSSC)', Via: <http://www.bsia.co.uk/CSSC> (accessed 06.09.12)

<sup>162</sup> This is not to downplay the centrality of the public sector's responsibility for London 2012 security, but this chapter has been concerned with the private sector's involvement. As indicated above, the Government held ultimate responsibility for ensuring Olympic Security; the author is grateful for discussions with Christopher Kinsey on the importance of this point. For a full list of public sector organisations involved in London 2012 security, see Keith Weston, 'The challenge of inter-agency coordination', in Richards et. al., *Terrorism and the Olympics*, pp.180-207

inclination of the (private) event organiser within the system, LOCOG, to decline to invest a substantial proportion of its own resources towards security; this appears to have resulted in the Government deciding during the final years of planning that it would be necessary to cover the Games' venue security costs. LOCOG could be forgiven for possessing this disposition in view of the Government's guarantees and the fact that it was ultimately a temporary event company; on the other hand, the Olympic security strategy was clear that the delivery of routine safety and security measures at venues was the responsibility of LOCOG<sup>163</sup> and, as it transpired, there were failures in both the assessment and delivery of the requirements around them.

Subsequent parliamentary scrutiny of the G4S contract affair has revealed more details about the public-private dynamics that existed within the Olympic security strategy. Most notably, senior figures including the Home Secretary and the leadership of LOCOG attributed the failure of the security contract to G4S in front of the HASC, with the Committee itself concluding that the blame rested 'firmly and solely' with the company.<sup>164</sup> Perhaps controversially, the author maintains the argument that this was a highly unsatisfactory and inaccurate conclusion; the level of interdependency that existed between the public and private sectors at the heart of London 2012's security governance framework was never properly examined by the HASC and can clearly be seen to have contributed to the G4S contract failure. That the 'ownership' of responsibility for venue security was shared - symbolised by the Government's decision to finance the arrangements at the same time maintaining that the contract was 'owned' by LOCOG - led

---

<sup>163</sup> Home Office, 'London 2012 Olympic and Paralympic Safety and Security Strategy', p.18

<sup>164</sup> HASC, 'Olympics Security', p.12

to the creation of an unusual, arguably highly undesirable governance structure that ultimately failed to prevent the ‘last minute hitch’<sup>165</sup> occurring shortly before the Games.

Whilst the Home Office and LOCOG appear to have worked together extremely closely - the CEO of LOCOG, Paul Deighton, stated to the HASC that together with the police ‘[t]he nature of the relationship between us and the Home Office (...) was extremely tight and collaborative’<sup>166</sup> - the ‘final’ venue security requirement for 10,400 ‘new’ private security personnel was only agreed in December 2011.<sup>167</sup> It is clear, therefore, that G4S had very limited time to deliver the additional numbers<sup>168</sup> and that the responsibility to monitor the implementation of the revised contract might have been discharged more effectively. Whilst the media and Parliamentary outrage which directly preceded the Games concentrated on G4S’s failures, the chapter has found that there appear to have been significant problems with the modelling that it has been suggested was completed by Deloitte; a private sector consultancy.

This chapter identified several additional factors which may have heavily impacted upon the security arrangements (and therefore associated expenditure) for the Games. The coalition Government’s realisation of its responsibilities following the General Election of 2010; the already existing ‘substantial’ terrorism threat to the UK; and key figures’ lack of experience at handling aspects of such major security operations may all have contributed to the increases in the security costs for London 2012. The system of interactions between the public and private sectors in this sector - the industrial-complex

---

<sup>165</sup> The Director General of the OSCT described it this way on the ‘Today Programme’, *BBC Radio 4* (20.07.12), Via: [http://news.bbc.co.uk/today/hi/today/newsid\\_9739000/9739444.stm](http://news.bbc.co.uk/today/hi/today/newsid_9739000/9739444.stm) (accessed 09.09.12)

<sup>166</sup> Home Affairs Select Committee, ‘Uncorrected Transcript of Oral Evidence’, Olympic Security Inquiry Session 2012-13, 11 Sept. 2012, Via: <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmhaff/uc531-iii/uc53101.htm> (accessed 24.09.12)

<sup>167</sup> Rosemont, ‘Reassessing the G4S Olympic security affair’

<sup>168</sup> *Ibid.*

in CT - can, therefore, only be properly considered one factor amongst several in accounting for the substantial growth in the London 2012 security budget.

In conclusion, the chapter demonstrated that the private sector's involvement in London 2012 security was extensive and highly varied. This reinforces the notion that an industrial-complex of a different character to the MIC now exists in the non-military CT arena, and that the private sector's involvement in UK national security strategy is now a crucial consideration.

## Chapter 6: Strategic Engagement

### Introduction

Detailed analysis of three large post-9/11 public sector security contracts has shown that, notwithstanding their serious difficulties, a considerable degree of ‘closeness’ emerged in the character of the relationship between the public and private sectors in CONTEST. Whilst the analysis of the case studies in the previous chapters has questioned whether the ‘industrial-complex’ in the CT sector should be considered a sinister conspiracy, an extensive network of public-private interaction clearly exists in at least these three sub-sectors of the CT aspects of security policy.

To develop this thesis’s investigation into the origins, character and consequences of the private sector’s involvement in UK national security strategy, it is necessary to look beyond individual themes and specific procurements; this is important because, traditionally, the MIC has itself been considered as a broader system than merely the acquisition of specific capabilities. This chapter therefore examines the origins, character and activities of the principal primary, official and formal channel of communication that was established in the UK between Government and the security industry on non-military, CT-related security issues; the UK Security and Resilience Industry Suppliers’ Community (RISC). The findings support the conclusions of previous chapters - the industrial-complex in the CT sector possesses some of the dynamics associated with the MIC, but its characteristics differ in important respects.

It is important to consider the character and operation of RISC when considering ‘the SIC’ in the CT sector because, with only limited exemptions<sup>1</sup>, a lack of scholarly attention has been paid to the motivations, potential influence and impact of industrial

---

<sup>1</sup> White has examined the collective political motivations of industry and one of its representative bodies in his recent book on the security industry. White, *The Politics of Private Security*. See also Rosemont, ‘Private sector engagement’, for an analysis of RISC’s input into the formation of the UK Government’s 2012 ‘National Security Through Technology’ policy document.

representative organisations upon security policy and associated spending levels. This is a surprising oversight in view of the ferocity and volume of the criticism that has been levelled towards the emerging 'SIC' since 9/11.<sup>2</sup> Indeed, one might have expected that RISC would have been subject to extensive scrutiny in view of the fact that UK Government security policy documentation after 9/11 has referred to the important role it plays in supporting the Government's security objectives.<sup>3</sup> This contrasts with the criticism levelled towards the engagement structures that have emerged between Government and industry within the defence sector<sup>4</sup>.

Several reasons may account for the apparent apathy with which scholars have treated the development of RISC. Firstly, in contrast to the defence sector there are some limitations around what can be discussed (let alone published) on structures dealing with what are undeniably sensitive CT matters. Secondly, it may be that 'domestic security' issues are seen as potentially less glamorous than military issues; discussing whether private contractors should be permitted to kill adversaries on the battlefield or whilst supporting military operations, whilst largely a fictional proposition, can be seen as more exciting than debating whether security guards should be able to search passengers at UK airports, for example. This lack of scholarly attention may need to change, however, in view of the extensive level of private sector involvement in non-military areas of national security such as CT, as illustrated above, and the growing prominence with which its role features in Government documentation.

---

<sup>2</sup> As discussed in Chapter 1, Section 1.1.

<sup>3</sup> The 2011 iteration of CONTEST states that RISC; '...is the mechanism by which Government communicates with industry about its counter-terrorism science and technology needs.' HM Government, 'CONTEST: The United Kingdom's Strategy for Countering Terrorism', p.112

<sup>4</sup> CAAT has been particularly critical, for example, of the 'high-level advisory bodies' that exist between government and industry such as the Defence Suppliers' Forum. 'High-level advisory bodies', CAAT Website, Via: <http://www.caat.org.uk/issues/influence/advisory-bodies.php> (accessed 03.04.14)



This chapter provides for the first time an analysis of RISC's ambition to support and influence Government on the industrial aspects of security policy after 9/11. Whilst there is nothing necessarily wrong with 'lobbying' per se, it is the contention of this thesis that it is essential for this development to be properly analysed to determine whether new mechanisms of oversight and accountability are needed in this sector. Furthermore, whilst defence spending continues to account for the largest proportion of the UK's national security budget, non-military security expenditure has grown substantially since 9/11. This thesis has consistently argued that it is right and proper, therefore, to consider whether the dynamics once attributed to the MIC have shifted to security sector, and/or affected policy. Finally, as Chapter 7 will examine in further detail, a more active and coordinated (yet remarkably little commented upon) UK Government strategy is now being pursued with RISC around how to harness the contributions of the security industry; including on controversial issues such as the promotion of security exports internationally. As RISC has sought to contribute to the development of this activity, proper attention should be afforded to the origins and character - not to mention the appropriateness - of the role it has played.

### **6.1 Origins of cooperation**

Whilst RISC was formally launched in March 2007, the original idea to establish a mechanism for more structured dialogue with the private sector on CT issues preceded this date. It is important to consider the origins of the organization not only to examine the causes of, and reasoning behind, its foundation, but also because such a historical enquiry provides insights into the character of public-private interaction that has emerged. In researching this element of post 9/11 public-private security cooperation, this thesis benefitted from interviews with individuals involved in the development of RISC, and for being provided access to a record of minutes and other archival documentation arising

from what emerges as RISC's direct predecessor organization - the little known Joint National Security and Resilience Advisory Council (JNSRAC).

### *Early ambitions*

The first and (as it transpired) only ever Chairman of the JNSRAC, Mr. John Backhouse, was interviewed and offered an account of how the entity initially emerged in 2005. The impression left is of an absence at the time of any existing structures for coordinating Government-industry liaison on CT matters, with only an ad hoc collection of individual companies and industry trade associations with various interests in 'security' apparently interested in creating such engagement. Serious discussions developed on the idea of forming a more comprehensive pan-industry engagement mechanism for the UK, albeit initially very informal in character. According to Mr. Backhouse in an interview with the author, initial discussions held at a preliminary security industry meeting convened by the Intellect Industry Association (now rebranded as TechUK) at a hotel on Park Lane in London in early 2004 - for 'so-called interested security companies within the Intellect membership, who in some way, shape or form, had innovations and products to offer within this new security sector'<sup>5</sup> - suggested much need for improvement. Backhouse reflected:

...it was apparent from that meeting there was no direction, no strategic planning or even interface with Government agencies. There was a mission statement, but (...) objectives, strategies or tactics seemed to be, light on the ground.<sup>6</sup>

Mr. Backhouse also recollected:

I was of the opinion there needs to be someone who can coordinate this activity because we were going through (...) a period of 'amber' in respect of some of the perceived threats to homeland security which were being reported in the news[.]<sup>7</sup>

---

<sup>5</sup> Interview, John Backhouse

<sup>6</sup> Ibid.

<sup>7</sup> Ibid.

According to Backhouse, in 2004-05 there was an overwhelming sense that the security industry was being treated on an ‘ad hoc’, uncoordinated basis and this needed to change in the new context.

The first meeting of the initially-named ‘National Security & Resilience Council’ was convened at the premises of the Intellect Trade Association on 20 June 2005 and the notes of the meeting immediately illustrate how consideration was given to the appropriateness of somehow replicating the structures that already existed in ‘defence’ to the ‘security’ sector. Indeed, the Chairman introduced the meeting by stating that the ‘objective was to ascertain whether members perceived any value in establishing a new Defence Council to address the Homeland Security (HLS) domain?’<sup>8</sup> In addressing this question, a consensus quickly emerged that the creation of such a forum would be beneficial; one attendee stated, for example, that ‘a collaborative approach should be developed’<sup>9</sup>, whilst another advanced the idea that ‘Industry should be collectively assembled even if HMG [Her Majesty’s Government] is not.’<sup>10</sup> Such were the perceived shortcomings of the existing, disorganised approach, that another member even ‘saw coordination as the ‘Holy Grail’<sup>11</sup>. There was no shortage of ambition during the group’s discussion on the ‘Proposal to Establish a Council’; it is even recorded that the Chairman ‘suggested that the ambition should be to become the lead single voice for UK/Europe/Global.’<sup>12</sup>

Further discussions took place on the possible future membership of the body, and on identifying the Council’s future objectives; the minutes state that the budding entity believed that ‘high-level coordination activity is essential’ and that ‘The Council should develop *a partnership between Industry and Government (Central and Local), Emergency*

---

<sup>8</sup> ‘Intellect Minutes’, Meeting of the National Security & Resilience Council, 20<sup>th</sup> June 2005, p.2

<sup>9</sup> Ibid.

<sup>10</sup> Ibid.

<sup>11</sup> Ibid. p.3

<sup>12</sup> Ibid. p.2

*Services & Academia*<sup>13</sup>. With the first stated objective of the organization being to develop a 'partnership' with Government, the organization quickly turned its attention to potential future membership. The initial meeting recognised the need to involve a broad coalition of interested parties in future meetings; an action was specifically agreed to 'invite the relevant industry Chairman from HLS groups in the DMA, SBAC, RUSI (Sandra Bell) and Chatham House to the next meeting'<sup>14</sup>. The group certainly seemed to be successful in addressing this issue; whilst the initial gathering attracted only six attendees - interestingly, from companies operating in defence and thus providing evidence of dynamics shifting from 'defence' to 'security'<sup>15</sup> - 14 representatives participated in the following meeting.<sup>16</sup>

A picture of increasing activism subsequently emerges from JNSRAC's documentation and the early discussions reflected a strong and increasingly coordinated industry-led desire to secure a more formal and regularized form of strategic engagement with the Government on security issues. For example, a discussion on the rationale and aims of the new structure took place during the second meeting of the now re-named JNSRAC on 27 July 2005. The Chairman opened the meeting as follows:

Our agreed purpose today is to establish a way forward, a direction, working together as one united body or council, with a broad and definite mandate intent to assist those National and Local Government and Authorities involved in the broad subject of Security and Resilience.<sup>17</sup>

Whilst not everyone might be comfortable with such a mandate being handed to an industry body, it is perhaps reassuring that the new structure purported to wish to support

---

<sup>13</sup> Ibid. p.4 (Emphasis in original)

<sup>14</sup> Ibid.

<sup>15</sup> All five of the industry figures present (the sixth attendee was a trade association official) represented companies who possessed defence as well as security sector interests. The companies were: Smiths Industries (two representatives), Thales UK, BAE Systems and EDS Defence. Ibid p.1

<sup>16</sup> 'Intellect Minutes', Meeting of the Joint National Security & Resilience Advisory Council, 27 July 2005, p.1

<sup>17</sup> Ibid.

the UK's security objectives, rather than be limited to the pursuit of its own commercial interests<sup>18</sup>.

The JNSRAC was clearly seeking to establish a formal structure for cooperation with Government and the group discussed how it would be important to identify an appropriate interlocutor; as one participant put it, the senior Cabinet Office official, Mr. Bill Jeffrey (then Security and Intelligence Coordinator), would be 'a good lever for industry to exercise especially in identifying an HMG focus to industry'<sup>19</sup> and the minutes also record the Chairman's statement that he '[u]nderstood that Mr. Jeffreys (sic.) is very keen to support this Council'.<sup>20</sup> This represents a clear desire on the part of industry, therefore, to establish a dialogue with a least one corner of the 'iron triangle' (the Executive), and the suggestion that Government might have been receptive to it.

#### *Emerging objectives*

Additional documentation shows that careful consideration was given to how to realize the JNSRAC's emerging objectives. Most strikingly, in an initial discussion of the 'Purpose and Tasks' of one of JNSRAC's working groups, a primary aim was recorded as being 'To understand and influence policy'<sup>21</sup>; this clearly establishes that the organization did consider developing a role for lobbying within its structures. Furthermore, having embarked upon an exercise in defining 'the key customers within National, Regional, and Local Governments and the Civil Sector'<sup>22</sup>, the participants agreed that 'Sir Richard Mottram (who had succeeded Bill Jeffrey as Security and Intelligence Coordinator) was the

---

<sup>18</sup> This early statement of intent on how the organization would wish to support national security objectives would also be a constant theme of RISC, at least on paper, as evidenced within its submission during the pre-NSST consultation process, as indicated below.

<sup>19</sup> 'Intellect Minutes', 27 July 2005, p.3

<sup>20</sup> Ibid.

<sup>21</sup> JNSRAC, Communications and Liaison Sub-Committee, 7<sup>th</sup> November 2005, p.2

<sup>22</sup> Ibid. p.3 This culminated in the creation of a chart, attached to the minutes, which indicated those 'UK Government Departments involved, in some way, with homeland security'

most important individual to target'<sup>23</sup> before identifying 'the key message to be delivered to him'<sup>24</sup>. In a statement that might concern critics of 'the SIC', one of the bullet points covering what it believed should be relayed to Sir Richard was that JNSRAC '...exists to bring coherence to advice and on industrial capabilities to *inform procurement decisions* by Government departments'<sup>25</sup>. Whilst such discussions appear to have been of only an informal nature, they are revealing of the JNSRAC's apparent desire to seek to inform government thinking outside official contracting procedures.

The JNSRAC's emerging efforts to engage Government achieved notable progress; meeting minutes record that two senior civil servants - Sir Richard Mottram and Bruce Mann<sup>26</sup> - were involved early on. Indeed, the JNSRAC's Chairman noted that the presence of Sir Richard at its meeting in December 2005 promised to make it a 'landmark event'<sup>27</sup>, introducing the meeting as follows:

Sir Richard, I stress that JNSRAC is not another Trade Association - neither is it a bureaucratic quango - It is a functional, voluntary, advisory and consultative body of senior executives all involved in the wide arena and scenario of National/Homeland Security, offering ourselves as a single collective advisory council for efficiency and effectiveness. - A single coordinated voice with one hymn sheet and without any grandiose Ideologies.<sup>28</sup>

In a pithy conclusion to the meeting seemingly designed to state industry's offering in no uncertain terms, the Chairman stated that JNSRAC aimed to become '...a National Defence Industrial Council for National Security and Resilience.'<sup>29</sup> This striking statement confirms, perhaps more than any other cited in the thesis, that the foundations of JNSRAC (and therefore RISC) were borne out of a comparison with the arrangements that already

---

<sup>23</sup> Ibid. A connection has not been made between the Committee's desire to 'target' Sir Richard with its curious insistence, captured within the minutes of the same meeting, that it 'did not intend to usurp any Government department' *ibid.* p.2.

<sup>24</sup> Ibid. p.4

<sup>25</sup> Ibid. (Emphasis added)

<sup>26</sup> Then Head of the Cabinet Office's Civil Contingencies Unit

<sup>27</sup> 'JNSRAC Minutes', Joint National Security & Resilience Advisory Council, 13 December 2005, p.3

<sup>28</sup> Ibid. p.5

<sup>29</sup> Ibid.

existed in the defence sector; arrangements around which the Cabinet Office's Security and Intelligence Coordinator would certainly have been aware. Critics might look upon this as alarming new evidence of the more damning SIC thesis - that the MIC was seeking new ways to institutionalize itself in the burgeoning CT sector. Worse still, the emerging collaboration appears to have been developing largely as a result of an 'industry push' and not a 'government pull'. It is clear that a form of systemic exchange was developing, and that JNSRAC was actively promoting the need for stronger mechanisms for strategic dialogue.

Further dialogue took place between the JNSRAC and its high profile guest; a roundtable discussion indicates how industry views were relayed to Sir Richard on the shortcomings of the status quo mechanisms for public-private sector cooperation. One attendee suggested, for example, that reforms to procurement could save Government 'a great deal of money'<sup>30</sup>, whilst another lamented how 'Requirements and needs are fragmented' in the security sector, meaning that; 'Industry is therefore reluctant to invest which puts risk on HMG as well as taking longer to achieve implementation of a solution'<sup>31</sup>. There is nothing in the minutes to suggest that the Government was in anything more than 'receive mode'<sup>32</sup> or that it would take the various issues raised by those present automatically at face value. However, Sir Richard's statement that '...I am concerned about what you have told me and I will go away and think this through' does seem to indicate that the Cabinet Office, if not other departments<sup>33</sup>, was minded to carefully consider JNSRAC's perspective.

---

<sup>30</sup> Ibid.

<sup>31</sup> Ibid.

<sup>32</sup> The minutes record several questions having being posed to the JNSRAC meeting by Sir Richard, including: 'Given the existing machinery is there a market failure?'; 'What are you thought's on the lessons from 7/7?'; and 'Has JNSRAC discussed these issues elsewhere within HMG?' *ibid.* pp.5-7

<sup>33</sup> There is evidence to suggest that there were differences in how different Government departments considered the potential value of JNSRAC. For example, the minutes from one meeting noted that 'ODPM [Office of the Deputy Prime Minister] and the Cabinet Office were supportive of

The extent to which the JNSRAC persuaded Sir Richard to commit the Government to work with it (and subsequently RISC) is not entirely clear - John Backhouse described Sir Richard's involvement in establishing the alliance as 'instrumental'<sup>34</sup> but there is no evidence that he personally attended another meeting of the organization. However, it is clear that Government thought enough of the organization that it continued to send officials to participate in its meetings<sup>35</sup>. It is easy to understand why the JNSRAC might have been able to achieve such resonance; whilst the first of its (internal) meetings described above notably took place shortly *before* the tragic events of 7/7, UK CT policy (including the industrial aspects thereof) quickly grew as a priority after this event. From the available evidence, JNSRAC quickly established itself as *the* leading industry forum that Government could engage with on this matter; on paper at least, it deliberately positioned itself as an easy and representative way in which the Government could consult the private sector.

## 6.2 Inappropriate Foundations?

The question of what constituted the motivations of those involved pushing for the establishment of a more formal structure for public-private cooperation is important to consider at this juncture; evidence that it was designed solely out of commercial self-interest might support the 'SIC-as-conspiracy' thesis. To apply the proposition put forward by White in his study on the politics of the manpower-orientated part of the security

---

JNSRAC. The Home Office were less so, with the exception of HOSDB [Home Office Scientific Development Branch] but the latter had to be seen to support the Home Office line.' JNSRAC, Communications and Liaison Sub-Committee, 7th November 2005, p.2

<sup>34</sup> Interview, John Backhouse. Backhouse also stressed that the involvement of the former Home Secretary, John Reid, was 'paramount' in the transition of JNSRAC to RISC. Written Correspondence, Backhouse

<sup>35</sup> For example, the Chairman of JNSRAC wrote to Bruce Mann on 20 February 2006, thanking him for attending its previous Council meeting (on 7 February of the same year) and for the 'constructive comments' he made. John B. Backhouse, Letter to Mr. Bruce Mann, Cabinet Office, 20 February 2006. Separately, a Home Office official attended the meeting of the JNSRAC Council on 12<sup>th</sup> December 2006. In another example of defence/security sector overlap, a representative of the UK Government's Defence Export Service Organisation (DESO) also attended JNSRAC Council meetings on 13 December 2005 and 12 December 2006.



industry - that, ultimately, 'private security companies are driven *purely* by profit motivations'<sup>36</sup> - one might assume that, in pursuing a more formalized cooperative structure, industry's desire to generate new business was the sole underpinning motivation behind establishing JNSRAC (and subsequently RISC). Any such conclusion would appear to be unfounded, however; judging by its public pronouncements, JNSRAC saw itself primarily as a structure capable of supporting the Government's national security and resilience objectives. This purported *raison-d'être* features particularly prominently, for example, in the 'Project GaIN report' that was submitted to the Government by the 'UK Security and Resilience Supply Base' through the JNSRAC in June 2006. Understood to have been drafted primarily by (JNSRAC Council member) Dr. Sandra Bell, then of the Royal United Services Institute (RUSI), this report illustrates how the case for creating 'a framework of operation across the entirety of the supply and demand communities'<sup>37</sup> was justified on the basis of the need to improve the public-private interface for national security reasons. Having presented the threat environment, the introduction of the document states explicitly:

*...security and resilience progress is being hampered by a lack of interest, on behalf of industry, to invest in capability solutions to meet the security and resilience challenges the nation faces. Much of this is driven directly by the lack of attractiveness of the UK security and resilience market which is widely viewed as fragmented, diffuse and opaque in places.*<sup>38</sup>

In responding to what it sees as 'barriers in the UK to industry investment'<sup>39</sup>, the report makes a series of bold (if not controversial) recommendations on how public private-cooperation in the CT sector should be structured. It includes, for example, the notion that there should be 'information exchange' on government strategies including CONTEST<sup>40</sup>,

---

<sup>36</sup> White, *The Politics of Private Security*, p.175 (Emphasis added)

<sup>37</sup> "Project Gain": Government and Industry Network for Security and Resilience, A proposal from the UK Security and Resilience Supply Base, June 2006, p.5

<sup>38</sup> "Project Gain", p.1 (Emphasis added)

<sup>39</sup> Ibid.

<sup>40</sup> "Project Gain", p.5

and that a series of what it calls 'Joint Policy Working Groups' should be established.<sup>41</sup>

Most significantly, the report proposed that the JNSRAC should be superseded by RISC, arguing that whilst there had been 'great success' under the 'trial'<sup>42</sup>, a new approach was needed:

It is recommended that the supply base build on the work of the JNSRAC and create a single body representative of UK suppliers across the entire security and resilience spectrum that can bring definitive industry expertise and enable the sharing of risks with the demand base. It is proposed that this new body be called Security & Resilience Industry Suppliers Council (RISC).<sup>43</sup>

In short, to be more representative a revised approach was being advocated that would include a wider set of participants than had been involved in JNSRAC. Whilst Project GaIN should be seen as more of a proposal than a policy, the report placed a significant emphasis on the need to improve the institutional cooperative arrangements that it argued would be needed to enhance security and resilience; i.e. to serve the public security interest, not solely industry's own commercial priorities.

That said, one interview conducted during this research raised an important new question around whether economic considerations may have been a driving motivation behind the idea of forming JNSRAC. In a potentially worrisome explanation given on the condition of anonymity by one individual familiar with the development of the organisation, it was suggested that industry's original purpose for setting up the organization was actually to generate business for companies; not to support national security objectives.<sup>44</sup> An awkward silence followed the author's follow-up question on whether this might validate the worst fears of those who would urge caution around, or might even oppose, private sector involvement in national security strategy.

---

<sup>41</sup> Ibid. p.6 Examples of possible groups are listed as 'Procurement/Acquisition, National Industrial Strategy, Research & Development, Manned Guard Legislation.....'

<sup>42</sup> Ibid. p.9

<sup>43</sup> Ibid. p.10

<sup>44</sup> Interview, Industry Executive

Other senior industrialists involved in JNSRAC and later RISC openly addressed the question of whether any more sinister motivations associated with SIC theories might underpin such strategic mechanisms of public-private engagement. Asked whether the dynamics associated with the MIC were now present in the security sector, the former Chairman of RISC replied:

I don't think the military-industrial complex concept really applies to security. After all, the military-industrial complex was supposed to be a kind of unhealthy relationship between very large companies and very large government spenders, with people (...) leaving the government service and going to work for large companies and all that. I don't think that really applies in the security sector because (...) there's a much higher proportion of smaller companies, and I don't see sort of anything equivalent to the kind of the US defence giants dominating the scene.<sup>45</sup>

The former secretary to RISC, Derek Marshall, also stated that the cooperation 'doesn't have the feel of a cosy conspiracy'<sup>46</sup>, reflecting; 'I don't start from the premise that I see industry and government colluding to whip up events to use their services.'<sup>47</sup> Of course, critics might argue that senior representatives of the security industry would naturally argue like this; their strategy, the argument might follow, is to conceal and/or deny any potentially inappropriate elements of the system. Whilst on the basis of the evidence obtained during this thesis such arguments are unproven, it is equally true that any protestation from industry that there is 'nothing to see here', however well-intended, should not necessarily be taken at face value.

The evidence suggests that to claim that a conspiracy existed would be to overdo it, however. Whilst there has hitherto been a shortage of analysis on the activity of JNSRAC and RISC, neither body has ever sought to pretend that industry did not possess commercial objectives in the security sector. For example, the Chairman of the JNSRAC was open about part of the motivation for establishing the alliance:

---

<sup>45</sup> Interview, John Howe

<sup>46</sup> Interview, Derek Marshall

<sup>47</sup> Ibid.

...that is why JNSRAC was created, as it were, to give companies a forum of opportunity for coordinated discussion, and to take their innovations further, commensurate with current Security status gained from intelligence, thus opening avenues for business and profit from sales in a new global market.<sup>48</sup>

Here, then, is clear recognition that commercial considerations did play at least some part in the establishment of JNSRAC - whilst this may be seen as undesirable, it is hardly surprising. Indeed, as the following chapter demonstrates, there is a sense in both Government and industry that it is entirely appropriate to align both national security and economic considerations in pursuing cooperation between the public and private sectors in this arena.<sup>49</sup>

Notwithstanding this thesis's later contention that the private sector's involvement in UK national security strategy should be afforded greater scrutiny and oversight, there appears to be limited evidence for any serious concerns about the activities of JNSRAC and RISC. Whilst it is clear that prior to 2006 there was very little publicly-available information on the ways in which Government was working with industry on CT issues, perhaps contributing to an impression of untoward activity, this can be explained as being mainly because any such strategic engagement was extremely ad hoc until the end of 2005. Furthermore, it should be noted that it was not until 2006 when the Government took the step of publishing CONTEST for the first time; a development that one industry executive saw as a 'big step forward'<sup>50</sup> for industry in the same way that it was for the general public. Government and industry subsequently became increasingly transparent on the work that they had been doing together on security and resilience issues, often through (but not limited to) the specific mechanism of RISC. That is not to say that it has been transparent about *all* its activity; or that there has been sufficient scrutiny of its activity.

---

<sup>48</sup> Interview, John Backhouse

<sup>49</sup> See, for example, the respective outlooks on security exports in Chapter 7, Section 7.3

<sup>50</sup> Interview, John Brading

### 6.3 From JNSRAC to RISC

Whatever the desirability of JNSRAC's agenda, the recommendations from the GaIN report were accepted and appear to have been taken forward with the wholehearted encouragement of senior Government officials. The minutes of the final meeting of the JNSRAC, for example, celebrated that within a speech he delivered in October 2006 the then Home Secretary, John Reid, had 'acknowledged Project Gain and sought further progress before the end of 2006.'<sup>51</sup> Further analysis of Reid's speech reveals a set of comments that deeply resonate with this thesis. In analyzing how innovation might be applied to the CT context, the Home Secretary stated:

There is much we can learn from the experience of such a mature sector [the defence industrial base] and what it can bring to the emerging market in security and resilience we are now seeking to create and grow. We don't do that with naiveté; it is always worth remembering what Dwight Eisenhower – hardly a renowned left-wing firebrand – had to say about what he called the "Military Industrial Complex" in his 1961 Farewell Presidential radio broadcast.<sup>52</sup>

This clearly illustrates that in its attitude towards working with industry on CT issues, the UK Government was seeking to take lessons from, if not replicate, the arrangements that existed in defence. Furthermore, it is prescient for this thesis that the Home Secretary - himself a former Defence Secretary - would choose to specifically refer to the MIC concept. The insistence of the then Home Secretary's that 'Eisenhower's warning' needed to be taken into account leaves no doubt that the dynamic was firmly in the mind of the most senior Government Minister engaged in, and ultimately responsible for, the initial formation of RISC.

Whatever concerns may have existed around the possibility for 'unwarranted influence' being exerted in this new context, they did not deter the Home Secretary from

---

<sup>51</sup> 'JNSRAC Minutes', Joint National Security & Resilience Advisory Council, 12 December 2006, p.3

<sup>52</sup> John Reid, 'speech on anti-terrorism measures', 31 October 2006, Via: <http://www.itnsource.com/shotlist/ITN/2006/10/31/R31100601/?v=1> (accessed 08.04.14)

warmly welcoming the ideas of Project GaIN and specifically the RISC initiative now under development. His comments have not been analysed elsewhere and are worth quoting in detail because they provide insights into how Government was thinking about the creation of the new structure:

The work you as suppliers are doing in forming a new trade body is most welcome. Of course, we have yet to see the details of the Security and Resilience Industry Suppliers Council (RISC) to be launched before New Year. But September's "Project GaIN" report from the UK Security and Resilience Supply Base is insightful. The statement in the report's introduction, which claims the UK market in security and resilience is fragmented and budgets too small, is striking. Inasmuch as I am determined that the emerging market grows through partnering for competitive advantage, that is no cover for allowing such important products and services to come to us only or mainly through foreign imports. As in all struggles, the winners are those able to innovate and learn ahead of the adversary. We need a clear lead in driving delivery, innovation and growth in security and resilience. Your emerging trade body's suggestion that links are established with ministerial leaders and wider stakeholders seems in keeping with my insistence that everyone is involved in the struggle to advance our values.<sup>53</sup>

Here is a clear suggestion, then, that the Home Secretary strongly favoured the development of a UK-based industry capable of providing innovative capabilities to support national CT objectives, and that such a sector should work closely with Government at all levels. Whilst John Reid would presumably have been unlikely to agree that something resembling a corrosive 'SIC' was under development, this shows how the establishment of a new, systemic exchange between the public and private sectors in the CT sector was being actively encouraged at the highest levels of Government.

JNSRAC had helped to persuade senior policymakers that stronger levels of engagement were needed, and served as a catalyst to the formation of RISC. Its successor organization wasted no time in developing its agenda - the first formal meeting of the new RISC Council took place just weeks later. Revealingly, the new Chairman<sup>54</sup> asked members

---

<sup>53</sup> Reid, 'speech on anti-terrorism measures'

<sup>54</sup> The inaugural Chairman of RISC was Mr. Stephen Phipson, then CEO of Smiths Detection

for ‘any opening points about their aspirations for RISC’<sup>55</sup>; several contributions indicate how commercial matters were not far from the forefront of attendees’ minds with one bullet point expressing, for example, a desire to obtain ‘[a] clearer picture of HMG’s plans and procurement strategy for security to guide private investment decisions’.<sup>56</sup> At the same time, an awareness also existed that any such priorities should not be developed in isolation; the record specifically lists ‘Striking a balance between improving the security of the nation and developing a competitive industrial base’ as one particularly self-aware aspiration. The fact that the meeting also discussed the appropriate Terms of Reference for the Council, launched a new Working Group on international matters, and considered whether funding for a new secretariat would be needed also shows how the organization had embarked upon a highly energetic start-up phase. Whilst no one from Government appears to have attended this meeting, the Home Office’s ‘apologies’ were noted – as was its reassurance that it ‘fully supported the creation and development of RISC, and hoped to engage further in the near future.’<sup>57</sup>

The formal launch of RISC took place during an event at RUSI on 29 March 2007, during which the Home Secretary was ‘delighted’ to deliver the keynote speech.<sup>58</sup> As part of his remarks, Reid referred to RISC as ‘a powerful channel of communication between Government and market in security and resilience’, arguing that industry’s ability to produce and sustain innovation ‘is certainly a vital key to our fight against terrorism’<sup>59</sup>. Given the alliance’s earlier, targeted efforts to secure the participation and support of Government, this would presumably have been seen as a significant victory and certainly a source of great encouragement. The positive energy on display by RISC’s Chairman in the

---

<sup>55</sup> ‘UK Security and Resilience Suppliers Council (RISC) Minutes’, 9 January 2007. Unless otherwise indicated, all subsequent citations in this paragraph are taken from the same.

<sup>56</sup> Ibid.

<sup>57</sup> ‘UK Security and Resilience Suppliers Council (RISC) Minutes’, 9 January 2007

<sup>58</sup> John Reid, ‘Speech to RUSI Launching RISC’, 29 March 2007, Via: [www.riscuk.org](http://www.riscuk.org) (accessed 20.12.11)

<sup>59</sup> Ibid.

media following this high profile announcement would certainly support this: ‘Through the formation of RISC, the UK security and resilience sector will act as one, in concert with government, to deliver a significantly fortified frontline of security and resilience’<sup>60</sup>. His optimistic reflections on the launch and RISC’s potential went even further, as he addressed his high hopes for how industry’s commercial performance could benefit; ‘The dual prize will be stronger economic growth and enhanced national security.’<sup>61</sup> The enthusiasm of those involved can be easily understood: whether for national security or economic reasons, or indeed a mixture of the two, RISC had now been formally endorsed by the Government. Far from worrying about whether it might be seen as a conspiracy, the industry was being open about its objectives - should anyone care to listen.

This chapter has already demonstrated that extensive interaction took place after 7/7 between the UK Government and the security suppliers’ community in forming the JNSRAC and RISC; an organisation which continues to exist today and which clearly remains the Government’s main conduit to the security industry. A recognition of both the national security and economic underpinnings of RISC consistently appeared in the (industry) discussions on the structure and the priorities of the new organization; the alignment of these were seen as positive by the industry, and by some in Government - including the Home Secretary.

#### **6.4 An Effective Mechanism?**

Whilst important, the process of establishing institutions or structures for public-private dialogue on security matters is only one aspect of the cooperation. As this dissertation is also concerned with the character and effectiveness of the implementation of such cooperation it therefore asks: how effectively did RISC develop in practical terms and, in

---

<sup>60</sup> Nicole Kobie, ‘New IT industry alliance to look at national security’, *ITPRO*, 2 April 2007, Via: <http://www.itpro.co.uk/109313/new-it-industry-alliance-to-look-at-national-security#ixzz2yIJQ8Xuj> (accessed 08.04.14)

<sup>61</sup> Ibid.



doing so, has it contributed to the creation of ‘an SIC’ of the character sometimes presented by critics?

As data pertaining to these questions was not previously available, interview participants were invited to comment on the effectiveness of the strategic mechanisms that had been established for public-private cooperation in CT including RISC. A wide variety of viewpoints were offered on the effectiveness of the organization since its establishment and what (if anything) it had actually achieved. For example, a former secretary of RISC, Derek Marshall, was conservative in his estimation of the success that had been achieved; ‘...it seems to me that some progress was made, but I mean it was limited progress.’<sup>62</sup> Comparing the experience of RISC with the arrangements that had long since existed in the defence sector, Marshall stated that the latter was ‘much closer’ and suggested that a deliberate effort was made not to replicate some of the deficiencies associated with that type of engagement in the security sector<sup>63</sup>. Having explained that ‘RISC showed itself to be useful to government in a number of ways’<sup>64</sup>, and that ‘Government lapped that up’<sup>65</sup>, he explained that he could ‘understand why government wouldn’t want to rush into that kind of more deep relationship’ in security<sup>66</sup>. This sense that more could have been achieved was reflected by other industrialists, including one executive who, speaking on the condition of anonymity, explained that he ‘...had seen lots of engagement and discussion but I wouldn’t necessarily describe it as a partnership, or a very loose one if it is.’<sup>67</sup> Another former trade association official, David Evans, described the engagement as ‘a mixed bag’<sup>68</sup>, explaining that the quality of engagement was extremely variable; albeit seeing the Home Office as ‘an open thinking body that saw

---

<sup>62</sup> Interview, Derek Marshall

<sup>63</sup> Ibid.

<sup>64</sup> Ibid.

<sup>65</sup> Ibid.

<sup>66</sup> Ibid.

<sup>67</sup> Interview, Industry Executive

<sup>68</sup> Interview, David Evans

engagement with the private security industry as being important<sup>69</sup>. The desirable end goal for industry, it seems, would be the emergence of a much closer relationship with (and across all relevant parts of) the Government. The existence of such a relationship in the CT sector - a relationship which if established might resonate with the concerns associated with 'the SIC' under consideration - has clearly not yet emerged in many leading industry figures' minds, despite the original vision and intentions of RISC.<sup>70</sup>

For a former Chairman of RISC, there is a more fundamental issue inhibiting progress considered in this way:

I'm not sure that either party to that relationship has thought yet quite carefully enough about what it needs from it. What does government actually want from industry in the security space? We have a partial answer: (...) it wants ideas; it wants ideas for solutions to new problems and all that. But it does tend to look at those very much through a kind of technical lens. It doesn't yet look at them through the eyes of someone who is concerned about efficient procurement.<sup>71</sup>

This view is supported by the first industry secondee to the OSCT who provided an interpretation on how industry was viewed inside the Home Office; 'It appeared to me that the Home Office considered that industry could solve some of the *technical problems* that they were facing, which is why they saw industry as fitting within the Science and Technology unit.'<sup>72</sup> The impact of the decision to locate industry's first ever secondee in the S&T section of the OSCT - not within its strategy unit - should not be understated; it can be reasonably argued that the effect of this would have been to make it more difficult to realize any aspiration to embark upon a more strategic conversation with Government from that location. The decision can be seen as symptomatic of the Government's hesitation - both at the time and arguably today - around the whole issue of industry

---

<sup>69</sup> Ibid.

<sup>70</sup> As reflected by the recommendations and proposals included in the 'Project Gain' report.

<sup>71</sup> Interview, John Howe

<sup>72</sup> Interview, Ogilvie-Smith, (Emphasis added)

engagement; whether or not this is a reassuring outcome will depend on the eye of the beholder.

If correct, the idea that Government and industry have not yet resolved (or even truly embarked upon) a proper, policy-level conversation on what should constitute the scope and priorities of industry's involvement in national security outside technical matters, despite the establishment of RISC, might temper the fears of those who believe that a unified, carefully-considered conspiracy has arisen. On the other hand, critics might be concerned at how this thesis's evidence clearly suggests that some industrialists would wish for an even deeper relationship with Government. The purpose of this section is not to conclude on which of these readings is the correct one; diverging views on the appropriate level of corporate involvement in security are to be expected and, when backed by evidence, extremely welcome. However, any idea that Government and industry have been on exactly 'the same page' with regards to the type, level and character of their engagement through RISC - as the 'SIC-as-conspiracy' theory might suggest - may be seen as a misreading once one understands the frustrations that exist in industry on the limited 'progress' made to date.

This is supported by leading industry figures' recognition of the limitations of even those RISC initiatives that have been looked upon by industry as being 'successful'. One such programme of activity was the creation of a set of joint Industry Advisory Groups (IAGs) that were established by RISC and the OSCT in 2008-09; the 2009 iteration of CONTEST explained that '[t]hrough RISC five joint Industry Advisory Groups have been established in areas of particular importance to this strategy'<sup>73</sup>. The Government outlined the rationale for the groups as:

---

<sup>73</sup> HM Government, 'Pursue, Prevent, Protect, Prepare', p.146 The groups are listed and were formed on the following topics: CBRN, CNI, Information and Communication Technology, Detection of suicide bombers, and Olympic security.

...to better exploit Government-funded research, develop Government requirements, focus private sector investment and enable access to innovation.<sup>74</sup>

Whilst the idea of industry helping to ‘develop requirements’ might set alarm bells ringing amongst those critical of any non-contractual basis for interaction, the impression left upon closer examination is that none of these groups actually delivered many tangible results. It transpires, for example, that significant issues arose within even the most highly praised of these fora; the ‘CNI IAG’. One industry executive aware of the group’s activity responded candidly upon being asked whether the method of engagement proposed for the CNI sector as represented by the ‘Omand Triangle’ (introduced in Chapter 1) had been achieved: ‘I can answer the question: The answer is no.’<sup>75</sup> The executive explained that despite attempts to ‘...create better engagement and capabilities capture, and more support for infrastructure operators, I still think there’s a long way to go[.]’<sup>76</sup> Separately, it can be observed that the Olympic Security IAG<sup>77</sup> did not prevent the emergence of the G4S contract issue.

Some participants were more positive about the overall role played by RISC. Richard Fletcher, for example, described RISC as ‘a sensible idea’, labelling as ‘successful’ what he described as the ‘R&D interface’ between various parts of government and industry.<sup>78</sup> However, he was also clear that some very practical difficulties arose; ‘Inevitably it [RISC] was bedevilled by bureaucratic jealousies within government and considerable commercial jealousies from the private sector.’<sup>79</sup> A separate positive appraisal was provided in interview by an industry executive with an understanding of the

---

<sup>74</sup> Ibid.

<sup>75</sup> Interview, Industry Executive

<sup>76</sup> Ibid. The most significant problems, it was explained, revolved around the question of costs and differing attitudes towards regulation of the CNI.

<sup>77</sup> The author was a member of the Olympic Security IAG

<sup>78</sup> Interview, Richard Fletcher. Industry’s first secondee to the OSCT also cited the ‘technology demonstrators’ that were developed by the OSCT through the (now defunct) ‘INSTINCT’ programme as examples of useful cooperation. Interview, Ogilvie-Smith

<sup>79</sup> Ibid.

OSCT's secondee arrangements. During the conversation, the interviewee was upbeat about the cooperation:

...we actually made a massive amount of progress, I felt, because we were *completely embedded* (...) and we were heavily engaging in really helping at the grass roots. Discussing; informing; putting in what industry would really think. What they would do. What they wouldn't do. How that policy would impact industry.<sup>80</sup>

The idea that because industry was 'embedded' in the OSCT it may have been able to articulate its viewpoint from that position is not a new one; RISC's first industry secondee to the OSCT was involved in the production of a series of booklets published by the Home Office that pertained to the role of industry, for example.<sup>81</sup> Some comments suggest more strongly, however, that the suppliers' community through RISC was seeking to exert greater influence upon Government policy through its engagement. In a discussion on the process around the formulation of the Government's 2012 'National Security Through Technology' (NSST) White Paper<sup>82</sup>, one industry executive explained (on the condition of anonymity) how concerns grew inside the Home Office:

...individuals then got worried that actually maybe industry was having too much of an impact to resolve. We [industry] were far more effective at corralling and inputting, and [...] coming out with logical arguments about why things should go certain ways, than Government was itself. So there was a feeling then that we were having undue influence on policy and strategy as a result of it. We clearly still have a lot of work, behavior to change and trust to build to dispel such fears.<sup>83</sup>

It appears that a view emerged inside the department that the arrangements had to be reined in. Reflecting on why the Government reviewed the scope of industry's involvement

---

<sup>80</sup> Interview, Industry Executive (Emphasis added)

<sup>81</sup> HM Government, 'Ideas and Innovation: How industry and academia can play their part', August 2009, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/97947/ideas-and-innovations.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97947/ideas-and-innovations.pdf) (accessed 30.12.14)

<sup>82</sup> Ministry of Defence, 'National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security', Cm8278, February 2012, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/27390/cm8278.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27390/cm8278.pdf) (accessed 01.15.13)

<sup>83</sup> Interview, Industry Executive

in the policymaking process, one industry executive (speaking on the condition of anonymity) explained;

...it definitely came out as a perception 'they're the private sector, they're all about profit and making money, they can't possibly have the same ethic as the civil service would have. This was disapproved (sic) but it remains a common perception.<sup>84</sup>

Whilst there is no evidence of any specific untoward activity having taken place, it is perhaps reassuring to find that someone in the Home Office was making an assessment of the appropriate level of industry's involvement in contributing to this policy. Following the publication of NSST, the Home Office took steps to establish its own new in-house 'Security Engagement Team' (SIET) headed by a new Director-level appointment. Whilst this decision was ultimately extremely sensible because it promised to develop stronger public-private coordination in the sector, the impression left is that, prior to this, RISC had the ability to affect at least the industry-related aspects of Home Office policy, and that it probably took Government too long to reach the conclusion that it must develop *its own* structures for working with the sector. In short, it may well have relied too heavily on contributions from the private sector that, upon more serious reflection, many (including, it would seem, individuals within Government) could consider as being inappropriate.

This chapter raises important questions about whether an industry body or its representatives should ever be in a position to influence Government policy matters directly. In addition, it also suggests that there is currently very limited (if not an absence of) external or independent oversight of the mechanisms that have been set up inside the Home Office to engage with industry. Whilst reassuring to a certain extent, it appears that only because of the concerns of certain unnamed officials, the scope of industry's involvement was reconsidered. The ad hoc character and lack of transparency around these developments should be viewed, therefore, as unsatisfactory. Without the

---

<sup>84</sup> Ibid.

development of stronger institutional constraints and formal oversight in this area, it is easy to see how the engagement might develop in such a way as to play into the (understandable) worst fears of those who might be concerned about the potential harm that could be done by unchecked cooperation.

It should be recognised that no one in industry would be likely to see the need to apologize for wishing to cooperate closely with Government in the policy space – especially on the development of specific industry-related policies such as NSST. Indeed, the overwhelming sense derived from interviews is that *more* could and should be done to reform and improve the quality of the structures that exist for developing dialogue between Government and security industry. For example, the current secretary of RISC, Mark Phillips, explained in discussing the effectiveness of the current engagement mechanisms:

The biggest issue is how do we ensure that Government has the reach it needs to all elements of the security sector, including those parts of industry who are working on technologies that you might be able to apply (...) in the security space.<sup>85</sup>

This clearly indicates that a view exists even within RISC that the organisation is not yet properly configured. The former CEO of EADS agreed that there is significant room for improvement in how public-private dialogue is developed on security matters, explaining soberly: ‘...do you feel that that’s a genuine conversation going on between industry and government? No, no.’<sup>86</sup> Whilst in making this comment Robin Southwell did not specifically refer to RISC or its performance, that the organisation was expressly set up for this purpose means that his comments can hardly be taken as a ringing endorsement of its

---

<sup>85</sup> Interview, Mark Phillips

<sup>86</sup> Interview, Robin Southwell

activity. The shortage of scholarly contributions covering how the arrangements might be developed or improved is regrettable in this context.<sup>87</sup>

Attitudes within Government on the desirability of engaging with industry at the policy level - and on the effectiveness of RISC for doing so - were also mixed. The Director of the Home Office's Center for Applied Science and Technology (CAST) was generally positive, explaining that RISC had been an important mechanism for Government in helping to engage with the whole sector:

...there are thousands of them that are out there and it is difficult to engage and to communicate. So the trade associations have been a very, very helpful vehicle for that - and therefore coming together as an umbrella under RISC.<sup>88</sup>

Interestingly, whilst recognizing the 'danger (...) of company commercial interests getting in the way of a more collective experience', Rob Coleman saw the opportunity that RISC had to act as 'an unbiased leveller', and even commented on the purported benefits he saw of the advocacy role being performed by the organisation: 'I think you have seen there has been quite a bit of lobbying, and that's not a bad thing - its helping understand some of the positions.'<sup>89</sup> The underlying assumption here appears to be that it should always be the Government who actually determines the policy.

Offering an alternative perspective, a former Head of Strategy at the OSCT, Charlie Edwards, drew on his experience to express doubts around whether it is useful for policymakers to involve the private sector in the policy-making process through organizations such as RISC. Referring to the formulation of the 2011 iteration of CONTEST, he explained:

---

<sup>87</sup> The author has recently sought to stimulate such a debate in Rosemont, 'Private sector engagement'

<sup>88</sup> Interview, Rob Coleman,

<sup>89</sup> Ibid.



...are they [the private sector] really going to provide anything of value to me when I am thinking about CONTEST? Probably not, in terms of thinking about the strategy. But do I want to share CONTEST with them, and understand what the implications are for them? Probably, out of interest, but it's not really going to affect me at all.<sup>90</sup>

Edwards was not the most senior individual to offer such a viewpoint. The former Minister for Security in the Home Office, Lord West, similarly expressed reservations around whether industry should ever be involved in policymaking in this area; 'Policy and strategy are not really the business of the private... of the private enterprises.'<sup>91</sup> He continued: '...that's not really where industry should be. Industry should be coming up with ways of achieving the policy and strategy the government has decided upon.'<sup>92</sup>

For Lord West, then, a clear line must be drawn between the respective roles of Government and industry. The attitude that Government in the form of the Home Office has hitherto merely been looking to industry for technical solutions seems to be prevalent amongst senior representatives of Government; its message certainly seems to have been transmitted across into some parts of industry. In further evidence of this, one executive summarized the engagement as follows; 'I'm not sure the Home Office part of the operation has really felt a need to involve industry in policy and strategy very much. I think they see us more as, well, you know; "we'll tell you what it is and then you can provide it."<sup>93</sup> This may well be the appropriate balance in terms of actually *determining* policy, but it does not necessarily reflect the repeated insistence, found in a number of security policy documents encountered during this research, that the Government *depends* on the private sector to realise the UK's security objectives.<sup>94</sup> Furthermore, it is notable that the attitude is far away from being the sort of cooperation that the GaIN report developed by industry originally envisaged - and that the Home Secretary at the time so warmly welcomed.

---

<sup>90</sup> Interview, Charlie Edwards

<sup>91</sup> Interview, Alan West

<sup>92</sup> Ibid.

<sup>93</sup> Interview, Industry Executive

<sup>94</sup> See footnote 56 (Chapter 1)

That is not to downplay the significance of the recent decision taken and aimed at improving the quality of engagement between Government and industry in the security sector, the appointment of a new 'Director - Security Industry Engagement' within the OSCT in June 2013. This was seen by many interview participants, both from Government and industry, as an important move that promised to considerably strengthen existing arrangements.<sup>95</sup> This thesis benefitted from the first appointee of the role agreeing to participate in the study and being interviewed. In responding to a question on the effectiveness of the strategic engagement to date, and the mechanisms for doing so, Stephen Phipson interestingly contrasted the situation with the arrangements of the defence sector; noting the benefits of the 'uniform market environment', in the case of the latter, where 'if you're in industry you can see the way that works'<sup>96</sup>. Reflecting the opinion of the Head of Industrial Policy at the MoD who believed that his department and industry have 'a good relationship at the strategic level'<sup>97</sup>, Phipson also saw the arrangements as working 'quite well' in defence;

...there's a great deal of exchange between MOD and the prime contractors both in terms of people and in terms of understanding of policy. So it's a pretty robust and mature way of doing business.<sup>98</sup>

Within security, by contrast, Mr. Phipson explained that it is more difficult to develop effective public-private engagement as a result of the widely-recognised perceived 'problem' of coordination in the sector; '...the issue (...) in national security is that we have more than 100 agencies involved[.]'<sup>99</sup> His concise summary of the effect this has on the supporting industry is worth citing as it appears to represent the view of many individuals operating in the security sector:

---

<sup>95</sup> For example, interviews with John Brading, John Howe and Lord West

<sup>96</sup> Interview, Stephen Phipson

<sup>97</sup> Interview, Paul Hamilton

<sup>98</sup> Interview, Stephen Phipson

<sup>99</sup> Ibid.

The fragmented approach from the departmental view in government creates a very fragmented industry underneath it, and so you get varying degrees of policy interaction.<sup>100</sup>

This problem of market ‘fragmentation’, as interviewees and RISC documentation describe it, is a core, defining characteristic of how the post 9/11 UK security market operates. The fact that the defence market possesses one customer, in the MoD, is a key differentiator, explaining why the ‘terms of engagement’<sup>101</sup> look different in that sector, and why they are arguably easier to achieve.

This fundamental difference in the operation of the defence and security ‘markets’ is of deep significance because it calls into question whether it is fitting, or even helpful, to categorize the sectors in the same way. Indeed, a case can be made that, to properly understand the landscape, the types of public-private interaction within each individual national security sub-sector often differ and thus need to be analysed on their own terms. From this perspective, it is easy to conclude that, whilst there may be some common or similar dynamics across different sub-sectors, any suggestion that the MIC has simply transferred into a singular ‘SIC’ would be misleading. Such simplifications do not take account of the complexities that this thesis has examined.

In addition to (and partly as a result of) the highly disaggregated landscape in the non-military security sector, the level and quality of public-private engagement within each sector varies considerably; this often depends on the ‘maturity’ of the policy portfolio and/or the individual approach of the relevant department or agency. In a revealing statement, Phipson described how he saw the variances across government:

I think the interaction on CONTEST, for example, in the Home Office has been quite good, but if you look at the interaction on other ones - absolutely not. Not very clear at all. And there’s lots of them.<sup>102</sup>

---

<sup>100</sup> Ibid.

<sup>101</sup> Footnote 35 (Chapter 1)

<sup>102</sup> Interview, Stephen Phipson

The evidence suggests that the defence and the security sectors operate very differently; as has already been seen in the previous chapters, 'security' is comprised of numerous sub-sectors, many of which can exhibit quite different characteristics. In national security considered in the broadest sense, responsibility for working with industry at the strategic or the programme level tends to be ad hoc and has generally been devolved to individual Government departments. Previous chapters have already demonstrated this fact; e-Borders, FiReControl and G4S Olympic Security contracts were all managed by different parts of Government, for example.

Understanding this 'fragmentation' issue as a core, differentiating, if not unique characteristic of the CT and wider security sector helps to explain why RISC (amongst other individuals and government organizations) has frequently articulated the need for improved levels of coordination in the sector; this argument featured as a core element, for example, in RISC's submission to Government as part of the pre-NSST consultation process.<sup>103</sup> This high level of fragmentation in the sector also illustrates why the core aspects of the Security Industry Director's role (as defined by the job description for the position that was available in 2012) placed such a strong emphasis on the need to coordination both *with industry*, but also, crucially, *across Government*.<sup>104</sup>

Whilst Stephen Phipson's appointment signaled that the Government had accepted responsibility for playing a greater role in working with the security industry, there appears to have been no attempt on either 'side' to pretend that commercial

---

<sup>103</sup> For example, the submission included the statement of the problem as follows: 'There are multiple customers in the national security and resilience sector, many of whom are outside direct Government control, and the fragmentation of demand makes it difficult for the security industry to achieve its potential in supporting national security objectives.' UK Security and Resilience Industry Supplier's Community, *Coordination of national security and resilience* (2011), p.1

<sup>104</sup> As also explained in Rosemont, 'Private sector engagement', the Home Office clarified within the job description for the role that 'it envisioned a number of 'key responsibilities' for the post holder and that these included, amongst others, the coordination of both 'cross-Government interaction with the UK security industry' and 'between the UK CT strategy, CONTEST, the security industry and security export opportunities'. p.151

objectives do not form a central element of the joint agenda. Critics may not welcome this development, but the increasing commercial orientation is perhaps not very surprising. When he was the Chairman of RISC, for example, Mr. Phipson was one of the most vocal proponents of the need for greater policy attention to help the sector realize its economic as well as security potential.<sup>105</sup> Now that he finds himself inside Government, and staffed with a team of over 10 people, he is arguably in an even stronger position to help to generate growth in this budding sector.

### **6.5 Origins and character of strategic engagement through RISC**

The experience of RISC's development - from its earliest inception as JNSRAC to the recent appointment of its first ever Chairman to a senior position in the OSCT - shows how industry and Government have increasingly sought to work closely together to harness the security capabilities and economic potential of the UK-based security sector. In its presentation of a set of new insights, the chapter has shown how the design and structure of the alliance drew much of its inspiration from prior arrangements in the defence sector, and that in this context a desire was expressed at the highest levels of Government for the need to prevent the more detrimental aspects of the MIC transferring into the security sector.

Whether one believes that this stated aspiration was genuine, or indeed successful, the chapter has shown how commercial motivations as well as concerns for national security underpinned both the origins of RISC, and its subsequent activities. Furthermore, the creation and development of this innovative new structure received the support of some of the most senior figures within the UK security policy community and from within industry. Having secured this joint support, a considerable array of new

---

<sup>105</sup> For coverage of Mr. Phipson's programme of policy recommendations presented to an audience at the 2010 Farnborough International Airshow, see; 'Invest in UK national security and resilience industry', *CT Review*, Sept/Oct 2010, pp.1-4

structures and mechanisms were created to improve communication between Government and industry, with the creation of advisory groups and industry secondments among the more innovative and arguably more controversial developments. It is almost perplexing in this context how so little scholarly attention has been devoted to the alliance's activity before now.

Whilst no interview participants were fully satisfied at the level of progress that had been achieved to date by RISC, this chapter has shown how, after 7/7 in particular, a systemic exchange developed and evolved between the Government and industry at the level of policy and strategy - at least insofar as industry issues are concerned. Whether such an exchange should be limited solely to supporting national security objectives is now no longer in question, since a policy agenda has clearly developed (supported by Government) around how best to harness the security industry's economic potential, as well as its role in the implementation of national security strategy. An analysis of how Government and industry have been seeking to realize such economic objectives in practice, and the extent to which other related concerns on the system of interaction in the CT sector may have materialized, follows.

## Chapter 7: Wider issues of concern

### Introduction

Micro-level analysis of three large post-9/11 public sector security contracts and RISC demonstrated considerable proximity in the relationships that have emerged between the public and private sectors in the CT aspects of national security strategy after 9/11. Whilst analysis of the case studies cast doubt on the notion of an 'industrial-complex' in terms of a sinister conspiracy, a network of public-private interaction clearly exists in relation to CONTEST.

This thesis's examination of the character of the private sector's involvement in national security now looks beyond analysis of specific case studies and into some wider characteristics of public-private interaction in CT. This is important because, as argued in Chapter 2, the MIC has historically been considered as a *broader system of interaction* than those revolving around the acquisition of specific capabilities. Chapter 1 introduced how the three additional issues are examined on the basis that they are concerns commonly associated with the MIC, classically conceptualized; this chapter subjects these more general characteristics to scrutiny, examining the extent to which the same (or similar) dynamics are now present in the CT and 'wider security' sector.

The first section of this chapter examines how the phenomenon known as the 'revolving door' - the rotation of government and private sector employees between the public sector and industry - has emerged in the CT sector, analyzing the potential significance of this development. The second section analyses the extent to which economic considerations have played a role in the post 9-11 non-military security sector; consideration is given to whether such dynamics feature in security procurement (as they have done previously in defence acquisition), and to whether employment considerations are a factor in the wider security policy arena. The third section of the chapter examines

the UK Government's emerging emphasis on CT-related security exports, analyzing this trend in the context of its traditional focus on (and the scholarly community's interest in) the support given the defence industry in overseas markets. The consideration of these three themes casts new light on the private sector's involvement in CT - and supports the conclusion drawn from the analysis in previous chapters - that the industrial-complex in the UK's CT sector possesses some of the dynamics associated with the MIC, but operates quite differently in important respects.

### **7.1 The 'Revolving Door'**

Analysis on the MIC has often cited the supposed effect that the phenomenon of one-time public officials joining the defence industry upon their retirement may have had on perpetuating a potentially corrosive system; perhaps even shaping individual contract awards inappropriately. Indeed, the movement of public officials into industry in this way is rarely looked upon positively. Roland, for example, describes the emerging trend as '[a] revolving door shuffled defense executives back and forth despite the evident and egregious conflicts of interest.'<sup>1</sup> The potential dangers of what has been presented as an almost perpetual, rotational phenomenon is also considered by Ledbetter, who identifies how the 'revolving door' came to be associated with what he describes as one of the major 'charges' levelled against the MIC:

...the notion of a revolving door between the military and its contractors was part of the merchants of death thesis back in the 1930s; by the late 1950s it operated on a much larger scale and in peacetime.<sup>2</sup>

The idea put forward by critics including Hughes and Wedel and Kennan, then, is that a corrosive system has emerged whereby (normally senior) former defence officials routinely

---

<sup>1</sup> Roland, 'The military-industrial complex', p.360

<sup>2</sup> Ledbetter, *Unwarranted Influence*, p.113



leave public service to take up well-paid jobs in industry, or in some cases vice versa.<sup>3</sup> Through this process, such officials are seen to adopt a vested commercial interest in promoting ever higher levels of defence spending - both generally, but also potentially in relation to certain capability areas or specific contracts. Such individuals are said to assist their companies by drawing on their pre-existing access, gained through prior Government service, to decision-makers and a wider network of contacts. In this way, it is argued, they can help to identify opportunities and influence future defence business decisions, advising their companies throughout on their strategic development. The suggested outcome is that the 'revolving door' dynamic contributes towards an inappropriate level of public-private engagement that ultimately helps defence companies make large sums of money.

The resulting popular image of the 'revolving door', therefore, is one of former public servants 'cashing in' and operating in a self-interested fashion in their attempts to bear influence upon defence acquisition. A recent story in *The Telegraph* newspaper neatly illustrates the disdain with which the dynamic can often be portrayed; it sought to implicate a number of former senior military officials for their involvement in assisting a fictional Korean company secure defence contracts, before presenting a view of the scale of the problem:

In 2009/10, the latest year for which full figures are available, 326 officers or MoD officials were cleared to join the private sector. Of these, 240 went to defence companies. Fully 20 were generals, admirals or air marshals.<sup>4</sup>

Investigative journalists are not alone in identifying (or being uncomfortable with) the circulation of employees between Government and industry in the national security sector; political campaigns have even been launched to challenge the processes around the practice. The UK-based Campaign Against the Arms Trade (CAAT), for example, considers the 'revolving door' to be 'a key feature of the relationship between the Government and

---

<sup>3</sup> Hughes, *War on Terror, Inc.*; Wedel and Keenan, 'Shadow Elite: Eisenhower's Dark Vision Realized'

<sup>4</sup> Andrew Gilligan, 'MoD lobbying claims: The muck and the top brass', *telegraph.co.uk*, 15 October 2012, Via: <http://www.telegraph.co.uk/news/uknews/defence/9608493/MoD-lobbying-claims-The-muck-and-the-top-brass.html> (accessed 26.02.14)

military industry'<sup>5</sup> and, in support of its overall aim 'to end the international arms trade'<sup>6</sup>, includes a 'Revolving Door Log' on its website to highlight what it sees as some of the most regrettable high profile appointments.<sup>7</sup> Another NGO, Transparency International (TI), aims to eliminate corruption in the defence and security sectors and has similarly published work on the 'revolving door'. A TI Working Paper on this subject identifies 'defence' as a sector that is 'particularly prone to the revolving door phenomenon'<sup>8</sup>, stating what it sees as the risks arising from the dynamic:

Increased interaction between business and government has also meant increased opportunities for corruption. A rise in conflicts of interest, and the creation of a 'revolving door' in government, demonstrates the thinning of boundaries between the public and private spheres.<sup>9</sup>

Such is the dominant tone of most analysis on the 'revolving door' phenomenon in the defence sector. This is notwithstanding the fact that many people in Government and industry have presumably seen the benefits of the practice, as supported by the employment dynamics evident in this chapter.

The main question for this section of the dissertation is whether since 9/11 there has been evidence of such a 'revolving door' existing in the non-military CT and other associated sectors. In line with this thesis's broader enquiry, it is important to consider the impact that the any such phenomenon may have on non-military security policy and expenditure; the effect of this type of public-private interaction has hitherto been in short supply in literature on the 'SIC'.

---

<sup>5</sup> 'Political Influence', CAAT Website, Via: <http://www.caat.org.uk/issues/influence/> (accessed 26.03.14)

<sup>6</sup> 'About CAAT', CAAT Website, Via: <http://www.caat.org.uk/about/> (accessed 26.03.14)

<sup>7</sup> 'Revolving Door Log', CAAT Website, Via: <http://www.caat.org.uk/issues/influence/revolving-door.php> (accessed 26.03.14)

<sup>8</sup> Tinatin Ninua, 'Regulating the Revolving Door', Transparency International Working Paper #06/2010, 1 June 2010, Via: [http://www.transparency.org/whatwedo/pub/working\\_paper\\_06\\_2010\\_regulating\\_the\\_revolving\\_door](http://www.transparency.org/whatwedo/pub/working_paper_06_2010_regulating_the_revolving_door), (accessed 26.03.14), p.1

<sup>9</sup> Ibid.

Interview data revealed a variety of attitudes on how the 'revolving door' operates in the UK's national security arena. Describing the character of the private sector's involvement in national security strategy, Omand identified the following dynamic:

If we were looking at general national security strategy, which of course is dominated by defence, then I think the relationship could be described as circular. Companies that are major defence suppliers tend to employ retired service personnel to advise them on future requirements and future direction of policy which could then help target research and development (...)[.]<sup>10</sup>

Omand also explained that, generally, such dynamics operate differently in the security and intelligence sectors; '...particularly in the internet age where thought leadership is as much in the private sector as the public sector'.<sup>11</sup> Whilst Omand stated that he had not 'come across many cases where the private sector really has views on the future direction of policy as against the future direction of, say, the equipment programme'<sup>12</sup>, the fact that such a senior former Government official - one that has operated at highest levels of both the defence and security sectors - believes that there may be increased scope for the private sector to contribute ideas on policy matters suggests that further consideration of this issue is needed.<sup>13</sup> The relevant point for this thesis is that the 'revolving door' within the industrial-complex in CT exhibits different characteristics when contrasted with defence.

Further analysis confirms the movement of employees between the Government and the private sector in the non-military security sector. An examination into the employment history of the individuals involved in interviews for this research reveals significant rotation. As Appendix B outlines, 15 of the 26 interviewees had during the course of their careers worked in more than one of the interview categories (i.e. in

---

<sup>10</sup> Interview, David Omand

<sup>11</sup> Ibid.

<sup>12</sup> Ibid.

<sup>13</sup> It could be asked, for example, how in this context it will be possible to maintain appropriate mechanisms of policy oversight and accountability in this sector.

Government, industry or academia).<sup>14</sup> Amongst them, it is notable that one former Chairman of RISC, John Howe, had been a Deputy Chief of Defence Procurement before joining industry (for Thales UK) in 2000.<sup>15</sup>

Analysis of the employment movements of those involved in contracts examined in Chapters 3-5 is also revealing. In the case of FiReControl, for example, EADs's Policy Adviser between 2005-2009, Richard Fletcher, was a one-time 'career official in British Intelligence & Security Organisations between 1966 and 1998'<sup>16</sup>. Regarding e-Borders, one industry executive speaking on the condition of anonymity identified the prominence with which one independent consultant, Mr. John Yard, helped Raytheon Systems to secure the IT contract; Mr. Yard's biography appearing on a company website confirms that he provided advice to Raytheon on their successful bid.<sup>17</sup> Significantly, Mr. Yard's short résumé both indicates that he was a former senior civil servant and that the positions he occupied appeared to serve as a highly marketable quality; 'His wide experience on *both sides of the fence* means that he is constantly in demand and he has often been brought in to help resolve problem contracts.'<sup>18</sup> Mr. Yard was not the only individual involved in e-Borders to have moved from the public sector and into industry; Ms. Brooke Hoskins, identified as Raytheon's programme director for the project<sup>19</sup>, had previously served at the Department of Trade and Industry.<sup>20</sup> Whether a more appropriate metaphor is 'hopping over fences' or 'whirling through revolving doors', two figures associated with Raytheon's e-Borders contract bid had once worked in senior Government positions.

---

<sup>14</sup> Appendix B, p.316

<sup>15</sup> 'John Francis HOWE', Debretts.com, Via: <http://www.debretts.com/people-of-today/profile/819/John-Francis-HOWE> (accessed 19.01.15)

<sup>16</sup> 'Richard Fletcher', Anthem Corporate Finance Website, Via: <http://www.anthemcf.com/team-senioradvisor-RichardFletcher.html> (accessed 26.03.14)

<sup>17</sup> 'John Yard', CIO Development Website, Via: <http://www.ciodevelopment.com/about-us/john-yard/> (accessed 26.03.14)

<sup>18</sup> Ibid. (Emphasis added)

<sup>19</sup> Andrew Jack, 'Britain set to test pioneering 'e-borders' monitoring system', *Financial Times*, 4 August 2008.

<sup>20</sup> 'NMI appoints Neul CEO Stan Boland as chairman', NMI Website, Via: <http://archive.nmi.org.uk/news/press-releases/nmi-stan-boland> (accessed 30.12.14)

Research into the employment dynamics around London 2012 security also reveals considerable movement between the public and private sectors; especially after the Games. At least four senior public officials involved in various phases of the planning and implementation - Tarique Ghaffur<sup>21</sup>, Robert Raine<sup>22</sup>, Chris Scott<sup>23</sup>, and Steve Cooper<sup>24</sup> - are known to have established their own private independent security consultancies after the Games, for example; it is understood that the latter two have provided support to FCO Services for support to the UK's burgeoning Government-to-Government (G2G) security export drive (see section 7.3 below). Regarding the G4S manpower security contract, by contrast, some of the employment movements were rotational but less traditional in character. Firstly, the former Director of Events for G4S, Mr. Paul Bullen, was LOCOG's 'Senior Contract Performance Manager'<sup>25</sup>; some awareness of G4S's operations would therefore have been known by the Olympic organisers. Secondly, the author is aware that the UK Home Office seconded a senior official to G4S in the run up to the Games. That the Home Office had a 'man on the inside' reinforces the idea of a 'revolving door' existing in the non-military CT area. It also supports the portrayal in Chapter 5 of an extensive level of interaction between the public and private sectors on London 2012 security.

Evidence of a 'revolving door' existing in the security sector extends beyond individuals operating at the operational level and into some more strategic positions. For example, the former Home Secretary and original Ministerial supporter of the establishment of RISC, John Reid, has been criticized for accepting an appointment as a senior adviser to G4S.<sup>26</sup> Furthermore, two recent Government Ministers of Security - Lord

---

<sup>21</sup> Formerly the Olympic Security Coordinator within the Metropolitan Police Service

<sup>22</sup> Formerly the Home Office Director of the Olympic Security and Safety Programme

<sup>23</sup> Formerly Head of Olympic Security Prepare Programme in the Home Office

<sup>24</sup> Formerly the Head of Security at the Olympic Delivery Authority

<sup>25</sup> 4Global, 'Testimonials', Via: <http://www.fourglobal.org/experience/testimonials.aspx> (accessed 31.08.14)

<sup>26</sup> Claire Sambrook, 'Surveillance + detention = £Billions: How Labour's friends are 'securing your world'', *opendemocracy.net*, 13 April 2010, Via: <http://www.opendemocracy.net/ourkingdom/clare->

West and Baroness Pauline Neville-Jones - have alternated between public service and private sector employment; prior to their appointments both worked (as a senior adviser and Chairman respectively) for the same UK technology company, QinetiQ, which provides technological security solutions.<sup>27</sup> Both previously held senior positions in the Armed Forces and the Foreign and Commonwealth Office, respectively. Similar employment movements are also evident amongst those who have served under such Ministers; upon the completion of his duties as Lady Neville-Jones' special adviser before the 2010 General Election, for example, Mark Phillips was appointed first as a Research Fellow at the Royal United Services Institute (RUSI) and, latterly (in 2012) as Security Policy Adviser to the ADS Group.<sup>28</sup> Employment rotation clearly exists in the most senior UK security policy circles<sup>29</sup>, but whether the appointment of 'security industry veterans' and their advisers to senior positions in Government and industry makes it more likely that certain security solutions are adopted, as suggested by Hughes<sup>30</sup>, is debatable. Whilst Ministers may be the ultimate decision-makers for public security procurements - and indeed their cancellation - it should be noted that they are not the only individuals involved in shaping such requirements.

Similar dynamics exist at senior official level. Most significant amongst these is the June 2013 appointment of Mr. Stephen Phipson as 'Director - Security Industry Engagement' within the OSCT. The reasons for this appointment have been analysed elsewhere<sup>31</sup>; suffice to note for present purposes that, prior to his appointment, Mr. Phipson had been the President of one of the UK's leading security technology companies, Smiths Detection. Perhaps more significantly, Mr. Phipson had also served as the inaugural

---

[sambrook/surveillance-detention-%C2%A3billions-how-labour%E2%80%99s-friends-are-%E2%80%98securing-your-w](#) (accessed 27.03.14)

<sup>27</sup> Hughes, *War on Terror Inc.*, p.230

<sup>28</sup> 'Register of Interests of Lords Members' Staff', Via: [www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests/register-of-interests-of-lords-members-staff/?letter=N](http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests/register-of-interests-of-lords-members-staff/?letter=N) (accessed 26.02.14)

<sup>29</sup> Pun not originally intended.

<sup>30</sup> Hughes, *War on Terror Inc.*, p.230

<sup>31</sup> Rosemont, 'Private sector engagement', pp.147-61

Chairman of RISC and Vice President of Security for the Trade Association ADS - roles which contributed to him receiving a CBE for services to the security industry in 2010.<sup>32</sup> That such a prominent, recognised one-time leader of the security industry has been given formal responsibility for engaging with the security industry on behalf of the Government is a particularly illuminating indicator of the 'revolving door' in action. Indeed, the Government was clearly proud of having secured Mr. Phipson's services for this very reason; outlining the Home Office's new plans for industrial engagement and the appointment, the UK's Security Minister explained that 'Stephen Phipson (...) brings with him a wealth of industry experience, knowledge and know-how which will be invaluable to this agenda.'<sup>33</sup>

For the avoidance of doubt, research conducted for this thesis revealed no evidence suggesting anything inherently problematic about the nature of such appointments. That being said, conversations with some interviewees gave the possibly worrying impression that some industry figures believe that they now have 'a man on the inside' of Government. Asked about the state of the effectiveness of the Government's new mechanisms for security industry engagement, for example, one industry executive replied:

...we have high hopes for Stephen Phipson and his team in the Home Office now as being *a voice of industry inside* and a trusted channel for communicating with.<sup>34</sup>

Whilst this is not read as being indicative of any sinister motivation, it suggests that some perceptions of the postholder's proper functions may be misguided. Ideally, the new Director should be there to develop the *Government's* engagement and relationship with the security industry and not vice versa. Whilst some shared objectives have already

---

<sup>32</sup> Edmund Tobin, 'CHIGWELL: CBE for security firm executive', *East London and West Essex Guardian*, 26 October 2010, Via: [http://www.guardian-series.co.uk/news/8475939.CHIGWELL\\_CBE\\_for\\_security\\_firm\\_executive/](http://www.guardian-series.co.uk/news/8475939.CHIGWELL_CBE_for_security_firm_executive/) (accessed 31.08.14)

<sup>33</sup> James Brokenshire, 'Securing Asia 2013: James Brokenshire's Special Address', 25 June 2013, Via: <https://www.gov.uk/government/speeches/using-international-partnerships-to-tackle-the-threat-of-global-terrorism> (accessed 12.05.14)

<sup>34</sup> Interview, Industry Executive (Emphasis added)

emerged (see section 7.3 on security exports), the position was presumably not designed to act on industry's behalf or established to serve its interests; it is to *lead the Government's engagement* with industry.

Only time will determine the character and effectiveness of the appointment. Interestingly, one interviewee expressed concern for Mr. Phipson in view of the commercial approaches that he had been seen to have so far adopted:

I fear for his longevity in the government to be honest, because I think that he's ruffling feathers - rightly so in my opinion, and God bless him for doing it - but he is ruffling feathers to get things done. And you know that's not how Government works.<sup>35</sup>

Regardless of whether the Home Office will eventually see Mr. Phipson's contribution as 'invaluable', its selection of this former industrialist as one of the Government's own senior officials is perhaps the ultimate representation of the 'revolving door' operating in CT.

Mr. Phipson's appointment is not the only example of former industry officials working at the OSCT; in 2008 the OSCT invited RISC to help it recruit for the position of 'industry secondee' to help manage the relationship. After a competitive recruitment procedure co-managed with industry, Adam Ogilvie-Smith (then of Thales UK) was the first appointee of this co-funded position; one he held from 2009 to 2011.<sup>36</sup> Subsequently, Alan Jenkinson of IBM was the second secondee to be recruited into the OSCT's position for industrial liaison. The appointment of around a dozen officials within the OSCT's SIET following its establishment in 2012 appears to have halted the recruitment of further secondees from RISC, thus perhaps removing the need to question the desirability of such a funding arrangement. Nevertheless, the appointment of joint RISC/OSCT secondees is further evidence of the 'revolving door' in CT.

---

<sup>35</sup> Interview, Industry Executive

<sup>36</sup> 'Profile for Adam-Ogilvie-Smith', Robert Gordon University Website, Via: <http://www.rgu.ac.uk/dmstaff/adam-ogilvie-smith> (accessed 27.01.14)



In Chapters 3-5 the involvement of consultants in managing security contracts or other government security programmes was noted and there is additional evidence that the OSCT has appointed other non-governmental experts to senior policy positions. Notable amongst these was the appointment of Charlie Edwards, on secondment from the Demos Think Tank<sup>37</sup>, as the Deputy Director for Strategy and Planning in the department, tasked with responsibility for developing the 2011 iteration of CONTEST.<sup>38</sup> The appropriateness of appointing a think tank secondee to such a senior security policy position is an interesting question; whilst there is no doubting the individual's personal expertise and qualifications, an unusual precedent may have been set owing to the fact that an outside expert was tasked to actually develop (i.e. not merely contribute to) strategy in one of the most sensitive areas of Government security policy.

This thesis is concerned with what it calls the 'industrial-complex' in the UK's CT sector specifically; its analysis on any 'revolving door' would not be complete, however, without considering how such a dynamic may be operating at the EU level. This is important because, whilst a full empirical analysis of the UK's EU CT involvement is outside the scope of this dissertation, significant aspects of security industrial policy relevant to the UK are increasingly being developed from Brussels.<sup>39</sup> It is relevant, therefore, to note the recent controversy surrounding the rotation of a senior EU security official on secondment into a security company (and back again). According to the Corporate Europe Observatory (CEO), the decision by the European Commission to approve Magnus Ovilius's<sup>40</sup> sabbatical

---

<sup>37</sup> 'Mr Charlie Edwards', CSaP Website, Via: <http://www.csap.cam.ac.uk/network/charlie-edwards/> (accessed 27.03.14)

<sup>38</sup> 'Charlie Edwards', Demos Website, Via: <http://www.demos.co.uk/people/charlieedwards> (accessed 27.03.14)

<sup>39</sup> For example, the Commission published a 'security industrial policy communication' in July 2012. European Commission, Communication from the Commission to the European Parliament, The Council and the European Economic and Social Committee, Policy 'Action Plan for an innovative and competitive Security Industry', Brussels, 26 July 2012, COM(2012) 417 final, Via: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF> (accessed 03.05.14)

<sup>40</sup> Previously the Director General for Justice, Freedom and Security, Head of Sector, Preparedness and Crisis Management at the European Commission

to Smiths Detection in 2008 ‘provokes important questions about how the Commission handles the risk of conflicts of interest.’<sup>41</sup> In the opinion of CEO, the Commission:

...should have been more sensitive to the potential conflicts of interest arising when a staff member goes on sabbatical to be employed in a sector related to his EU post and particularly where there is a lobbying element to the new work.<sup>42</sup>

The lobbying role that Mr. Ovilius would be expected to undertake upon his appointment as the Vice President of Government Relations for SD was seen as inappropriate by CEO. This prompted the organization to write an official letter to the Commission in December 2013, requesting details on both whether he had returned to the organization and the assessment process for doing so.<sup>43</sup> According to the Commission’s carefully-worded response, Mr. Ovilius was ‘reintegrated’ into a new role at the Commission in March 2013 after the following process had been completed:

Before the reintegration of Mr Ovilius, the absence of links between his former position at Smiths Group (a multinational diversified engineering company) and his future possible post at the Commission, and any potential risks of conflicts of interests were thoroughly assessed, so as to ensure that there was a complete absence of conflict of interest on his return to the Commission.<sup>44</sup>

Choosing to highlight this case study is not to suggest that in the course of any of his duties Mr. Ovilius behaved in any inappropriate manner, or that his ‘reintegration’ into a border management (not security-specific) role<sup>45</sup> was not carefully considered. It nevertheless

---

<sup>41</sup> ‘RevolvingDoorWatch Cases – Magnus Ovilius’, *Corporate Europe Observatory Website*, Via: <http://corporateeurope.org/revolvingdoorwatch/case/Magnus-Ovilius> (accessed 28.03.14)

<sup>42</sup> Ibid.

<sup>43</sup> Vicky Cann, ‘Magnus Ovilius and sabbatical’, Letter to Human Resources and Security, European Commission, 20 December 2013, Via: [http://www.asktheeu.org/en/request/magnus\\_ovilius\\_and\\_sabbatical](http://www.asktheeu.org/en/request/magnus_ovilius_and_sabbatical) (accessed 28.03.14)

<sup>44</sup> Irene Souka, ‘Your application for access to documents - Ref GestDem No 2014/31’, Letter to Vicky Cann from European Commission, Directorate-General Human Resources and Security, 27 March 2014, Via: <http://www.asktheeu.org/en/request/1111/response/4515/attach/3/Signed%20letter%20by%20Ms%20Souka.pdf> (accessed 28.03.14)

<sup>45</sup> Mr Ovilius was appointed as Policy Officer responsible for ‘ensuring the proper management and functioning of the European Migration Network (EMN)’. Ibid.

provides a useful indication that a security-related 'revolving door' appears to be operating at EU level.

It is worth considering how the revolving door might operate in security sub-sectors other than CT in view of Omand's earlier suggestion on how it operates differently than in defence. Certainly, some former UK government officials working on cyber security policy have moved into industry; Graham Wright's move to Northrop Grumman in 2011 from his position as Deputy Director of the Office of Cyber Security and Information Assurance is one such example.<sup>46</sup> This is not an isolated transition; the former Director General for Information Security and Assurance at GCHQ, Nick Hopkinson, became the Director of Cyber Security at CSC<sup>47</sup> and, additionally, John Suffolk took up the position as the Global Cyber Security Officer for Huawei Technologies in October 2010<sup>48</sup>. Evidence of a revolving door operating in this sector clearly connects to the suggestion that a 'cyber-industrial complex' may be emerging<sup>49</sup>; this thesis's conclusion considers how its findings in the CT sector might relate to research on any broader type of 'SIC'.

With regards to this dynamic existing in other non-military UK security sectors, the recent case of the former Chairman of the Serious and Organised Crime Agency, Sir Ian Andrews, provides a relevant example, with a controversy emerging in August 2013 when he resigned from his position after he 'had failed to declare his directorship in a management consultancy company, Abis Partnership.'<sup>50</sup> It is also not uncommon for senior

---

<sup>46</sup> 'Northrop Grumman Appoints Graham Wright and Kathy Salyan to Key Cyber Security and Intelligence-Related Roles in the UK', Northrop Grumman News Release, 4 January 2011, Via: [http://www.irconnect.com/noc/press/pages/news\\_releases.html?d=210183](http://www.irconnect.com/noc/press/pages/news_releases.html?d=210183) (accessed 28.03.14)

<sup>47</sup> Advisory Committee on Business Appointments, The Advisory Committee on Business Appointments, Twelfth Annual Report 2010-2011, Via: <http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/acoba/assets/acobatwelfthreport2010-2011.pdf> (accessed 28.03.14), p.53

<sup>48</sup> Advisory Committee on Business Appointments, The Advisory Committee on Business Appointments, Thirteenth Annual Report 2011-2012, Via: <http://acoba.independent.gov.uk/media/26724/acoba%20thirteenth%20annual%20report%202011-12.pdf> (accessed 28.03.14), p.64

<sup>49</sup> Brito and Watkins, 'Loving the Cyber Bomb?'

<sup>50</sup> 'Soca chairman resigns over undeclared directorship', BBC News, 1 August 2013, Via: <http://www.bbc.com/news/uk-23537513> (accessed 28.03.14). An unfortunate additional irony of

retired UK intelligence and police officials to accept security-related jobs in the private sector. Amongst the most prominent of these, a former Director General of MI5, Lord (Jonathan) Evans, recently became a Non-Executive Director at HSBC Holdings plc.<sup>51</sup> Earlier, Sir David Pepper's application to become a Strategic Adviser for the consultancy firm, Defence Strategy & Solutions LLP, and his role as a member of the Advisory Board for Thales UK, was approved in 2009.<sup>52</sup> In addition, Sir David Omand - cited as a leading author on the private sector's involvement in national security throughout this thesis - was granted approval in 2005 to become an Adviser for SBAC.<sup>53</sup> Sir Richard Mottram - cited as a key figure in the development of RISC in Chapter 6 - has moved in and out of Government since leaving the Cabinet Office, at one stage (between 2008-2014) serving simultaneously as the Chairman of the board of Amey PLC and of the Defence Science and Technology Laboratory (DSTL).<sup>54</sup> Finally, within the policing sector, *the Financial Times* has reported on the practice of senior officers - including two former Commissioners of London's Metropolitan Police Service - taking jobs in the security industry upon their retirement.<sup>55</sup>

Three points should be made in assessing the character of the 'revolving door' in the CT and 'wider security' sector. Firstly, clearly not everyone supports the practice whereby Government security officials take up related commercial roles either before or after their appointments. Whilst he is not alone in his criticism, Hughes is perhaps the most

---

this episode was that Sir Ian's wife, Moira Andrews, was also reported to be the Head Lawyer of a private security and investigations consultancy known as the Good Governance Group.

<sup>51</sup> 'Appointments taken up by former Crown servants', Advisory Committee on Business Appointments Website, Via:

[http://acoba.independent.gov.uk/former\\_crown\\_servants/former\\_crown\\_servants\\_appointments\\_2012.aspx](http://acoba.independent.gov.uk/former_crown_servants/former_crown_servants_appointments_2012.aspx) (accessed 28.03.14)

<sup>52</sup> Advisory Committee on Business Appointments, Eleventh Report 2009-2010, Via:

<http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/20565/acobaeleventhreport2009-2010.pdf> (accessed 28.03.14), p.29

<sup>53</sup> Advisory Committee on Business Appointments, Eighth Report 2005-2006, Via:

[http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/acoba/assets/acoba eighthreport2005\\_06.pdf](http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/acoba/assets/acoba eighthreport2005_06.pdf) (accessed 28.03.14), p.29

<sup>54</sup> 'Sir Richard Mottram', CSaP Website, Via: <http://www.csap.cam.ac.uk/network/richard-mottram/> (accessed 18.01.15)

<sup>55</sup> Andrew Bounds and Helen Warrell, 'Senior City police detective decamps to private sector', *Financial Times*, 21 February 2014

vocal critic of this phenomenon. In *War on Terror Inc.*, he makes bold statements about the corrosiveness of this phenomenon; such was the erosion of the boundaries between public and private sector employees after 9/11, he argues, that it became 'impossible to tell who was driving British security policy - permanent officials or the directors of private companies.'<sup>56</sup> It is important to note, however, that his work declines to make any mention of the formal processes that exist around such appointments - specifically the formal approval mechanism that exists in the UK in the form the Advisory Committee on Business Appointments (ACBA) - and does not produce substantive data on specific acts of wrongdoing (such as corruption) to which the tone of his work alludes. Were such evidence to be provided then it would be reasonable to contemplate the desirability of an 'SIC' existing along the lines popularly envisaged; in the absence of such material, it seems premature to draw on the employment movements illustrated in this chapter as conclusive evidence that a conspiracy exists.

A second key consideration arising from this analysis of the 'revolving door' in CT is that the overlap that now exists between defence and security complicates the picture considerably. Whilst the above provides evidence of Government CT or security officials (i.e. not military personnel) taking up non-military security opportunities in the private sector, the reality is that examples abound of individuals providing advice *across* both sectors, and/or serving companies who operate in both sectors. In addition to having provided advice to the SBAC, for example, David Omand has also served as both a senior director of the Babcock management team and a non-Executive Director of Finmeccanica<sup>57</sup>; both these companies' interests include security but are also (if not primarily) associated with the defence sector. Similarly, it is not only intelligence or public officials working on security-related issues who have later secured employment in the

---

<sup>56</sup> Hughes, *War on Terror Inc.*, p.232

<sup>57</sup> 'Management Team', Babcock Plc Website, Via: <http://www.babcockinternational.com/mobile/about-us/management-team/> (accessed 28.03.14)

security sector; there is now evidence of diplomats<sup>58</sup> and military officials<sup>59</sup> moving to work in the non-military security industry. It is crucial to take these evolving dynamics into consideration in our analysis of contemporary government-industry interaction; at this stage it can be tentatively suggested that the ‘overlap’ in the character of revolving door identified above supports the idea that in a contemporary context we might do well to continue to explore the potential emergence of a ‘national security-industrial complex’ even more broadly defined.

Finally, substantive evidence has been obtained in the course of this research to suggest that the ‘revolving door’ dynamic is by no means limited to the defence and security sectors - even a cursory review of the annual reports of the ACBA illustrates that such employment movements occur across the breadth of the public sector. Supporting this observation, a recent BBC radio documentary, ‘The Accountant Kings’, focused on the use that is now made of secondments from large accountancy firms like KPMG and CAPITA within the National Health Service. The reaction of one senior KPMG consultant to the programme’s exploration into whether the Government’s use of secondments ‘all looks a bit cosy’ was as follows:

I think we as a profession have been probably a little stunned by some of the reaction to secondments. I mean we see secondments as a way in which we can give better value provision of experienced resource into departments, for example. Its great training for the individuals and they receive a different exposure to a different set of organizations and challenges and so on. We get them back with experience of different

---

<sup>58</sup> For example, following his retirement from the FCO, Sir William Patey KCMG became ‘Foreign Affairs Adviser’ for the strategy security and risk advisory firm, Control Risks. Advisory Committee on Business Appointments, Thirteenth Annual Report 2011-2012, Via: <http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/26724/acoba%20thirteenth%20annual%20report%202011-12.pdf> (accessed 28.03.14), p.61

<sup>59</sup> For example, Lieutenant General Sir Gary Coward KBE CB became a non-executive Director of Redline Aviation Security Ltd following his retirement from the Army in October 2012. Advisory Committee on Business Appointments, Fourteenth Report 2012-2013, Via: <http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/29744/acoba%2012-13%20annual%20report.pdf> (accessed 28.03.14), p.60

things, in the same way that we might second them to a charity or to a company aswell. We've definitely seen it as mutually beneficial [.]<sup>60</sup>

Asked to respond to criticism that private consultancies are merely serving their own interests through such secondments, Mr. Collins replied:

I think it's a million miles away from being capable of being characterized as us drafting policy or, you know just... it just doesn't feel like that. That isn't the substance of it. That isn't the intention of it - either in the government or the private sector.<sup>61</sup>

It is timely to question the appropriateness of the increasing use of private sector secondments in policy departments (if not policy roles) - many senior political figures including the Chairman of the PAC have also recently done so.<sup>62</sup> It can also be noted that whilst there may be a trend towards greater transparency around the use of consultants or secondments in and around Government, this in itself does not necessarily mean that the practice is desirable. However, there is also an additional possible explanation for the use of private sector employees in government in this way - that the additional capacity is genuinely needed. This view certainly resonates with the interviews conducted for this thesis; whilst the 'revolving door' clearly exists in the CT arena, this practice appears to have been pursued to boost capacity on either 'side' and no evidence has been found that such movement is hidden, or that any untoward behaviour is taking place. That such dynamics clearly also exist outside the military sector should perhaps not surprise observers; it does however inform our conceptualization of the industrial-complex in CT.

## **7.2 Economic Emphasis - Procurement and Employment**

---

<sup>60</sup> 'The Accountant Kings', BBC File on 4 Documentary, 9 March 2014, Via: <http://www.bbc.co.uk/programmes/b03wpjig> (accessed 30.03.14)

<sup>61</sup> Ibid.

<sup>62</sup> Polly Toynbee, 'Accountancy's Big Four are laughing all the way to the tax office', theguardian.com, 1 February 2013, Via: <http://www.theguardian.com/commentisfree/2013/feb/01/accountancy-big-four-laugh-tax-office> (accessed 30.03.14)

This section considers, and contrasts with comparable arrangements in defence, the character of the existing overall structures for managing non-military security procurement. In the process, it considers the extent to which employment considerations have (or have not) become a factor in Government investment or decision-making in this arena.

The operation of acquisition institutions within the defence sector has long been subject to scholarly criticism; some authors have questioned, for example, the desirability of the presence of industrial considerations in the sector.<sup>63</sup> Harsher critics see these aspects of military-industrial cooperation as further evidence of the harmful nature of the system; CAAT is openly critical, for example, of public money being allocated to companies through the defence procurement system<sup>64</sup>, and actively seeks to close the UKTI Defence and Security Organisation (DSO) - the body responsible for supporting companies on military-related UK exports.<sup>65</sup> The management and operation of the UK's procurement system has also attracted significant scholarly scrutiny; even supporters of industry's role in supporting the military have criticized the lack of effectiveness in defence acquisition.<sup>66</sup> Certainly, UK defence procurement has not operated perfectly. To properly examine the character of the private sector's involvement in the non-military aspects of contemporary national security, this section considers whether procurement in security sectors such as CT exhibit the same characteristics and systemic failures as defence; this helps to explore whether an 'industrial-complex' of the same type as the MIC now exists in other areas of security.

---

<sup>63</sup> For a critique of the pursuit of economic interests within the defence sector see Feuchtwanger, *The Best Kit*

<sup>64</sup> At the time of writing the CAAT is promoting a campaign titled 'Time to Shift Priorities' which calls 'for military spending to be redirected to meet human needs'. 'Home', Global Day of Action on Military Spending UK website, Via: <http://demilitarize.org.uk/> (accessed 01.04.14)

<sup>65</sup> 'UKTI: Armed & Dangerous', CAAT Website, Via: <http://www.caat.org.uk/issues/ukti/> (accessed 01.04.14)

<sup>66</sup> See, for example, Page, *Lions, Donkeys and Dinosaurs*. The House of Commons Defence Select Committee has also often been robust in its criticism of the MoD's acquisition process.



Data gathered during interviews shows the character of the 'security market' differs significantly when contrasted with defence; including in relation to the structure and operation of what might generously be called the security procurement 'system'. RISC's first secondee to the OSCT identified, for example, how the procurement structure in security is considerably more diverse and disaggregated, comprising 'many purchasers' when compared to defence.<sup>67</sup> A former Chairman of RISC amplified the point, highlighting the significance of the contrasting arrangements:

...there is a feeling in industry that this [the security sector] is not quite the same as the defence sector, although many of the companies that operate are common to both sectors. But it is not like the defence sector in the sense that there is no single customer – a myriad of customers, public and private sector.<sup>68</sup>

Whilst this striking difference in market structure is widely recognised amongst UK security practitioners, a case can be made that the significance of this point has not been sufficiently taken into account by the scholarly community; no previous study has addressed it at length in the UK context. This is a major oversight because the simplistic narrative that has arisen - the notion that the MIC has simply transferred into the security sector - does not stand up to scrutiny. Whilst some industry figures argue that more coordinated procurement arrangements are needed across the breadth of the 'diverse' security sector<sup>69</sup>, the present landscape is beset with challenges. At the risk of repetition, the fact that many 'customers' in the security sector are private companies differentiates the security market from defence; whilst it could be argued that many smaller defence companies provide products and services directly to private sector 'prime contractors' like BAE Systems, the reality is that, in defence, the Government (in the form of the MoD) has a more direct relationship with the supply base than any non-military security department.

---

<sup>67</sup> Interview, Ogilvie-Smith

<sup>68</sup> Interview, John Howe

<sup>69</sup> The secretary of RISC, for example, has argued recently that that reform to policing procurement is needed to reduce the level of 'fragmentation' in the sector. Mark Phillips, 'The Challenge of Police Procurement – What is ADS doing about it', *ADS Blog*, 15 April 2014, Via: <http://blog.adsgroup.org.uk/challenge-police-procurement-ads/> (accessed 23.04.14)

Fundamentally, this arises largely because of the fact that, as one interviewee explained to the author, the MoD is ultimately the *sole funder* of defence and therefore a monopsony exists in the market.<sup>70</sup>

Analysis of efforts to improve effectiveness in non-military security-related procurement casts further light on these dynamics. That it would be desirable to increasingly purchase capabilities across the 43 policing constabularies of England and Wales, rather than individually, for example, has been identified by senior policymakers as one such area for improvement. The former Minister for Security, Lord West, has described his own experience of the practice arising whereby Police Chief Constables can deliberately seek to purchase different capabilities:

...I was at a dinner sitting with a chief constable each side of me. One of them was explaining what he was about to buy, and the other one did say; 'well there's no way I'm going to buy that then.' And I thought this was (...) a bit of a belter. And I'm sure there were very good reasons for it, but it just added to my feeling that actually we really do have to move forward in this area.<sup>71</sup>

It appears that the long-standing shortcomings of police procurement are finally being taken seriously, with serious Parliamentary discussion now taking place on how to improve the Government's approach. One identified successful reform relates to how Police Forces are now compelled to collaborate nationally around the procurement and utilization of air support such as helicopters; in written evidence to the PAC, the Home Office's Permanent Secretary explained how, by collaborating through the 'National Police Air Service' in the way that was now compulsory;

It is anticipated that it will save up to £15 million a year compared to the cost of previous arrangements when all forces have joined it.<sup>72</sup>

---

<sup>70</sup> Written correspondence, Ogilvie-Smith

<sup>71</sup> 'Part 3 of 3 - Admiral the Lord West of Spithead speaking at The BSIA Annual Lunch 2009', Via: 13 August 2009, Via: <http://www.youtube.com/watch?v=eHSPGuvlCBQ> (accessed 24.04.14)

<sup>72</sup> Committee of Public Accounts, 'Police Procurement', Twenty-first Report of Session 2013–14, 17 July 2013:

It would be difficult for even the most vehement critic of ‘the SIC’ to argue against the benefits to be had from the implementation of a national approach to police procurement when appropriate; especially where collaboration is so clearly financially beneficial, and where capabilities are so obviously needed. Other instances of non-military security procurement after 9/11 have yielded benefits from adopting a more centralized approach; as Chapter 3 indicated (pages 104-105), the delivery of the ‘New Dimension’ programme, for example, has been considered as exemplary in successfully acquiring new CBRN-related capabilities for the Fire Service nationally.

The key implication from a policy perspective, it appears, is not necessarily to centralize all aspects of ‘security procurement’ - such a task would be difficult to coordinate across all of the purchasers operating in the ‘market’.<sup>73</sup> Rather, the most sensible approach seems to be to identify potential areas of public security procurement that might benefit from a more coordinated approach at the national level, and where doing so would lead to quality and cost-effectiveness benefits.<sup>74</sup> Naturally, the development of more centralization in procurement might worry those concerned by the emergence of ‘the SIC’; a more streamlined procurement system might make it easier for companies to interface with the State in shaping requirements, for example. However, it may be the case that the landscape currently remains so fragmented as to mitigate against the likelihood of any such dynamic emerging.

Notwithstanding this last assertion, both the character and operation of the system for non-military security procurement has not received the scrutiny it deserves; in addition to the shortage of analysis on specific contracts, addressed above, it is noticeable how little scholarly attention has been given to analyzing the mechanisms that have been

---

Via: <http://webcache.googleusercontent.com/search?q=cache:http://www.publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/115/115.pdf> (accessed 23.04.14) Ev.17

<sup>73</sup> Rosemont, ‘Getting down to Business’

<sup>74</sup> A list of possible such areas is suggested in Phillips, ‘The Challenge of Police Procurement’

(or could be) established to improve the overall structures for non-military security acquisition. This is a general problem that was illustrated in the case of the recent establishment of a new Police ICT company; a body designed to manage the procurement of IT for all Police forces across England and Wales where appropriate. Whilst prior to its emergence the HASC had examined the possible scope and activity of the company, strikingly little serious analytical work has been done around the appropriateness of outsourcing to a private company the task of police procurement. Even where scrutiny of the proposal took place, it was incomplete; the HASC even observed in a report that ‘...[t]here is so little detail currently available about the police-led IT company that we find it difficult to reach a conclusion about its viability.’<sup>75</sup> This can be seen as a worrying statement; but perhaps it should be little surprise that the establishment of the Police ICT Company went ahead in 2012, despite such profound questions being raised.

The scholarly silence which greeted the new Police ICT company contrasts with the extensive analysis which surrounded the MoD’s proposal to outsource its defence acquisition arm, Defence Equipment and Support (DE&S); the proposition emerging was that a Government-Owned Contractor-Operated (GOCO) entity should be created. In this case, serious doubts were expressed in Parliament, in industry and in particular within the research community around the desirability of proceeding with the controversial scheme. The RUSI think tank, for example, published two briefing papers which questioned whether it would be sensible to outsource defence procurement along the lines suggested.<sup>76</sup> In the first of these, the RUSI Acquisition Group stated:

---

<sup>75</sup> Home Affairs Committee, ‘The New Landscape of Policing’, Fourteenth Report of Session 2010-12, 15 September 2011, Via: <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/939/939.pdf> (accessed 24.04.13), p.69

<sup>76</sup> Trevor Taylor and John Louth, ‘What the Government must do in Defence Procurement The Inherently Governmental Function and the GOCO Proposal for Defence Equipment and Support’, Briefing Paper, September 2013, Via: <https://www.rusi.org/downloads/assets/GOCO.pdf> (accessed 24.04.14); and RUSI Acquisition Focus Group, ‘The Defence Materiel Strategy and the

The GOCO proposal suffers from an inherent weakness, since it seemingly rests on an argument that, because the government is not very good at negotiating and managing contracts with the private sector, it is going to negotiate a contract with a private sector entity to undertake the task on its behalf.<sup>77</sup>

In other words, the report was damning of the logic underpinning the entire proposal. RUSI was not alone in its condemnation; a research note also acknowledges how the head of the industry trade association, ADS, believed that the Government needed to answer questions on the scheme.<sup>78</sup>

Several potential reasons can be offered for the differing levels of external interest in the Police ICT and GOCO initiatives. Firstly, as RUSI's Acquisition Group explored, the GOCO scheme was extremely broad in scope - covering not just ICT but *all* aspects of defence acquisition - and would therefore have been a more significant innovation. Secondly, the effect of the comparative level of resource allocated to 'defence' and 'security' should not be overlooked. A better understanding of this helps to explain why defence (not security) procurement continues to dominate the discussion; defence acquisition comprises in excess of £13bn annually, whereas total expenditure on police contracts has recently been measured as comprising £1.7bn<sup>79</sup> per year (of which, as an indication, £1.1bn was spent specifically on police ICT in 2010-11<sup>80</sup>). Perhaps it is little wonder why defence acquisition attracts more scrutiny.

This imbalance in analytical attention may not continue, as there is now a clear sense - both in Government and industry - that the non-military security procurement system is beset by difficulties; perhaps almost even unworkable. Chapters 3-5 illustrated

---

GOCO Proposal for Abbey Wood', Briefing Paper, July 2012, Via: [https://www.rusi.org/downloads/assets/GOCO\\_Briefing.pdf](https://www.rusi.org/downloads/assets/GOCO_Briefing.pdf) (accessed 24.04.14),

<sup>77</sup> Ibid. p.6

<sup>78</sup> Louisa Brooke-Holland, 'In brief: Outsourcing defence procurement', Standard Note SN06633, 10 May 2013, Via: <http://www.parliament.uk/briefing-papers/SN06633.pdf> (accessed 24.04.14), p.2

<sup>79</sup> Committee of Public Accounts, 'Police Procurement', p.3

<sup>80</sup> Home Office, 'Have you got what it takes? The Police ICT Company', Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/117420/police-ict-company.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/117420/police-ict-company.pdf) (accessed 24.04.14), p.2

the shortcomings at the micro-level; perceptions on the more general effectiveness of the procurement system revealed in interviews add weight to this argument. One industry executive speaking anonymously dryly commented:

...having worked with the Home Office on programmes, and having worked with the MoD on programmes, the MoD ought not to be too hard on themselves in terms of how they procure and manage programmes.<sup>81</sup>

The apparent lack of coordination in the security procurement system, in contrast with defence, might help to explain this. The problems that exist also clearly connect to the underlying character of the security market examined above. As Howe explains:

My feeling is, to be quite candid, that the parts of government with the biggest responsibility for security and counter-terrorism are actually quite remote from procurement activity.<sup>82</sup>

Of course, this is all in the context that the initiation of several major non-military CT programmes is only a relatively recent development.

As a general characteristic of the non-military security sector, therefore, it seems that central Government is more *detached* from the actual process of acquisition; with the exception of some major procurement projects, purchasing tends to be done by first responders, individual agencies or even private sector customers directly - not by departments like the Home Office. This is very different from the arrangements that exist in the defence sector, where the MoD has created within its remit (and devotes substantial resources to) the structures that are needed to pursue acquisition as a core aspect of the department's activity, however inefficiently. Should such an apparently undesirable state of affairs be accepted? The problem is clearly recognised at senior levels in Government and, in discussing policy options on how to deliver more effective security procurement,

---

<sup>81</sup> Interview, Industry Executive

<sup>82</sup> Interview, John Howe

Stephen Phipson stated soberly: ‘...that’s red on my list: I really have no clear idea on that one at the moment’.<sup>83</sup>

The absence of an official, centrally-coordinated structure to develop the policy aspects of the CT-related acquisition agenda, and across the national security sector more generally, would suggest that there would be little likelihood of economic considerations becoming a significant factor in the non-military security procurement decision-making process. This would certainly appear to be the case in the three major security contracts examined above; only with the G4S security contract was a proactive, positive case made around the prospect of employing local individuals in the security industry. Yet whether the establishment of the ‘Bridging the Gap’ initiative was a central factor in the contract award is not certain; the crucial consideration appears to have been that, rightly or wrongly, G4S was originally viewed as being ‘large enough’ to deliver the capacity that was needed. This is not to say that there were not repercussions for employment around the cancellation of any such contracts, however; the former CEO of EADS suggested that the UK Government’s decision to terminate the FiReControl project costed 500 jobs at EADS’ manufacturing and technology centre in Newport.<sup>84</sup> That said, the robustness of the Government decisions to cancel the e-Borders and FiReControl contracts can be seen as evidence that their employment aspects were not more important than other considerations.

Whilst economic considerations appear to have played a minimal role in the procurement aspects of CT, this is not to suggest that they do not continue to exist (or that they are not emerging) in the national security field more generally. The notion that ‘pork barrel’ politics exist in the UK is prominent in media coverage on UK defence policy; the connection between the New Labour Government’s decision to develop two new aircraft

---

<sup>83</sup> Interview, Stephen Phipson

<sup>84</sup> Interview, Robin Southwell

carriers and the location of the then Prime Minister's Parliamentary constituency has been noted, for example.<sup>85</sup> Economic considerations also feature in the UK Government's emerging strategy for cyber security; its first objective is to make 'the UK one of the most secure places in the world to do business'.<sup>86</sup> In parallel, the Government has recently developed an export strategy for UK-originated cyber technology.<sup>87</sup>

The evidence suggests that it is fair to conclude, perhaps with the exception of the growing attention that is being afforded to exports in the CT and wider security sectors<sup>88</sup>, the structures that have been established for (and the decisions made around) public-private cooperation around non-military CT-related procurement have not yet attracted the same level of policy and external analytical attention that has been seen in the defence sector. Whilst there are growing signs that this may not always be the case, the above analysis casts doubt over whether companies have been able to significantly influence, let alone 'capture' non-military security procurement. Should this issue develop as a policy priority, academia could have an important role to play in providing advice to the Government on how to improve the current arrangements for security acquisition; after all, as Chapter 2 noted, scholars have not held back in offering analysis and expertise on how to improve or reform UK military acquisition.<sup>89</sup>

### **7.3 Non-military, CT-related exports**

Whilst the CT-related procurement system has been shown to be disaggregated, there are some areas of non-military public-private security interaction where coordination has been

---

<sup>85</sup> David Robertson, Roland Watson and Angus Macleod, 'Revealed: truth about the aircraft carrier deal', *The Times*, 22 Oct. 2010, Via: <http://www.pressawards.org.uk/userfiles/files/entries-01287-01284.pdf> (accessed 10.12.14)

<sup>86</sup> Cabinet Office, 'The UK Cyber Security Strategy', p.36

<sup>87</sup> UKTI, 'Cyber Security: The UK's approach to exports', April 2013, URN 13/720, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/275566/UKTI\\_Cyber\\_Security\\_Brochure.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf) (accessed 30.04.14)

<sup>88</sup> Section 7.3 analyses non-military security exports.

<sup>89</sup> See references listed in footnote 74 (Chapter 2)



strengthened; the joint emphasis placed on promoting UK non-military security exports is a case in point. This aspect of cooperation is important to consider because, as noted in Chapter 2, the topic of 'exports' has often emerged as a core theme of MIC-related scholarly literature and wider public discussion. As well as addressing *why* the UK Government supports industry with defence trade promotion - in essence, for both economic and security/political reasons<sup>90</sup> - the literature debates the supposed benefits of pursuing such a strategy<sup>91</sup>, with wider discussions covering both the effectiveness and appropriateness of military-industrial relations around this priority. Whatever the benefits of pursuing an arms export policy, it has undoubtedly become a core element of UK defence-industrial interaction and associated strategy; as Smith and Smith recognise, '[i]n those states for which manufacturing industry is a part of security policy, arms exports have also become a part of the policy.'<sup>92</sup> It follows that, in considering the character of the private sector's involvement in CT, it helps to pursue an inquiry into any equivalent non-military export structures and/or activities. This section considers how and why there has been an increasing emphasis on joint working to promote UK security capabilities, and analyses the character of public-private engagement in this area.

The most significant machinery of Government change relating to arms export policy after 9/11 - the replacement of DESO with the establishment of DSO within UKTI in 2008 - also had the effect of re-orientating the Government's emphasis on the pursuit of military exports in the national security field. The organization's website at the time explains how responsibility for policy on defence exports moved from the MoD:

UKTI DSO was formed on 1st April 2008, when responsibility for defence trade promotion transferred from the Ministry of Defence to UKTI. The

---

<sup>90</sup> As explained in Chalmers et. al., 'The Economic Costs and Benefits of UK Exports' and Smith, *Military Economics*

<sup>91</sup> For a critical analysis, see Martin 'The subsidy savings'. Smith identifies that there is a 'dispute about the costs and benefits of arms exports to the economy.' Smith, *Military Economics*, p.146

<sup>92</sup> Smith and Smith, *The Economics of Militarism*, p.79

new group brings together trade development support across the defence and civil sectors under the umbrella of UKTI.<sup>93</sup>

This decision now seems straightforward, but it proved to be controversial at the time.

According to the Prime Minister's 2007 statement, the decision was taken because:

The Government believe trade promotion for defence exports should be more effectively integrated with the Government's general trade support activities, while recognising and accommodating the specific requirements of the defence sector.<sup>94</sup>

The UK Government's intention to align defence exports with its work on promoting other sectors of the economy is certainly a logical one; a persuasive case can always be made in Whitehall that increased coordination can yield considerable benefits such as avoiding the potential for duplication. Other reasons may have existed, however, and one not implausible account suggests that the decision was in fact driven by the Treasury; which was reported only too happy to cut costs by reducing the subsidy received by the defence industry from what was considered an 'anachronistic' department.<sup>95</sup> Certainly, critics of the industry (and the support it received through DESO) argued at the time that the level of subsidy was intolerable. One Think Tank supported the closure of DESO;

...because it was part of an unwarranted subsidy of profitable defence companies; resulted in arms exports that undermined human rights; and because of wider concerns about the impact of subsidised arms sales on Britain's international reputation and security.<sup>96</sup>

The decision to relocate responsibility for promoting defence-related exports away from the MoD was also criticized by some leading industry figures. The CEO of BAE Systems, for

---

<sup>93</sup> 'About the UKTI Defence & Security Organisation', 2 December 2009, Via: <http://webarchive.nationalarchives.gov.uk/20100222170314/http://dso.uktradeinvest.gov.uk/about.htm> (accessed 30.04.14)

<sup>94</sup> 'Machinery of Government: Defence Trade Promotion', Written Ministerial Statement, 25 July 2007, Via: <http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070725/wmstext/70725m0005.htm#07072565000047> (accessed 30.04.14)

<sup>95</sup> Rob Evans and David Leigh, 'Treasury plans to shut arms sales department', *The Guardian*, 9 July 2007, Via: <http://www.theguardian.com/uk/2007/jul/09/armstrade.economy> (accessed 30.04.14)

<sup>96</sup> British American Security Information Council, 'Four major UK security announcements on eve of parliamentary recess', July 30 2007, Via: <http://www.basicint.org/press/releases/2010/four-major-uk-security-announcements-eve-parliamentary-recess> (accessed 30.04.14)

example, wrote to the Prime Minister to express his ‘considerable concern’ about the proposal, lamenting the lack of consultation that had taken place with industry on it. He argued damningly: ‘I can think of no benefit that “synergy” with UK T&I can offer that will begin to outweigh the lost excellence of the DESO operation.’<sup>97</sup> Industry was not successful in reversing the decision, however; DSO was formed in April 2008.

Some of industry’s worst fears appear to have been realized as the number of Government personnel dedicated to promoting defence exports reduced significantly after the transfer; DESO was staffed by 450 people upon its closure and around 150 personnel are now employed at UKTI DSO.<sup>98</sup> By contrast, as UKTI DSO developed, the ‘synergy’ that could be achieved by developing the UK’s approach to security exports alongside defence was significant; at least certainly for those security companies who would not have previously had access to focused Government attention in supporting their export objectives. Indeed, such was the emphasis on promoting security as well as defence exports that the Head of UKTI DSO publicly referred to his organization’s focus on ‘security’ being ‘the middle name of DSO.’<sup>99</sup>

New structures were created which would aim to help develop the DSO’s new emphasis and strategy on security exports. Most significantly, an industry-chaired UKTI ‘Security Sector Advisory Group’ (SSAG) was established and initially chaired by Stephen Phipson (then President of Smiths Detection). According to the ‘Open to Export’ website:

---

<sup>97</sup> Letter from Mike Turner (CEO of BAE Systems) to the Prime Minister titled ‘Support for Exports’, 26<sup>th</sup> July 2007, Via: [http://www.defenseindustrydaily.com/files/DESO\\_Letter\\_BAE\\_2007-07-26.pdf](http://www.defenseindustrydaily.com/files/DESO_Letter_BAE_2007-07-26.pdf) (accessed 30.04.14)

<sup>98</sup> Critics might contest the usefulness of this comparison. One 2008 briefing note by CAAT argued that the numbers of staff were simply becoming more diffused; ‘Around 240 of DESO’s 450 staff were transferred to UKTI, with the remainder, predominately those managing the Saudi arms deals, staying within the MoD.’ However, the same briefing document also recognises explicitly that the decision signalled ‘The down-grading of the arms trading operation’. CAAT, ‘Arms trading at UKTI’, November 2008, Via: <http://www.caat.org.uk/resources/publications/government/ukti-briefing.pdf> (accessed 30.04.14)

<sup>99</sup> Ramananda Sengupta, ‘Interview: UK-India defence ties’, *sify.com*, 11 February 2009, Via: <http://www.sify.com/news/interview-uk-india-defence-ties-news-columns-jegsUJhhaib.html> (accessed 30.04.14)

The Sector Advisory Group is led by a senior businessperson with extensive corporate and commercial experience who (sic) purpose is to work closely with the Security Directorate within the UKTI to advise and assist on the development of effective strategies to boost UK and international growth.<sup>100</sup>

This body is an example of systemic, strategic interaction between Government and the security industry on non-military, CT-related export issues - in this case (unlike RISC) it was even a Government-hosted entity. The 'closeness' of the relationship between Government and the security industry on this issue is further exemplified by the fact that the SSAG is now chaired by another former Chairman of RISC, Michael Clayforth-Carr. Furthermore, the forum includes industry members from technology companies such as BAE Systems/Detica and EADS as well as service providers like Control Risks and the Olive Group<sup>101</sup>; at least on exports, this shows that the Government has adopted a broad conceptualization of how it looks upon the 'security sector'. Interestingly, the SSAG, which meets approximately 'quarterly', is also attended by at least one prominent academic; the Director-General of RUSI, for example, is a member.<sup>102</sup> This shows how on the issue of UK security exports a system of formal public-private interaction has emerged whose representation extends beyond government and industry; this characteristic resonates strongly with existing MIC theories which portray the system as encompassing broader involvement.

Other new structures emerged to support this priority; a dedicated 'security directorate' was even formed inside the new DSO. A UKTI brochure indicated the purpose of this department:

---

<sup>100</sup> 'Security Sector Advisory Group (SSAG)', *Opentoexport.com*, 4<sup>th</sup> April 2012, Via: <http://opentoexport.com/article/security-sector-advisory-group-ssag/> (accessed 01.05.14)

<sup>101</sup> Ibid.

<sup>102</sup> Ibid.

The UKTI DSO Security Directorate provides advice to homeland security, fire, police and commercial security sector companies to optimise government support for the UK's unique and leading-edge UK industry.<sup>103</sup>

In support of its objectives, the UKTI has also supported - both financially as well as through the provision of staff assistance - a number of high profile security trade events and exhibitions to promote UK capabilities. As part of its programme, DSO's involvement in the Home Office's annual Security and Policing Exhibition is perhaps the most notable; whilst the support it brings to industry in issuing invitations to overseas delegations is welcomed in the sector, organizations including CAAT have campaigned against what it sees as unwarranted support for 'some of the world's most repressive regimes'.<sup>104</sup>

The picture that emerges, therefore, is of Government and industry increasingly working together on CT-related exports since the establishment of UKTI DSO in 2008. Whilst DSO's emphasis has continued to be directed mainly towards supporting the defence sector – even a cursory review of the DSO's latest 'contact directory' indicates that it has only appointed a minimal number of security sector-specific employees when compared to the defence sector<sup>105</sup> - 'security' now appears as a core aspect of its activity. Whilst some industry interviewees believed that UKTI DSO could operate more effectively on security issues, all those questioned during this research recognised the role it had been playing in supporting the industry in overseas security markets.

---

<sup>103</sup> UKTI DSO, 'UK Trade & Investment Defence & Security Organisation: Helping UK companies to export', April 2009, Via: [http://webarchive.nationalarchives.gov.uk/20100222170314/http://dso.uktradeinvest.gov.uk/docs/UKTI\\_DSO\\_Brochure\\_Apr\\_09.pdf](http://webarchive.nationalarchives.gov.uk/20100222170314/http://dso.uktradeinvest.gov.uk/docs/UKTI_DSO_Brochure_Apr_09.pdf) (accessed 02.05.14), p.7

<sup>104</sup> 'Delegations', CAAT Website, Via: <http://www.caat.org.uk/issues/arms-fairs/security-and-policing/delegations/> (accessed 01.05.14). CAAT states that countries including Bahrain, Kuwait and Saudi Arabia were invited to the 2013 Security and Policing Exhibition event.

<sup>105</sup> Four bespoke non-military security sector specialists were identified: a Senior Security Adviser, a Police and Security Advisor, a Cyber Security Advisor and an International Cyber Security Director. By contrast, the directory lists nine 'Overseas Defence Specialists' alongside a wide range of other regional and bespoke defence sector positions including a Senior Army Advisor and a Senior Military Advisor. UKTI DSO, 'Contact Directory 2014', July 2014, Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/328090/UKTI\\_DS\\_O\\_Contacts\\_Directory\\_July\\_2014.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/328090/UKTI_DS_O_Contacts_Directory_July_2014.pdf) (accessed 30.12.14)

Furthermore, there is increasing evidence that 'security exports' is becoming more prominent as a policy priority not just for UKTI DSO, but also for other Government departments. One official indicated in a confidential interview that the centrally-organised Ministerial Working Group on national security-related exports '...has security sales as well as defence sales within its remit' and insisted that a 'Sales Review' conducted by Cabinet Office shortly prior to the interview included security exports.<sup>106</sup> The 2012 NSST White Paper also placed a significant emphasis on the steps the Government (in the form of the Home Office) planned to take to promote CT-related as well as defence exports; it announced, for example, an intention to potentially develop a 'UK Security Brand' as one 'mechanism for supporting security exports in a fragmented market'<sup>107</sup>. Most significantly, the appointment of the Director of Security Industry Engagement in June 2013 - referred to above and a position which arose as a direct consequence of a commitment made in NSST<sup>108</sup> - generated a formal role for the Home Office on exports. The central importance of the export dimension to this new senior Home Office position was clarified in its original job description; it included under a list covering the 'key responsibilities' of the role the requirement to coordinate 'between the UK counter-terrorism strategy, CONTEST, the security industry and security export opportunities'.<sup>109</sup>

True to the originally-envisioned role, Stephen Phipson has been vociferous in promoting UK security exports since his appointment. In a magazine interview focusing on how the UK's experience in hosting the London 2012 Olympics might boost UK security exports, for example, he explained how he looked upon his and his team's responsibilities: 'Within the Home Office I lead a dedicated team focused on supporting and promoting the

---

<sup>106</sup> Interview, Government Official

<sup>107</sup> MoD, *National Security Through Technology*, p.55

<sup>108</sup> NSST stated for the first time publicly that the Government was '...evaluating the potential benefits of appointing a Senior Responsible Owner (SRO) within Government to head up a security authority and the merits of developing a UK Security Brand.' *Ibid.*, p.1

<sup>109</sup> Home Office, 'Director - Security Industry Engagement', Job Description (2012), p.6, cited in Rosemont, 'Private Sector Engagement'

UK security industry, and increasing the UK's share of the security export market[.]'<sup>110</sup> The idea that the Home Office would become so directly involved in the security export agenda would have seemed a very alien concept only a few years ago. The agenda appears to be developing rapidly and Mr. Phipson is clear that the relationship is not only developing at the official level. He is reported as stating to one industry association meeting:

There's a lot more senior ministerial interest in the security industry. The defence sector is under pressure, the demands are going down, it is a difficult environment globally; the security sector is a growth market.<sup>111</sup>

Whether greater Ministerial attention towards promoting security exports is desirable may split opinion, but there is no doubt of the significance of this new trend; efforts are being made by the Home Office to replicate in the security sector the attention that companies have previously 'enjoyed' from the MoD in many areas including defence trade promotion.<sup>112</sup>

This move towards such a strong new emphasis on security exports is especially important because it inevitably presents similar (if not the same) ethical dilemmas traditionally associated with international military sales. One Government official referred to an (almost literally) explosive example to illustrate how this ethical dimension applies equally to 'security':

We've had requests for police helicopters to be armed. Do you want to be the government that's doing that work with that foreign government? And so the ethical question is actually raising a lot of red flags; a lot of questions to be considered extremely carefully.<sup>113</sup>

It is perhaps reassuring that the public official in question was minded to consider the appropriateness of exporting armed 'non-military' security capabilities, but there is little

---

<sup>110</sup> Robert De la Poer, 'Securing the Olympic legacy', *Intersec*, 17 November 2013, Via: <http://www.intersecmag.co.uk/olympics-nov13/> (accessed 01.05.14)

<sup>111</sup> 'More markets at the double', *Professional Security Magazine*, Vol.24.4, April 2014, Via: <http://www.professionalsecurity.co.uk/online-magazine/20-03-14/april/#p=46> (accessed 01.05.14), p.47

<sup>112</sup> Rosemont, 'Private Sector engagement'

<sup>113</sup> Interview, Government official

evidence of external analytical attention being directed towards the potential implications of this increasing policy emphasis. Asked why the ethics of exporting security capabilities had not generated the same level of attention and analysis as has been seen in the defence sector, the same official replied; 'that's because we haven't done big G2G [Government to Government] arrangements before, and we're about to.'<sup>114</sup> Whilst the pursuit of this policy may be beneficial to the UK for both security and economic reasons, it should be recognised that other risks could emerge that have more unforeseen and longstanding consequences. In addition to the obvious risks for human rights that could be presented by the policy - either directly or indirectly, despite protestations to the contrary - one interviewee noted (on the condition of anonymity) the irony of the fact that, as the Government aimed to export UK security capabilities, it did not appear to be procuring the same capabilities domestically. The interviewee's sobering observation raises serious questions about the effectiveness and desirability of the current approach:

And actually, by pushing it this route, and not addressing our home market, I think strategically there is a risk that we're going to enable overseas countries to have better capability and be much better placed to operate in the 21<sup>st</sup> Century than we are ourselves.<sup>115</sup>

This thesis has found little evidence to suggest that the UK Government has yet considered such potentially deeper implications of its strong current focus on exporting UK security capabilities; and in particular whether developing this in such a disconnected way from the UK's own domestic security procurement programme is desirable.

It is nevertheless easy to agree with Stephen Phipson's assertion that, if the Government is successful in signing and developing G2G's in the security arena, '...it's going to change the way the interaction works with industry.'<sup>116</sup> Indeed, such is the Home Office's increasing involvement in security exports that one DSO official explained how the

---

<sup>114</sup> Ibid.

<sup>115</sup> Interview, Industry Executive

<sup>116</sup> Interview, Stephen Phipson



department was the UKTI's 'main partner nowadays when supporting UK security companies looking to export'.<sup>117</sup> Not all those observing developments in this area would agree that the approach being pursued is an optimal one. The editor of one UK security trade publication has been critical of the lack of detail around the department's proposal to develop a 'security brand' for promoting exports and, following an explanation of the proposal by the Home Office, he argued that it raised '[t]oo many question marks by far.'<sup>118</sup> Separately, the secretary of RISC explained that his 'big bug bear' was in trying to persuade the Home Office: 'don't forget that there is a domestic agenda that needs to be done.'<sup>119</sup>

Whilst frustrations exist around what has been seen as the overly export-orientated direction being pursued by the Home Office's SIET, its decision to publish a security export strategy document in early 2014 - a document penned jointly with UKTI DSO<sup>120</sup> - was a significant development that was warmly welcomed by the sector's representative trade associations.<sup>121</sup> Whilst 'Increasing our Security Exports' was not the first public UKTI document on security exports, it is clearly the most strategic in orientation and transparent in detail. As well as listing specific target markets (such as Saudi Arabia and Kuwait) and high value opportunities (such as the Qatar 2020 World Cup) pertaining to the security industry, it outlines seven 'capability areas' of UK expertise that it will aim to

---

<sup>117</sup> Interview, Simon Everest

<sup>118</sup> Mark Rowe, 'Editor's Comment', *Professional Security Magazine*, Vol.24:5, May 2014, Via: <http://www.professionalsecurity.co.uk/online-magazine/28-04-14/24-5/#p=6> (accessed 01.05.14), p.7

<sup>119</sup> Interview, Mark Phillips

<sup>120</sup> UK Trade & Investment, 'Increasing our Security Exports: A new government approach', February 2014, Via: <https://www.gov.uk/government/publications/increasing-our-security-exports-a-new-government-approach> (accessed 02.05.14)

<sup>121</sup> For example, the ADS Group described the launch date of the strategy as 'a significant day for the security sector'. Mark Phillips, 'The UK's first security export strategy', *ADS Blog*, 27 February 2014, Via: <http://blog.adsgroup.org.uk/uks-first-security-exports-strategy/> (accessed 02.05.14). Another RISC trade association, techUK, has also commented on the new strategy, stating that it was 'delighted to attend the launch and support its creation.' techUK, 'Increasing our Security Exports - New Strategy Launched Today!', Via: <http://www.techuk.org/insights/news/item/1080-increasing-our-security-exports-new-strategy-launched-today> (accessed 02.05.14)

promote through the development of 'specific export plans'.<sup>122</sup> Furthermore, additional information is provided, for the first time in public, on how the Government would see G2G agreements potentially working in the security sector:

Through a G2G agreement we would offer, where appropriate: access to security expertise and strategic thinking within government, police and agencies; support to overseas governments to identify and specify their security requirements; and assistance in accessing the necessary capabilities from the UK security industry.<sup>123</sup>

This is a clear signal that the UK Government is comfortable with security exporting, and that it aims to act as a broker with its allies in respect of promoting the capabilities of the UK security industry overseas. As the Ministerial Foreword to the document makes clear, Government and industry need to 'work hand in hand to achieve our objective to increase UK security exports.'<sup>124</sup>

Whilst Government and industry may need to work 'hand in hand' to realize this aim, it is useful to consider the influence that companies may have exerted on the formation of the UK's security export strategy - any suggestion that they did might resonate with 'SIC-as-conspiracy' arguments. Whilst the trade associations underpinning RISC have clearly seen a role for themselves in the development of this Government strategy - ADS has stated that it aims to 'set up and oversee the operation of a UK Security Brand'<sup>125</sup> proposed within the document, for example - the actual usefulness of industry input into the strategy appears mixed. Explaining that Government and industry 'engage better than we once did' on security exports, the official offered the following observation about the process:

---

<sup>122</sup> The seven capability areas are: CNI Protection; Cyber Security; Border Security; Policing and Counter Terrorism; Major Event Security; Offender Management; Services – including consultancy and training. UKTI, 'Increasing our Security Exports', p.20

<sup>123</sup> UKTI, 'Increasing our Security Exports', p.11

<sup>124</sup> UKTI, 'Increasing our Security Exports', p.1

<sup>125</sup> 'Security Policy', ADS Group Website, Via: <https://www.adsgroup.org.uk/pages/58346194.asp> (accessed 02.15.14)

...in terms of consultations with industry, we had some good discussions. Have I always received a huge amount of feedback on our approach or suggestions of how it could be improved? Not sure that I have particularly. In the early days we were pretty much driven by what we were going to do and thought we should do, but nowadays we bounce ideas off industry and the trade associations and have a completely joined up dialogue.<sup>126</sup>

This reveals the sometimes indifferent attitude that Government officials can adopt towards industry's contributions on policy matters, perhaps reflecting the perception in and around Whitehall that 'Government always knows best'. The more important point here, however, in the context of assessing the level of private sector (or 'SIC') influence that may exist, is that ideas are 'bounced off' industry; not the other way around. Whilst there is clearly a degree of 'cosiness' in the emerging government-industry relationship around security exports - the dialogue is 'joined-up' and the same interviewee explained that he can 'pick up the phone and talk to anyone'<sup>127</sup> in industry on this topic - the actual influence that the private sector has asserted on the Government's policy orientation appears marginal; even if the Chairman of RISC insisted at the launch of the document that industry 'will have a key role in developing performance measures and overseeing the delivery of the strategy'<sup>128</sup>. Whilst it is now apparent that Government and industry see 'security exports' as a shared priority, it is not clear that undue influence has been exerted on the development of the strategy. Whilst some will argue that Government should not be working on this issue, Government does appear to 'hold the pen' on its own security export policy.

The UK's security export strategy makes several important references to the way in which the MOD is itself involved in the oversight and implementation of the Government's policy. Most notably, the paper explains how a Ministerial Working Group on Defence and Security Exports chaired by the Defence Secretary will '[p]rovide ministerial leadership to

---

<sup>126</sup> Interview, Simon Everest

<sup>127</sup> Ibid.

<sup>128</sup> Tim Crofts, 'RISC Chairman's Speech', Launch of the UK's Security Exports Strategy, 27 February 2014, Via: [https://www.adsgroup.org.uk/pages/42220705.asp#aGroup\\_1](https://www.adsgroup.org.uk/pages/42220705.asp#aGroup_1) (accessed 02.05.14), p.11

the development of UK Defence and Security export strategy<sup>129</sup> and that it will seek to exploit 'synergies between military and security sectors where appropriate'<sup>130</sup>. That the security export strategy would appear to be subsumed into the remit of 'Defence' through this governance structure suggests that 'Security' might be considered in Government as the lesser partner in the arena of exports. Whether or not this perception is grounded in reality, it would be difficult to argue that a classically-configured, equivalent 'SIC' has emerged in the field of exports when, in reality, the structures which guide and oversee them remain so closely wedded to the defence sector.

An additional important difference in how public-private interaction on export matters operates across defence and security is that many more Government stakeholders are involved in the promotion of non-military, CT-related exports. The strategy document includes a table which lists no less than 15 different individual government departments or agencies - including, perhaps controversially, the signals intelligence agency GCHQ<sup>131</sup> - that are considered to be involved.<sup>132</sup> The public-private dynamics around security exports, like the operation of the security market more generally, are therefore much more diverse than is, and has long been the case, in the defence sector; in this latter instance the UKTI DSO now leads, with the MoD viewed as the 'sole customer'. It is this significant difference which again raises serious doubt as to whether the MIC-translation theory can so easily be applied to exports, let alone accepted more generally.

---

<sup>129</sup> It is striking that the Government would refer to a single strategy across defence and security, when the document within which this statement appears is solely concerned with the Government's approach to security exports. 'Increasing our Security Exports', p.18

<sup>130</sup> Ibid.

<sup>131</sup> It has also been suggested that the Intelligence Agencies have played a role in promoting defence exports. Robert Dover, 'For Queen and Company: The Role of Intelligence in the UK's Arms Trade', *Political Studies*, Vol.55 (2007), pp.683-708. The point here, however, is to note the even wider number of Government departments/agencies involved in security exports.

<sup>132</sup> UKTI, 'Increasing our Security Exports', pp. 18-19. Strangely, the table also incorrectly lists 'trade associations' - all of which are private companies - within its list of 'government departments'.

Finally, the document's section on 'Export Controls' recognises that whilst it is important that 'the UK should not export capabilities where there is a clear risk that they will be used to violate human rights or for internal repression'<sup>133</sup>, a significant difference exists in how the official mechanisms of oversight operate across defence and security exporting; the document recognises that '...[t]raditional export controls do not always readily apply to security systems.'<sup>134</sup> Informal conversations with industry figures have revealed a pervasive view that, in some areas of security policy, the export security system has simply not reached the level of maturity as exists in defence. This characteristic is another indication that, on the basis of practices in the CT field, non-military public-private security engagement operates differently. Such evidence provides additional support to the contention that the use of the SIC concept to describe government-industry relations in the non-military security export context is an over-simplification; unique characteristics of interaction have emerged and evolved, and should be recognised as such.

#### **7.4 Character and impact of the 'industrial-complex' in three additional areas of concern**

This chapter has illustrated how the system of public-private cooperation in the UK CT sector after 9/11 replicates some, but not all, of the features traditionally associated with defence. In terms of similarities, the 'revolving door' has been shown for the first time to be much in evidence in the non-military, CT-related security aspects of UK national security strategy; whilst the movement in employment terms of public officials taking positions in industry (and vice versa) does not necessarily confirm the existence of, or inclination towards, any 'unwarranted influence' being exerted by such a system, it is striking how a number of the most senior individuals operating in the sector have followed career paths which have transgressed both public and private sectors.

---

<sup>133</sup> UKTI, 'Increasing our Security Exports', p.17

<sup>134</sup> Ibid.

The UK Government has, since the formation of UKTI DSO in 2008, exhibited a very significant new emphasis on promoting UK CT-related security exports for both security and economic reasons. Interestingly, the Home Office is now seeking to operate in the wider security sector in the same way that the MoD has traditionally played a role in supporting UK defence exports; that of seeking to facilitate G2G contracts with overseas partners, creating (ultimately commercial) opportunities for industry to help to deliver the capability. As with the experience in the defence sector, the Government's new approach presents a controversial set of issues; the suggestion that the intelligence agencies are involved in promoting exports, or that the UK Government aims to provide security capability to controversial regimes such as Kuwait or Saudi Arabia, for example, will not be supported by everyone.

Nonetheless, the chapter also showed that the structure of the procurement 'system' in the CT and security sector more broadly is more 'fragmented' than is the case in defence; this reflects how the security market has often been observed generally.<sup>135</sup> It comprises a considerably wider range of public and private sector customers, and some of the State's purchasing arms (such as for police IT) have already even been privatized. The evidence suggests, resonating with the findings of previous chapters, that whilst defence acquisition is not immune from its own challenges and difficulties, the system of acquisition that exists in the non-military, CT-related security arena is riddled with inefficiency and a lack of expertise, leaving considerable room for improvement. Economic considerations relating directly to the public procurement system in the CT and wider security field did not appear as a significant factor in the appointment (or indeed the cancellation) of the three main contracts examined for this thesis, perhaps owing to the smaller amount of resources that are available in the sector.

---

<sup>135</sup> Interview, Stephen Phipson; "Project Gain", p.1

## 8. Conclusion

This thesis has sought to reassess the origins, characteristics and the consequences of the private sector's involvement in the non-military CT aspects of contemporary UK national security strategy after 9/11. The resulting dissertation is intended to contribute an innovative assessment - supported by new micro-level analysis of hitherto under researched UK security contracts and other public-private interactions in CONTEST - of the character of private sector involvement in the security sector, and the extent to which any or all of the dynamics that have historically been associated with the MIC are present within this sector. Whilst the thesis recognised that hypothesizing over the *existence* of an 'industrial-complex' presents methodological challenges, and poses some possible limitations, it is designed to explore whether the use of such terminology in the wider security context is actually appropriate.

The thesis examined the character of the 'industrial-complex' in the UK's CT sector between 2002 and 2014 by addressing the following main research question:

- What are the origins, characteristics and consequences of the private sector's involvement in the (non-military) CT aspects of UK national security strategy?

Three additional supporting questions were addressed to inform the analysis:

- Is the character of 'industry engagement' in the UK's CT sector comparable with 'defence'?
- Has any industrial-complex in the UK's CT sector exerted any 'unwarranted influence'?; and
- What are the consequences of any such system for researchers and practitioners?

Having addressed these questions throughout this dissertation, the remainder of this chapter presents the conclusions of the thesis.

### 8.1 Origins

The dissertation's combination of theoretical and empirical analysis means that the origins of the private sector's involvement in CONTEST can be presented in new light. In short, the

significant variety and new types of public-private cooperation that emerged after 9/11 (and especially after 7/7) represent nothing short of a major revolution in the way that the Government interacts with non-state actors to implement its security objectives. As the risk of terrorism evolved, and has come to be perceived (at least by some in Government) to pose a significantly greater threat to the UK and its interests than prior to 9/11, so major new security programmes such as New Dimension and e-Borders have been developed by Government departments other than the MoD as a major component of the response. That the considerable additional investment that followed would attract the interest of commercial suppliers is perhaps hardly surprising. The ferocity with which many commentators criticized both the Government's perception of the threat and the increasing level of corporate involvement in CT has nevertheless been notable.

The extensive involvement of private companies in the non-military CT aspects of UK national security is not only explained by the greater number of commercial opportunities to have arisen in the sector. Other factors have contributed and include, for example, the public policy programme of privatization that was developed during the 1980s and 1990s, which continue to this day. Whilst it does not appear to have been anticipated by policymakers at the time, this resulted in a situation in which the Government became (and continues to be) more dependent on 'private operators' of infrastructure to deliver contemporary national security because it is now companies, not government, that own these installations. Furthermore, initiatives such the CSSC Olympic security project have shown how parts of the private sector became more assertive and more organised after 9/11 in seeking to strengthen their own security. Such industry-led initiatives may form the basis of future collaboration and appear to defy the logic of one of the main arguments associated with MIC theory - that companies are *only* involved in security to generate greater profits.



Furthermore, it is the thesis's contention that the private sector's extensive involvement in the non-military aspects of national security strategy can actually be seen as reflecting the Government's changing conceptualization of 'national security' in the contemporary threat environment. The opening chapters examined, with the private sector's involvement in mind, the evolution of the UK Government's definition of 'security' in more detail, highlighting how it now pays greater emphasis on addressing non-military security risks such as terrorism and cyber insecurity. More than any other single factor, this significant shift in understanding (and thus associated change in policy emphasis) has resulted in the emergence of new non-military security strategies (and associated programmes) which have drawn on the involvement of private companies to an unprecedented extent. Partly because the Government depends on private actors within these 'new' arenas such as CT, and partly because commercial companies have themselves sought to play an active supporting role, the result has been a significant level of private sector involvement in the security sector. It is the contention of this thesis that the combination of the various public-private interactions (however fragmented) amounts to what should be properly viewed as an extensive *set of systems*, and as such represents, an original contribution to the field.

It is arguably appropriate in the closing stages to briefly recall how this thesis's inquiry into the origins of the private sector's involvement in UK national security strategy might connect to (or be explained by) other existing literature which relates to the privatisation of security. Amongst the many existing offerings in this space (examined in Chapter 1, Section 1.3) is Professor Philip Bobbitt's theory on the emergence of what he has called the 'market state'. Bobbitt's central argument is supported by the findings of this dissertation; the thesis has shown with reference to the UK CT sector that a high level of interaction (if not interdependency in some areas) has emerged between the Government and the private sector in the delivery of the UK Government's most

sensitive and fundamental duty: security. Bobbitt has had his critics but, absent any substantial refutation of the 'market state' theory, his thesis has profound implications in the sense that it advances the idea that, in the contemporary environment, it is not only desirable but now *necessary* for Governments to interact with companies on security issues such as CT.

Seen from this perspective, the extensive level of private sector involvement evident in CONTEST thus potentially reflects a fundamental change in the underpinnings of the contemporary State structure; in short, any transition towards the coalescing of the market and the State might make it inevitable (and more understandable) that the Government would seek to work with the private sector on security issues. This radical idea should provoke deep reflection; that this thesis's theoretical and empirical analysis can connect to it in a UK context is identified in the hope that it might encourage future debate.

## **8.2 Characteristics**

The thesis has illustrated an extensive and often dysfunctional system of public-private interaction in the CT elements of contemporary UK national security strategy. In its analysis, several characteristics that have traditionally been associated with the MIC have been shown to be present in the non-military arena; especially in respect of commercial security suppliers' involvement in this area. Most notably, several large-scale CT-related security programmes were established or funded by the UK Government after 9/11 to counter the terrorism threat; these closely resembled the type of large, fully-integrated programmes that have become associated with the defence sector. Like in the military arena, commercial suppliers became centrally involved in 'delivering' what in many cases became problematic contracts with deep-seated and high profile difficulties - often leading to substantial waste of taxpayers' money; the cases examined in this thesis rightly received

sharp criticism as a result. The boundaries between the public and private sectors in the management of these contracts often appeared unclear or blurred - the public-private dynamics in the case of London 2012 were particularly 'circular' - and acquisition in the security sector was shown to be no less afflicted with the difficulties that have arisen previously in the defence sector.

Evidence has been provided of (and criticism has been levelled against) the UK Government's approach to working with industry on other controversial issues relating to CT. In particular, concerns have been raised over the emergence in the CT sector of the 'revolving door' (most commonly associated with the MIC) and, secondly, the significant emphasis being placed on developing a strategy to work with the security industry to promote UK security exports (i.e. alongside its traditional focus on seeking overseas defence business). The thesis concludes that some of the rotational dynamics that are popularly associated with the MIC are now present in the UK's non-military CT sector.

The extent to which evidence has been found that such dynamics have been genuinely detrimental, in line with most theories on the MIC (and any modern-day variety), is debatable, however. Whilst in the cases of all three major procurement projects examined in the preceding chapters - FiReControl, e-Borders and the G4S Olympic Security contract - there was some evidence of an arguably unhelpful role being played by some private sector entities (in particular several consultancies), no evidence has been found of any deliberate effort at threat inflation, or corruption, on the part of the involved companies, and/or any coalition of public-private interests comprising what has been labelled 'the SIC'. Far from a serious picture emerging of a 'sinister' coalition of public and private sector actors or entities working closely together to 'over-hype' threats, and thereby encourage higher levels of spending on security contracts, this thesis's analysis of three of the largest UK security contracts instead presented a picture of chaotic,

disorganised and highly inefficient public-private interaction. In the end, all three contracts under examination 'failed' in the sense that they were not fully implemented; both the Government and the companies associated with them have suffered reputational damage as a result. The impact that was inflicted does not reflect the picture of 'the SIC' frequently presented by critics of public-private security interaction.

Having illustrated the emergence of wide range of differing public-private dynamics in three specific CT sub-sectors, Chapter 6 identified the establishment of a close *strategic* relationship between the security suppliers' community and the Home Office through 'RISC'. In analyzing the origins of the alliance, new data drawn from interviews and archival documentation provided some evidence of the underpinning financial motivations of those who were involved in establishing the entity; the creation of this new body, and the widespread support it received in Government and industry, might be seen as confirming the worst suspicions of SIC critics. The thesis provides an original indication of the wide variety of activities that have been conducted between RISC and Government; to re-cap on some of the more eye-catching initiatives, these have included industry briefings, the formation of advisory groups on technical subjects, and the appointment of industry secondees inside Government (and vice versa).

The lack hitherto of scholarly interest in the level and types of activity being pursued by RISC has been surprising. That said, this research found no attempt by RISC, the Home Office or any other involved parties to conceal the scope of this activity; by contrast, it was striking how open senior Government and industry interview participants were willing to talk about its development with the researcher (albeit sometimes on the condition of anonymity), and how much information on the alliance's involvement in CT is available in both Government and industry documentation. Reflecting this, the existence of an overarching, organised and concealed conspiracy at the policy level could not be

detected; differing views existed within the sector on the effectiveness of RISC's activity and this thesis would not agree with those who would argue that 'unwarranted influence' is being exerted on CONTEST.

Furthermore, RISC's interest in seeking to work with Government would appear, from the evidence obtained (and arguably quite properly), to be focused on matters relating to the industrial aspects of national security - not on wider policy issues. In so far as this former priority is concerned, many views were presented of those who might be considered to be operating inside 'the SIC'; the overall sense gained was that, whilst some progress had been made in improving the level of cooperation between Government and industry since 9/11, there was considerable room for improvement. Furthermore, doubts were raised in some interviews with policymakers as to the actual, genuine *need* for Government to consult with industry and the effectiveness of RISC's activity; the picture that emerges is that Government can be dismissive of such external contributions, and therefore that the relationship is not always as 'cosy' as has sometimes been presented. This, of course, is not to deny the need to remain alert to any potential risks, or to suggest that everyone will agree that such a limited focus or desire for greater cooperation (not to mention the lack of effectiveness in it) is desirable; clearly more vehement critics of 'the SIC' might look unfavorably towards any such prospect. However, the evidence does not show that RISC has been seeking to extend its remit into the formation of CT policy outside industry-specific issues. Its possible motivation and ability to do so has been considered at the micro and macro levels and it would obviously be worrying if any such aim were to be successful. The reality, though, is that views in industry were disjointed and generally lacking unity of purpose; interviewees and other industry documentation raised questions of RISC's effectiveness at hitherto forging anything resembling a genuinely 'strategic' relationship with the Government on security issues.

A wide and diverse range of public-private interactions in the non-military aspects of CT was nevertheless presented by the evidence; even if such examples were generally found at the programme level. In contrast to the defence sector, however, what this study calls the ‘industrial complex’ in the CT sector incorporates several different features to those which characterize the classically-defined MIC. In CT, what constitutes ‘industry’ has been argued to comprise a *wider set of commercial entities* than merely profit-making security suppliers operating in the sector; private operators and business sectors clearly have a deep sense of their own roles in CONTEST, with the Government frequently articulating its own view of their necessarily strong level of involvement. Whilst questions were raised in the course of this dissertation around the extent to which companies or business sectors are genuinely engaged in or *pivotal* to the success of CONTEST, the research has shown that, in the sub-sectors under examination, the Government has made numerous and often serious efforts to engage the private sector in the pursuit of UK security objectives. Most notably, the success or failure of the UK’s CONTEST strategy (or any specific elements thereof) has been shown to have hinged in particular on the effective involvement of what this study has called the *private operators* of security; this was seen especially in the cases of e-Borders (with the aviation operators) and the London 2012 Olympics (with LOCOG). In these cases, it is argued that difficulties arose in part because, in the context of the complex governance arrangements that exist in the sector, there were serious problems with the manner in which the private sector was engaged.

A related, major differentiating characteristic of the ‘industrial-complex’ in CT, in contrast to the MIC, is that the sector possesses many more ‘purchasers’ of capability, spanning both the public and private sectors; ‘The markets are quite diverse – you have many purchasers’<sup>136</sup>, as one interviewee put it. Whilst this is not a new observation amongst policymakers, a case can clearly be made that its significance has hitherto been

---

<sup>136</sup> Interview, Ogilvie-Smith

under appreciated by the scholarly community. On the basis of this thesis, this characteristic of the security sector starkly contrasts with arrangements in 'the MIC' system where it is the MoD that is the 'single customer'<sup>137</sup> of capability. Furthermore, in the UK's non-military security arena, there was until 7/7 an absence of any serious attempts at consolidating Governmental departments and agencies insofar as they relate to the private sector. These differences are significant and deserve a wider appreciation.

It is this extreme multiplicity or diversity of stakeholders - the 'fragmentation' in the customer base as it was labelled by numerous interviewees - that can be seen to be a defining characteristic of the industrial-complex in the UK CT sector today. Within this system, it is not only governmental structures that are disaggregated; 'industry' itself can hardly be described as a cohesive supply chain. Indeed, as Stephen Phipson explained in response to a question on the effectiveness of government-industry cooperation across the security sector; 'The fragmented approach from the departmental view in government creates a very fragmented industry underneath it[.]'<sup>138</sup> Whilst some critics might disagree, the conclusion of this research is that it is this defining characteristic of the security sector - its structural fragmentation arising from its history and arguably very nature - that has hitherto mitigated against the emergence in the security sector of a 'cosy conspiracy' or singular 'industrial-complex' of the sort that has been often presented in MIC theory. Whilst several efforts - such as the formation of RISC and the appointment of an SRO for the Security Sector - have been made in recent years to increase levels of coordination in the security sector, the reality is that it remains a highly disaggregated picture, with multiple actors, departments, and companies working together on an almost countless number of sub-sectors and issues. The realities of Whitehall and commercial politics in this context have meant that, to date, nothing like the degree of proximity that has existed

---

<sup>137</sup> Interview, Industry Executive

<sup>138</sup> Interview, Stephen Phipson

between the defence industry and the Government has emerged in the non-military CT aspects of security.

Finally, the fact that the security sector is 'less mature'<sup>139</sup> than the defence market can also be identified as another significant difference in the character of the industrial-complex in CT when contrasted to the MIC. In a practical sense, the thesis showed how in the case of FiReControl, for example, a Government department (DCLG) did not possess the experience and expertise needed to deliver such a major security programme successfully. Additionally, it has been documented how the primary mechanism of strategic engagement between the Home Office and the security industry on CT issues, RISC, only emerged *after* 7/7. More generally, it is perhaps obvious to observe in retrospect that, as a result of the terrorist threat evolving so considerably (not to mention dramatically) during the 2000s, new security requirements would be bound to emerge, thus creating a relatively 'new' CT market for companies to compete within (and profit from). Whilst this statement might apply most directly to the experience of the US, the thesis has revealed and examined the allocation of significant additional resources for CT in the UK after 9/11, and the greater emphasis on public-private cooperation thereafter. As covered throughout this thesis, many writers, commentators and even scholars have been tempted in this context to apply MIC-type analogies to the security sector.

It would be overly simplistic to conclude that the dynamics of the MIC have simply transferred from 'defence' to 'security' in an identical way, however; this research has shown that whilst some of the dynamics associated with the MIC certainly have appeared in the CT sector, several important, if not fundamental differences exist in the manner in which the sector operates. Caution should be applied, therefore, in using the 'industrial-complex' label to describe the non-military security sector, or indeed any one of its

---

<sup>139</sup> Nick Watts, 'Latching onto the future', Interview with Richard Paniguan, 29 March 2014, Via: <http://www.defenceviewpoints.co.uk/interviews/latching-onto-the-future> (accessed 18.01.15)



individual sub-sectors such as CT; Chapters 3-5 illustrated considerable variety in the types of public-private cooperation even *within* one sector. MIC terminology may have perfectly reflected its time - it was first conceived in the 1960s - and may still be particularly applicable to categorizations of the military arena. That being said, neither the term 'the MIC' nor 'the SIC' fully capture the realities and the diversity of the private sector's involvement in all aspects of national security strategy today.

After careful examination of the MIC concept and close attention to the (limited) existing available literature on 'the SIC', the new data gathered for this thesis supports the conclusion that, provided that the clear and major differences that exist in the military and non-military sectors are recognised, 'industrial-complex'-type terminology can nevertheless be a useful term for describing the system of public-private (and wider) interaction that now so clearly exists in the non-military CT aspects of UK national security strategy. A system of extensive (and often malfunctioning) public-private interaction has undoubtedly emerged within CT and it is important to characterize and analyse this. Whilst the thesis has shown that several important differences exist in the character the MIC and the 'industrial-complex' in CT, dynamics once associated with the MIC are obviously present in CT; the 'revolving door' clearly operates in the non-military field, for example, and the examined case studies have also cast light on the commercial motivations of companies (such as EADS, Raytheon or G4S) or more strategic alliances (such as RISC) operating in security.

The system of public-private cooperation within CT is nevertheless extremely disaggregated. The 'industrial-complex' that has been presented in this thesis reflects how, in contrast to defence, the non-military security sector comprises many more public and private sector entities than the relatively more straightforward, simply three-cornered triangle (presented in Figure 2) that characterizes the MIC. The character of the structure

and typology of actors within the system that are present in the CT aspects of UK national security strategy are thus more multifaceted. On the basis of this research, it can be conceptualized as follows:

**Figure 5: The industrial-complex in the CT aspects of UK national security strategy**

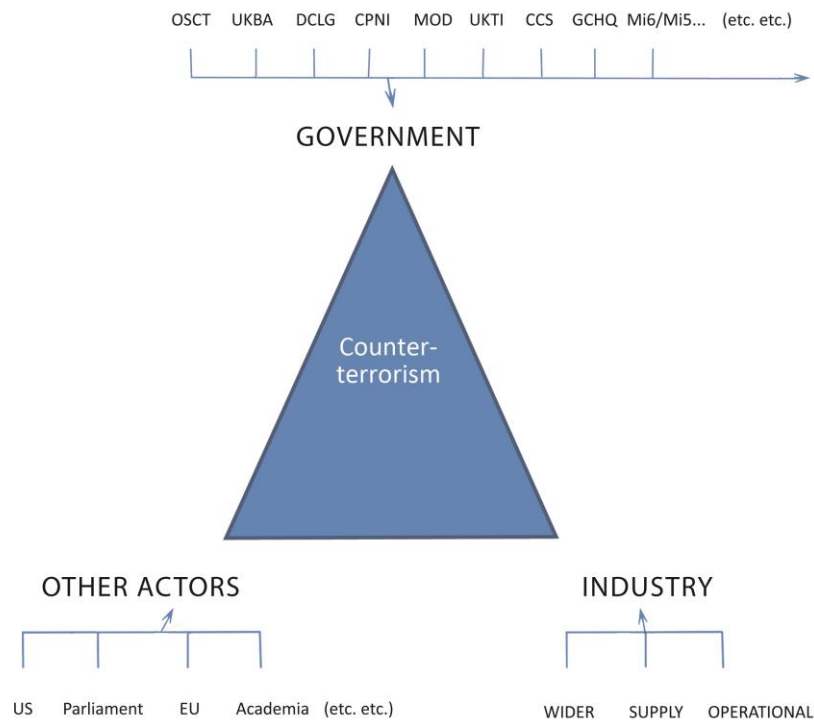


Figure 5 illustrates the ‘industrial-complex’ in the UK CT sector. The system encompasses extensive public-private interaction on CT issues; includes the involvement of a wide variety of public sector stakeholders; incorporates a diverse range of industrial entities; and stimulates the interest of other external ‘actors’ such as Parliament, the research community and other international entities.

Whilst in empirical terms the research has shown that the private sector has become deeply involved in various aspects of CONTEST, and that both Government and the private sector have frequently articulated the need for close cooperation, in a more general sense the ‘industrial-complex’ in this sector has not been found to have become organised to the extent that any combination of such actors has defined a shared, common

interest of a potentially damaging nature - let alone organised itself in the pursuit of any such interest. Supporting the above, a definition of the 'industrial-complex' operating in the CT sector is offered as flowing from this research:

A complex network of public-private security coordination, cooperation and transactions in the non-military CT aspects of UK national security strategy, whether monetary or non-monetary, that is often - but not necessarily always - mutually encouraged and fostered by a multiplicity of state, corporate (i.e. particularly those companies falling within 'Private Suppliers', 'Private Operators' and 'Wider Business' categories<sup>140</sup>) and sometimes legislative actors, the various parts of which may possess potentially variable interests in promoting high levels of private sector involvement in 'security', and indeed levels of CT security spending.

Whilst this definition could be seen as multi-faceted, and critics of 'the SIC' might not embrace it, based on this work it is argued that such a characterization of the industrial-complex in the UK CT sector is a fair one which could serve as a useful basis for future debate on the scope and potential impact of this proposed system.

As well as presenting a new understanding of the character of the 'industrial-complex' in operation within the UK's non-military CT sector, this thesis also concludes that there may be some value in continuing to explore whether something resembling an overarching 'national security-industrial complex' now cross-cuts *all* aspects of contemporary UK national security strategy; i.e. in keeping with the Government's broader interpretation of national security covered above, and as Hughes and two other scholars have recently argued.<sup>141</sup> Whilst this thesis has focused its attention on the non-military CT aspects of UK national security alone, thus making it impossible to make a definitive conclusion on this matter, there is, however, reasonable evidence above to suggest that there could be solid grounds for a skeptical reading of this particular theory for several reasons. Firstly, this thesis has clearly shown that, within the CT sector alone, there is a considerable lack of coordination between industry and Government on numerous issues;

---

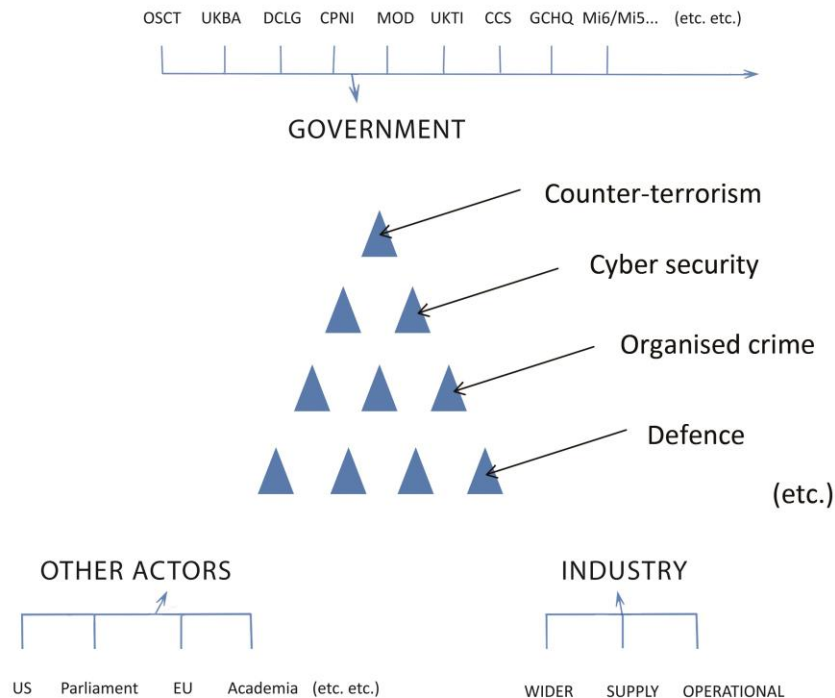
<sup>140</sup> Introduced in section 1.7

<sup>141</sup> Hughes, *War on Terror Inc.*; Baker-Beall and Robinson, 'The Emergence of the Security-Industrial Complex'

the idea that a structured, organised system able to exert influence encompasses this and the interactions within so many other diverse security policy issues - many of which it is widely recognised are at a very early stage of development - seems implausible.

Secondly, it is not clear that it is desirable to 'lump' together under the same overarching label the various types (and aggregation) of the public-private interactions that exist within the different sub-sectors of national security broadly defined; not enough is yet known about the character of the rapidly-evolving relationships in each area of security, and such a grand argument might actually help to conceal the plausible reality that there are a variety of systems at play. For example, it can be recalled from the opening chapter that the MoD continues to draw the largest share of UK national security expenditure; it should not be forgotten, therefore, that the MIC traditionally associated in the military sector continues to operate. In the non-military security arena, it is entirely feasible on the basis of this research that each major theme or specific area of non-military security (such as CT, cyber security, or organised crime, for example) could possess different, potentially unique or distinct public-private interactions from one another. In the absence of more comprehensive mapping of such dynamics within each and every sub-sector of the security arena (and, indeed, analysis of any identifiable connections between them) - a task outside of the scope of this thesis - it is concluded that it may be more useful, at the present time, to refer to the presence of a variety of individual 'industrial-complexes' existing in each specific sub-sector - as indicated by the multiple triangles within then system presented in the diagram below:

**Figure 6: A multitude of security-industrial complexes?**



Whilst a case can be made, therefore, that further conceptual and empirical analysis in these wider areas of security is needed, this thesis has clearly illustrated that an ‘industrial complex’ of a new description has arisen in one contemporary non-military security field; the CT strand of the UK’s national security strategy.

Finally, it should be recalled that whilst this is not the first piece of writing to have argued that an ‘industrial-complex’ has emerged in the context of the post-9/11 terrorism threat, it is novel in the UK context that, having considered new and hitherto unavailable data, this thesis views the system in a less negative and a more nuanced way than many authors. In its analysis of the character of the private sector’s involvement in the non-military CT aspects of contemporary UK national security strategy the thesis did not find any meaningful evidence to support the conspiracy-type theories that have been presented; it provides a reassessment of ‘the SIC’. It is hoped that in its new interpretation

of this system of public-private interaction in CT, the analysis, models, and findings it has provided will help to inform future policy and scholarly discussions on the character and consequences of the private sector's involvement in other areas of national security strategy.

### **8.3 Consequences**

This thesis has addressed questions of relevance to policy practitioners, and as such efforts have been made within the analysis to highlight some of the consequences of the private sector's involvement in specific areas of CT. Having presented the character of the 'industrial-complex' in CT, it is now possible to draw a more general set of lessons about the consequences of such involvement; and to apply them to future efforts at public-private security cooperation.

The first such conclusion to be drawn from this research is that, as certain dynamics associated with the MIC clearly now operate in the CT arena, Eisenhower's previous concerns do appear equally relevant in their application to the non-military security field, and thus remain prescient. Whilst as noted above no overarching conspiracy has been detected in the UK CT arena, two insights in particular suggest that, as Eisenhower famously encouraged, it would be beneficial for the public to remain alert to the potential dangers associated with any 'unwarranted influence' arising in the security field. The thesis has shown that, in three instances, several commercial, profit-making suppliers gained financially from their involvement in major publicly-funded CT-related security contracts; contracts which ultimately were not delivered in full, or had to be cancelled. Furthermore, whilst none of RISC's specific behaviour or activity has been found to have been inappropriate, both its motivations and the potential influence it has exerted to date have been shown to be at least partly commercially-orientated. Whilst many if not most policymakers would appear to have little difficulty with for-profit entities being

involved in working with Government in areas of national security such as CT – indeed Chapter 7 detailed, for example, how the current Administration is actively pursuing a policy aimed at promoting UK-based security companies in international markets - it is a cause of concern that in some cases companies (suppliers and consultancies) have profited financially from programmes that have simply not been delivered.

It should also be recognised, as this thesis has consistently noted, that the industries supporting national security do have many critics; any balanced analysis of the private sector's involvement in CT (or any 'SIC' more generally) must recognise this, along with the conclusion that, as Eisenhower explained, it would be alarming if any individual or coalition of companies were able to unduly exert influence in directing Government security policy. Many critics have suggested, for example, that the terrorism threat to the UK has been over-inflated – and, indeed, that companies are either involved in or are set to profit from such an assessment. Furthermore, as discussed in Chapter 7 there may be some emerging, specific areas, or public-private interaction where critics may be justified in expressing concern. The UK Government's growing level of support for CT-related industry exports, for example, including to countries where human rights concerns have been expressed, is an area that warrants greater attention. In the same way that Government strategies on defence exports have historically been strongly associated with concerns over the MIC - and generated considerable scholarly scrutiny - so this is an area of public-private coordination around which the proximity in the relationship should generate greater debate.

Whilst it is clear that difficulties arising with major UK Government contracts (including those leading to complete failure) are not limited to the CT or wider security sector<sup>142</sup>, it is noticeable how three of the largest CT-related contracts let after 9/11 and

---

<sup>142</sup> As recently illustrated in King and Crewe, *The Blunders of our Governments*

examined in this thesis all encountered significant problems. The reasons for the challenges associated with each of FiReControl, e-Borders, and the G4S Olympic security contract have been covered extensively in Chapters 3-5, and will not be repeated here; suffice to say that the lack of experience within the Government's non-military departmental structures for managing such major schemes can be seen to have contributed to the difficulties. Furthermore, the need for deep and extensive external stakeholder engagement in implementing each contract - a much broader type of engagement than has been seen with classic military procurements - was in the cases of FiReControl, e-Borders and the G4S security contract not properly executed for several reasons. Serious challenges and obstacles were encountered, with unfortunate scenarios emerging whereby requirements were changing frequently; the sense left was that those in Government who were responsible for them were simply not equipped to handle the level of complexity they encountered.

The thesis concludes, on the evidence of the examined CT case studies, that the system of non-military security procurement in the UK requires a radical overhaul. The implication of this is that those involved in the UK CT and 'wider security' sector should strive to do better in their approach to the development and implementation of major acquisition projects. This could be achieved by drawing on existing best practice in this area through training as necessary; by seeking to work with the private sector on this issue more strategically; and by resisting wherever possible the unfortunate political (and other short-term) urges that were clearly evident in the examined case studies. In considering any new approach or future reforms in this area, it is also suggested that all concerned parties would do well to take account of an argument that has been made by one UK analyst, Gash, who argues convincingly:

The contracting process can't be seen as separate from policy and operational matters as it has allowed to become and incentives need to



change to shift focus from getting a 'good deal' upfront to securing value for money and quality across the contracting period.<sup>143</sup>

In retrospect, the dynamics identified within this statement were all too evident in the cases of FiReControl, e-Borders and the G4S security contract; the schemes all suffered from short-term considerations, and it has been shown that the policymakers that were responsible for the programmes either mishandled or took too little interest in them. It has, of course, often been observed that many major UK Government contracts (especially IT-based solutions) frequently encounter difficulties, potentially leading to expensive contract failures; an idea which has arisen both inside and outside the security sector. That being said, it is obviously an undesirable state of affairs and should therefore not be too readily accepted. The non-military UK security community has lessons to learn on the basis of the examined contracts and must aim for improvement; particularly given that 'security' represents the State's primary duty. At the risk of over-stating the case, an argument could easily be made that those involved in the sector should strive to establish new, more effective procurement models that might even form the basis of reform to acquisition across the whole of Government.

In addition to identifying problematic CT-related security contracts, and wider concerns over the types and level of public-private cooperation in the sector, it has also been shown that the character of the current system of independent, external oversight over such dynamics in the non-military security arena has been ad hoc, reactive and, on occasion, ineffective. Whilst the NAO has conducted a number of useful reviews on FiReControl, and in relation to UK CT-related security acquisition more generally, Parliamentary scrutiny of the interactions under examination has in particular been very mixed. Not only did it not help to prevent - or, indeed, see a role for itself in preventing - the contract failures which occurred, the thesis has argued that in one case (Olympic

---

<sup>143</sup> Tom Gash, 'Blame Games', *Institute for Government Blog*, 20 July 2012, Via: <http://www.instituteforgovernment.org.uk/blog/4658/blame-games/> (accessed 28.11.13)

Security) the UK Parliament (in the form of the HASC) actually misdiagnosed the problems which occurred. Whilst this finding might offer SIC critics some comfort in the sense that the UK Legislature appears to have avoided becoming a part of a potentially corrosive system of the type Eisenhower warned against, its political posturing on the issues appears to have hardly been constructive. Unlike the often detailed scrutiny conducted historically by the Defence Select Committee around the role of the DIB in national security, for example, the private sector's involvement in the non-military aspects of contemporary security strategy such as CT has simply not received the Parliamentary attention that it probably deserves in the context of the extensive levels of cooperation that has been revealed in this thesis.

Whilst this dissertation's main focus has been to analyse the character of the private sector's involvement in the non-military CT field, rather than develop recommendations, several practical policy implications regarding public-private security cooperation can be drawn from the work. Firstly, it is striking how so many Government officials involved in the public-private cooperation under examination do not appear to fully appreciate the various commercial motivations at play in the private sector; a lack of commercial awareness and skills in Government has been cited as a major contributor to why the public and private sectors had not developed a stronger level of cooperation. The logical conclusion, therefore, is that those in Government with responsibilities for engaging the private sector would do well to think more commercially than they currently do, and that more could be done to equip them with the knowledge and tools they need to succeed in managing their relationships with companies. Equally, it is not clear that all the private sector participants engaged with during this research - or, indeed, the industry structures that have been created to facilitate cooperation with Government, such as RISC - possess a realistic understanding of how far (and on which issues) Government may actually wish to engage the private sector in their response to national security issues. The

impression left is that, on both strategic and programme-level CT engagement, the two 'sides' have not yet conducted a proper discussion on the desirable level of cooperation that should be developed. Given the level of interdependency that would appear to exist between them - a level arising from the aggregation of the large number and variety of public-private interactions within CT that might surprise some - this can be seen as a major, if not *the* major failing of both the public and private sectors in so far as they may have mutual responsibilities for providing national security.

Secondly, whilst in its empirical analysis this thesis has focused on the CT elements of national security strategy, at the theoretical level it can be suggested that it is likely that a significant, perhaps even increasing level of interdependency may now exist between Government and the private sector in the implementation of UK objectives in other non-military areas of security. As noted above, privatization has taken place extensively within the CT sector; whilst it was not the focus of this thesis, it often seemed when discussing broader security issues in interviews as if few areas are now 'off limits' for private sector involvement. Having been asked whether some security functions should never be handed to the private sector, for example, one Government official replied: 'I'm not sure that there are many that I would say could *never* be outsourced.'<sup>144</sup>

Finally, a consensus view emerged amongst interview participants that much could be done to strengthen public-private security cooperation. Indeed, the impression left is that, in contrast to defence, the level and quality of the Government's interaction with the CT sector (and the 'wider security' field more generally) remains 'ad hoc' and often at an early stage of development. The implication of this, in the context of the UK Government's perception of the strategic security risk environment (i.e. where non-military issues such as terrorism are seen to be the highest priority issues), is that both the UK's formal National

---

<sup>144</sup> Interview, Government Official (Emphasis added)

Security Strategy and its associated documentation (such as the SDSR) should rethink their primary defence orientation and adopt a more security-focused outlook; especially insofar as its industry aspects are concerned. Within this context, having not yet properly re-orientated their outlook, it is not implausible that in other emerging areas of security strategy, such as cyber security, policymakers may need to reassess the nature of their relationship with the private sector. It became apparent during research for this thesis that the private sector is already deeply involved in the implementation of the UK's cyber security response, and that the Government recognizes its crucial dependence upon companies in this field. It is extremely doubtful, however, that the task of developing robust structures for public-private cooperation on cyber security is 'complete' - this thesis has shown the mixed effectiveness of the structures established for CT-related public-private interaction over the course of more than a decade. On the basis of this research, the development of effective coordination mechanisms with the private sector in the cyber security arena may prove to be as important as other types of public-private interaction (such as contracts) in this emerging sector.

In addition to highlighting these potential implications for policymakers, this thesis also argues that the findings of the research have significant consequences for the scholarly community; especially insofar as future research priorities on the 'privatization of security' and indeed 'the SIC' should ideally be developed. In particular, the thesis has shown that, in line with the emergence of the UK Government's broader understanding of 'national security', the private sector has been playing an extensive supporting role, at least in CT; in that context, it follows that an even broader research agenda on the private sector's involvement within this arena is desirable. Whilst as noted in Chapter 1 some efforts have been made to direct the research agenda in this respect - and indeed to revisit what constitutes the 'security industry' in the new context - it is fair to say that the existing body of literature does not yet go far enough. In seeking to fill a gap in existing work, this

research has shown how in the CT aspects of UK security policy a much wider variety of under-researched public-private interactions have emerged, encompassing a considerably broader range actors than the scholarly community has to date properly acknowledged. The consequences of the aggregation of these multiple public-private dynamics and associated interests - an aggregation or a system which this thesis presents as an 'industrial-complex' of a different character to the MIC - have not been properly considered within the research community. In the absence of stronger scholarly analysis and oversight in this context, it can be stated that academia has not properly scrutinized Government activity in this area.

Furthermore, it has become apparent that the primary preoccupation of both policymakers and scholars within the 'security privatization' field has been, and remains, focused on the activities of the traditional DIB and/or PMSCs operating overseas. These sectors will obviously continue to draw substantial investment and present important and difficult policy, legal, operational and ethical questions, all of which will continue to demand expert attention and analysis. However, this thesis has considered the multiple interactions, difficulties, tensions and even accusations relating to the private sector's involvement in the non-military CT arena after 9/11, and shown how enormous difficulties have emerged in this emerging area of public-private cooperation. In this context, the adoption of an even broader approach to future research on the privatization of security - an approach incorporating both CT but also many other additional non-military security issues - is not only completely warranted, but now overdue.

Whether the result of academia's lack of awareness, or interest, to properly address the substandard operation of many of the public-private interactions illustrated in the CT field - a situation which has contributed not only to the loss of billions of pounds of UK taxpayers' money, but also raised serious doubts over the efficacy of many of the UK's

existing security arrangements - has been a regrettable oversight. It is not to seek to dismiss or undermine the important research that has been completed in the defence sector to say, in support of the argument made previously by Abrahamsen and Williams, that it is time to broaden perspectives outside the current PMSC preoccupation.<sup>145</sup> The private sector's involvement in national security strategy is more widespread and this suggests that additional scrutiny should be applied to other public-private relationships. This thesis seeks to make a contribution towards a new understanding of the UK's CT sector in this respect, and offers a framework that could be adapted to conduct analysis of the private sector's involvement in other security sub-sectors. The application of this approach to the field of cyber security may actually be the most pressing immediate research priority. Indeed, an apparent shortage of analysis in this area is potentially creating the situation where - much like with the experience of the many negative presentations of 'the SIC' examined in this thesis - misconceptions may be arising about the roles of the private sector in mitigating challenges in the cyber area. In particular, the suggestion that a damaging 'cyber-industrial complex' may be emerging - as Brito and Watkins have recently argued in a U.S. context<sup>146</sup> - would warrant further scrutiny.

#### **8.4 Concluding remarks**

This thesis has found that a direct application of the MIC (as it has been traditionally defined) - or, rather, some of its individual dynamics - to the security sector is appropriate in several identified areas, but that ultimately any presentation of 'the SIC' in exactly the same terms does not sufficiently capture the character of the public-private dynamics now present in the non-military aspects of contemporary security such as CT. In presenting a more detailed analysis of such dynamics in the UK's CT field than has even been

---

<sup>145</sup> See footnote 68 (Chapter 1)

<sup>146</sup> Brito and Watkins, 'Loving the Cyber Bomb'

attempted, the dissertation has sought to provide a reassessment of the 'industrial-complex' in this sector.

In analysing the dynamics of this system, the thesis highlights several shortcomings in respect of how public-private security cooperation (especially in relation to contracts) has been handled in the UK CT sector after 9/11. The CT sector (and 'wider security' arena more generally) has been shown to be characterized by complexity, and in this context numerous issues have arisen around the effectiveness of public-private cooperation within it; despite every best effort, there is discontent within the sector that the 'terms of engagement'<sup>147</sup> between the Government and the industries supporting national security are not operating as effectively as they could. Furthermore, whilst there have been some successful examples (such as 'New Dimension'), the UK has experienced a series of costly contract failures in the CT sector; 'failures' seen both from a financial and operational perspective. When problems have arisen, rather than these being addressed more constructively we have seen how 'blame games' have played out very publicly. Whilst such dynamics are not unique to the security sector, it is striking how Government representatives in particular pointed the finger of blame towards industry forcefully in two of the three examined contract case studies (e-Borders and the G4S contract). Whilst these experiences support this thesis' overall argument that it is unlikely, therefore, that an industrial-complex of a more conspiratorial character has emerged in the UK's CT sector, that such disputes appear to have arisen so frequently in this arena can hardly be viewed as being reflective of an ideal situation.

The final recommendation of this thesis, therefore, is that all those concerned with the examined issues would do well to seek to develop a much more informed and nuanced approach towards public-private engagement in CT and other areas of 'wider security'. This

---

<sup>147</sup> See footnote 35 (Chapter 1)

thesis offers some ideas on how the public and private sectors might come together more effectively on public security (and wider government) contracts; in the end, however, it seems that what is really needed is an improved attitude towards engagement. One interviewee for this thesis perhaps summarised it best when offering ideas on how public-private engagement might be improved in the security sector:

Certainly government would get more out of industry if they tried to get their heads round how industry work (...) as well as sort of acknowledging the huge part that industry plays in delivering security, and making it more of a partnership in terms of how they acknowledge it explicitly[.]<sup>148</sup>

The reality, therefore, is that whilst after 9/11 the public and private sectors have probably cooperated more closely on CT than on any aspect of national security in recent centuries, it is not as much of a 'partnership' (or shadowy conspiracy) as some authors have previously asserted. A variety of attitudes and outlooks exist in the sector, but Stephen Phipson summarized it well when describing the character of the relationship:

...it's almost like two different universes in many respects. I think there are different motives and different objectives between the public and private sectors. (...) And it's quite hard to mesh those two things together.<sup>149</sup>

Some critics of the SIC might be reassured that the public and private sectors are seen at senior levels of Government to be so far apart, and that they are so difficult to 'mesh' together.

This thesis offers an analysis on the origins, character and consequences of the private sector's involvement in the non-military CT aspects of contemporary UK national security strategy and has found that a form of 'industrial-complex' exists in this sector. The evidence found does not support the contention that it is an exact replica of the MIC, or that it has hitherto constituted a conspiracy. This is not to say, however, that 'the SIC' - whether it exists within an individual sector or more generally across national security

---

<sup>148</sup> Interview, Industry Executive

<sup>149</sup> Interview, Stephen Phipson



strategy - should not continue to be discussed or debated. On the contrary, this thesis argues that in the CT sector an 'industrial-complex' of a new character has emerged, which demands considerable additional attention, and that the spirit of Eisenhower's final Presidential address should continue to be heeded in this context. It is vital, therefore, that these emerging public-private security relationships are developed in as 'open' a manner as possible, and that they draw a new, heightened level of analytical attention from policymakers and researchers alike. To start the new debate, this thesis concludes that the extensive network of public-private interaction is not only a reality within contemporary UK national security strategy; it is an under-appreciated necessity.

## Appendix A: Interview Participants

**John Backhouse** - Formerly Non-Executive Director/Consultant, *Smiths Detection* and Chairman, *JNSRAC*

**John Brading** - Formerly Head of Security Systems and Solutions, *Raytheon Systems (UK)*

**Michael Clayforth-Carr** - Executive Director of International Subsidiaries, *Selex ES*, Chairman of Security Sector Advisory Group, *UKTI*; Formerly Chairman, *RISC*

**Rob Coleman** - Director of Centre for Applied Science and Technology, *Home Office*

**Ruth Davis** - Head of Programme - Cyber, Justice and Emergency Services, *techUK*

**Charlie Edwards** - Director, National Security and Resilience, *RUSI*; Formerly Deputy Director for Strategy and Planning for Security and Counter Terrorism, *Home Office (OSCT)*

**David Evans** - Chief Executive, *IntraVires*; Formerly Co-Chairman of Industry Advisory Group on London 2012 Olympic Security and Project Director, *BSIA*

**Simon Everest** - Senior Security Advisor, *UKTI DSO*

**Richard Fletcher** - Formerly Security Policy Advisor, *EADS (UK)*

**Paul Hamilton** - Head of Industrial Policy, *Ministry of Defence*

**Shaun Hipgrave** - IBM i2 Lead UK and Ireland, *IBM (UK)*, Vice President of Security, *ADS Group*, and Member, *RISC Council*

**John Howe** - Member, *RISC Council*; Formerly Vice Chairman, *Thales (UK)* and Chairman, *RISC*

**Alan Jenkinson** - Director Strategic Business, Home and Foreign Affairs, *Hewlett-Packard (UK)*; Formerly Industry Seconded, *Home Office (OSCT)*

**Derek Marshall** - Formerly Director of Policy, *ADS Group*; Secretary, *RISC*

**Francesco Norante** - VP Smart Cities and Major Events, *Selex ES*; Formerly Director of Security Integration and Planning for Vancouver 2010 and Turin 2006 Olympic Games

**Professor Adam Ogilvie-Smith** - Security Consultant, *CGI* and Visiting Professor, *Robert Gordon University*; Formerly Industry Seconded, *Home Office (OSCT)* and Industry Seconded, *UKTI DSO*

**Professor Sir David Omand** - Visiting Professor, King's College London; Formerly UK Security and Intelligence Coordinator, *Cabinet Office*, Permanent Secretary, *Home Office*, and Director, *GCHQ*

**Mark Phillips** - Policy Adviser, *ADS Group* and Secretary, *RISC*; Formerly Head of the Land Operations and Capabilities, *RUSI*, and Chief of Staff to Baroness Neville-Jones (Shadow Security Minister)

**Stephen Phipson** - Director Security Industry Engagement, *Home Office (OSCT)*; Formerly Chairman, *RISC* and Chairman of Security Sector Advisory Group, *UKTI*

**Robin Southwell** - CEO, *EADS (UK)*; Formerly President, *ADS Group*

**Neil Stansfield** - Head of Head of Knowledge, Innovation, and Futures Enterprise, *DSTL*; Formerly Head of Science and Technology Unit, *Home Office (OSCT)*

**Sir David Veness** - Chairman Security and Resilience Board, *London First*; Formerly Assistant Commissioner (Specialist Operations), *Metropolitan Police Service*

**Admiral the Lord West of Spithead** - House of Lords; Formerly Minister for Security, *Home Office*

Three additional interviews were held on the condition of anonymity.

## **Appendix B: Interview Process**

### *Ethical Approval*

This thesis planned to generate new and potentially sensitive material relating to UK national security through semi-structured interviews and, as such, it was necessary to receive ethical approval from King's College London's War Studies Group Research Ethics Panel. In completing this requirement, the author proposed that several risks would be managed in completing the interviews; robust confidentiality and withdrawal arrangements were designed and codified by a 'consent form', for example, and the fact that many of the participants would already be known to the author meant that steps were taken to ensure that the research was conducted in an appropriate way. The author would also mitigate more sensitive security risks by focusing on the philosophical aspects of the research questions, rather than operational aspects which might relate to them. The Ethics Panel was satisfied with the design and approach of the interview methodology, and granted ethical approval to the author on 19th May 2011.

### *Participants: Selection and Breakdown*

37 potential interviewees were invited to participate in interviews on the basis that they were identified as having had some direct experience of working on, or possessing detailed knowledge about, issues pertaining to this thesis's examination of the private sector's involvement in the CT aspects of contemporary UK national security strategy since 9/11.

Judgments informing the issuing of invitations were based on three factors relevant to the individuals' relevant involvement or knowledge: 1) their likely direct working knowledge/experience of the subject arising from publicly-available biographical information; 2) their direct involvement in government-industry initiatives (such as RISC and the SSAG, for example); and 3) consideration of whether the individual was directly involved in, or would be aware of, the specific case-studies included in the thesis. In two cases, individuals were approached on the basis that a separate interviewee had

recommended that the author might benefit from meeting with them. Decisions to issue invitations were also informed by the author's previous experience in the sector (outlined in Appendix C).

26 of the 37 people who were invited to be interviewed agreed to participate; the remaining 11 declined (seven of whom were crown officials and one of whom initially agreed to participate before later declining). The 26 participants were individuals who at the time of their interview were actively working on issues relating to the private sector's involvement in CT from within government (7), industry (10), trade associations (2), or academia (3). The remaining four (4) individuals who participated in the research were retired individuals who had until recently been operating at senior levels in the sector (three of whom had operated in both government and industry, and one of whom was a former senior industrialist). It should also be noted that 15 of the 26 participants had during the course of their careers worked in more than one of the categories of interviewee (i.e. government, industry or academia).

#### Question Design

A programme of semi-structured, elite interviews - each approximately 45 minutes - was conducted to explore the philosophical aspects and case-studies examined in this thesis; its design allowed for discussions on a wide and varied range of topics relating to the thesis, and provided considerable scope for the generation of new material.

Seven general questions were formulated to guide and help structure the interview; this number was judged to be optimal in that it allowed for a response time of around 5 minutes for each. Having been introduced to the aim of the research, each participant was asked the following opening question to explore their own understanding of the core questions around/issues pertaining to the thesis:

1. How would you describe the character of the relationship between the public and private sectors in contemporary UK national security strategy?

Six (6) additional general questions were also asked of every participant in order to help facilitate discussions / generate viewpoints on the origins, characteristics and the consequences of the private sector's involvement in CT since 9/11:

2. Is there anything specific about the character of the relationship between the public and private sectors in the CT aspects of national security, i.e. in contrast to other areas of security policy?
3. Are there any national security tasks/functions that you would consider to be 'inherently governmental'? (i.e. that should only be conducted by the state and not the private sector)
4. How effective do you consider public-private engagement in UK national security strategy to be at the level of policy and strategy-making? (e.g. RISC)
5. How effective do you consider public-private engagement in UK national security strategy to be at the programme and procurement level? (e.g. G4S / e-Borders / FiReControl)
6. What accounts for the levels of expenditure in CONTEST, and/or specific contracts discussed in question 5. (as relevant)?
7. How could public-private cooperation in the CT/wider security sector be improved in the future?

Possible alternative 'leading' interview questions were considered; these related to such issues as the private sector's role in stimulating investment in CONTEST and the appropriateness of the methods of private sector oversight in the CT sector. Whilst these issues are addressed in this thesis, they were not selected as 'core' interview questions because they were considered to be too 'loaded' and/or not seen to relate to the main research questions as directly as those listed above.

#### Transcription and Quotation Process

All 26 interviewees who participated agreed to sign a consent form prior to the interview, and all were content with the author using a digital recorder for the purpose of subsequent transcription. Three interviewees requested that their contributions be non-attributable under all circumstances, with the remaining 23 participants indicating that they would be happy to be quoted (or be approached for a direct quotation) following their interviews. Having completed each interview, the author completed a full note of the session for his own records; this included a transcription of all passages and quotations judged to be

directly-relevant to the thesis. A phase of consultation took place during later stages of the project; all of the quotations arising from interviews in this thesis appear after the participant confirmed that: 1) it was a fair reflection of what was said / their interpretation of events; and 2) they approved of the manner in which it appears (i.e. attributable or non-attributable).

## **Appendix C: About the Author**

Hugo Rosemont is an award-winning security policy analyst and practitioner. In January 2015, he was appointed Teaching Fellow and Assistant Director of the Centre for Defence Studies at the Department of War Studies, King's College, London. He has pursued his PhD with the same Department at King's College since January 2011.

From 2008-2012, Rosemont served as Security Policy Advisor to ADS - the UK trade organization advancing the British aerospace, defense and security industries. In this role he provided security policy advice to the ADS Security Board and supported the UK's leading security industry alliance: RISC.

Previously, he served as a member of the UK Home Office's Olympic and Paralympic Industry Advisory Group and was Security Executive to both the winning London 2012 Olympic bid team and the London 2012 Organizing Committee (LOCOG) during its initial stages. He also has experience in project management roles at HM Treasury and for a political party's conference unit.

Hugo holds Masters degrees in European Politics from London Birkbeck University and in International Security Studies from the University of St Andrews, for which he was awarded a distinction in 2006.



## BIBLIOGRAPHY

### PRIMARY MATERIAL

#### A. UNPUBLISHED

##### Interviews

Backhouse, John. Formerly Non-Executive Director, Smiths Detection, Derby, 14 March 2014.

Brading, John. Formerly Head of Security Systems, Raytheon (UK), London, 28 November 2013.

Clayforth-Carr, Michael. Executive Director of International Subsidiaries, Selex ES, London, 17 June 2013.

Coleman, Rob. Director of CAST, Home Office, London, 12 September 2013.

Davis, Ruth. Head of Cyber, Justice and Emergency Services, techUK, London, 16 April 2014.

Edwards, Charlie. Director, National Security and Resilience, RUSI, London, 20 December 2013.

Evans, David. Chief Executive, IntraVires, London, 17 June 2013.

Everest, Simon. Senior Security Advisor, UKTI DSO, London, 26 November 2013.

Fletcher, Richard. Formerly Security Policy Advisor, EADS (UK), London, 11 December 2013.

Government Official (under anonymity). London, 27 November 2013.

Government Official (under anonymity). London, 18 March 2014.

Hamilton, Paul. Head of Industrial Policy, Ministry of Defence, London, 27 November 2013.

Hipgrave, Shaun. IBM i2 Lead UK and Ireland, IBM (UK), London, 26 June 2013.

Howe, John. Member, RISC Council, London, 19 June 2013.

Industry Executive (under anonymity). By telephone, 11 December 2013.

Jenkinson, Alan. Director Strategic Business, Home and Foreign Affairs, Hewlett-Packard (UK), London, 16 September 2013.

Marshall, Derek. Formerly Director of Policy, ADS Group and Secretary, RISC, London, 9 September 2013.

Norante, Francesco. VP Smart Cities and Major Events, Selex ES, London, 12 March 2013.

Ogilvie-Smith, Adam. Security Consultant, CGI and Visiting Professor, Robert Gordon University, London, 12 June 2013.

Omand, David. Visiting Professor, King's College London, London, 20 June 2013.

Phillips, Mark. Policy Adviser (Security and Resilience), ADS Group and Secretary, RISC, London, 12 June 2013.

Phipson, Stephen. Director Security Industry Engagement, Home Office (OSCT), London, 12 July 2013.

Southwell, Robin - Formerly CEO, EADS (UK), 12 December 2013.

Stansfield, Neil. Head of Head of Knowledge, Innovation, and Futures Enterprise, DSTL, London, 13 September 2013.

Veness, David. Chairman Security and Resilience Board, London First, London, 21 June 2013.

West, Alan. House of Lords, London, 19 September 2013.

#### **Official Documents**

Home Office. 'Audit and Review of Olympic & Paralympic Safety & Security Planning. November 2010.

Home Office. 'Director - Security Industry Engagement'. Job Description. December 2012.

Home Office. 'Levering Games Security success to boost UK security industry strength and economic growth – post workshop proposal'. March 2013.

#### **Industry Documents**

Backhouse, John B. Letter from John Backhouse to Bruce Mann (Cabinet Office). 20 February 2006.

'Intellect Minutes'. Meeting of the National Security & Resilience Council. 20th June 2005

'Intellect Minutes'. Meeting of the Joint National Security & Resilience Advisory Council. 27 July 2005

JNSRAC. "'Project Gain": Government and Industry Network for Security and Resilience, A proposal from the UK Security and Resilience Supply Base'. June 2006.

JNSRAC. 'JNSRAC Minutes'. Communications and Liaison Sub-Committee. 7th November 2005

JNSRAC. 'JNSRAC Minutes'. Joint National Security & Resilience Advisory Council. 13 December 2005

JNSRAC. 'JNSRAC Minutes'. Joint National Security & Resilience Advisory Council. 12 December 2006

RISC. 'UK Security and Resilience Suppliers Council (RISC) Minutes'. 9 January 2007

RISC. 'Security and Resilience Growth Partnership - Proposal'. DRAFT Version.2.1. June 2013.

### **Private Correspondence**

Backhouse, John. Former Chairman of JNSRAC. Response to questions via email. 23 October 2014.

Barclay MP, Stephen. Member of the House of Commons Committee of Public Accounts in the UK Parliament. Response to questions via email. 6 January 2014.

Amery, Andrew. Former Head of Security Operations for the London 2012 Organising Committee. Response to questions via email. 12 August 2014.

Evans, David. Former Project Director – 2012, BSIA. Response to questions via email. 6 November 2014.

Marshall, Derek. Former Director of Policy at ADS and Former Secretary to RISC. Response to questions via email. 17 September 2013.

Ogilvie-Smith, Adam. Security Consultant, CGI and Visiting Professor, Robert Gordon University. Response to questions via email. 22 October 2014.

Phillips, Mark. Secretary of RISC and Policy Adviser (Security and Resilience) at ADS. Response to questions via email. 13 November 2014.

House of Commons Library. Response to question via email. 7 January 2014.

## **B. PUBLISHED**

### **Official Documents**

#### *Government Documentation*

Cabinet Office. Departmental Report 2001. Cm5119 . Via:  
[http://webarchive.nationalarchives.gov.uk/20100304041448/http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/annualreport/co\\_report2001.pdf](http://webarchive.nationalarchives.gov.uk/20100304041448/http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/annualreport/co_report2001.pdf) (accessed 30.10.13)

Cabinet Office. Departmental Report 2002. Cm5429 . Via:  
[http://webarchive.nationalarchives.gov.uk/20100304041448/http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/annualreport/co\\_report2002.pdf](http://webarchive.nationalarchives.gov.uk/20100304041448/http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/annualreport/co_report2002.pdf) (accessed 30.10.13)

Cabinet Office. Departmental Report 2003. Cm5926. Via:  
<http://webarchive.nationalarchives.gov.uk/20100416132449/http://www.cabinetoffice.gov>

[v.uk/media/cabinetoffice/corp/assets/publications/reports/annualreport/co\\_report2003.pdf](http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/annualreport/co_report2003.pdf) (accessed 30.10.13)

Cabinet Office. 'National Risk Register of Civil Emergencies – 2013 Edition'. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/211867/NationalRiskRegister2013\\_amended.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/NationalRiskRegister2013_amended.pdf) (accessed 29.12.14)

Cabinet Office. 'The National Security Strategy of the United Kingdom: Update 2009: Security for the Next Generation'. June 2009. Via: <http://www.official-documents.gov.uk/document/cm75/7590/7590.pdf> (accessed 17.06.11)

Cabinet Office. 'Responding to Emergencies, The UK Central Government Response, Concept of Operations'. 23 April 2013. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/192425/CONOPs\\_incl\\_revised\\_chapter\\_24\\_Apr-13.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192425/CONOPs_incl_revised_chapter_24_Apr-13.pdf) (accessed 30.07.13)

Cabinet Office. 'Security in a Global Hub: Establishing the UK's new border arrangements'. Ref: 284440/1107. November 2007. Via: [http://webarchive.nationalarchives.gov.uk/20071204130052/http://cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/publications/reports/border\\_review.pdf](http://webarchive.nationalarchives.gov.uk/20071204130052/http://cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/publications/reports/border_review.pdf) (accessed 24.01.14)

Cabinet Office. 'Strategic National Framework on Community Resilience'. March 2011. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/60922/Sstrategic-National-Framework-on-Community-Resilience\\_0.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60922/Sstrategic-National-Framework-on-Community-Resilience_0.pdf) (accessed 31.07.13)

Cabinet Office. 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world'. November 2011. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/60961/uk-cyber-security-strategy-final.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf) (accessed 15.01.12)

DCLG. 'FiReControl – An Overview'. 20 May 2009. Via: <http://webarchive.nationalarchives.gov.uk/20120919132719/http://www.communities.gov.uk/documents/fire/pdf/firecontroloverview.pdf> (accessed 08.08.13)

DCLG. 'FiReControl Business Case: Version 1.1'. May 2009. Via: <http://webarchive.nationalarchives.gov.uk/20120919132719/http://www.communities.gov.uk/documents/fire/pdf/1207425.pdf> (accessed 09.08.13)

DCMS. 'London 2012 Olympic Games and Paralympic Games Annual Report'. January 2008. Via: <http://webarchive.nationalarchives.gov.uk/+http://www.culture.gov.uk/images/publications/dcmsgoeannualreportjan08vs3update.pdf> (accessed 24.04.12)

DCMS. 'London 2012 Olympic and Paralympic Games - Quarterly Report'. December 2011. Via: [http://www.culture.gov.uk/images/publications/DCMS\\_GOE\\_QR\\_Dec\\_2011.pdf](http://www.culture.gov.uk/images/publications/DCMS_GOE_QR_Dec_2011.pdf) (accessed 11.01.12)

DCMS. 'London 2012 Olympic and Paralympic Games - Quarterly Report'. June 2012. Via: [http://www.culture.gov.uk/images/publications/DCMS\\_GOE\\_QR\\_JUNE-2012.pdf](http://www.culture.gov.uk/images/publications/DCMS_GOE_QR_JUNE-2012.pdf) (Accessed 03.09.12)

DCMS. 'London 2012 Olympic and Paralympic Games - Quarterly Report'. October 2012. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/78251/DCMS\\_GOE\\_Quarterly\\_Report\\_Q3.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78251/DCMS_GOE_Quarterly_Report_Q3.pdf) (accessed 11.08.14)

European Commission. Communication from the Commission to the European Parliament, The Council and the European Economic and Social Committee, Policy . 'Action Plan for an innovative and competitive Security Industry'. Brussels. 26 July 2012. COM(2012) 417 final. Via: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF> (accessed 03.05.14)

European Commission. 'Study on the industrial implications in Europe of the blurring of dividing lines between Security and Defence - Final Report'. 2010. Via: [http://ec.europa.eu/enterprise/sectors/defence/files/new\\_defsec\\_final\\_report\\_en.pdf](http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf) (accessed 24.02.12)

Greater London Authority. 'London Events Coordination Calendar – Delivery Support'. Via: <http://www.london.gov.uk/sites/default/files/ODD24%20LECC%20Project%20Support%20PDF.pdf> (accessed 30.12.14)

HM Government. 'A Strong Britain in an Age of Uncertainty: The National Security Strategy'. London: The Stationary Office, 2010. Via: <http://www.cabinetoffice.gov.uk/resource-library/national-security-strategy-strong-britain-age-uncertainty> (accessed 30.06.11)

HM Government. 'CONTEST: The United Kingdom's Strategy for Countering Terrorism.' Cm8123. London: TSO, 2011. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/97995/strategy-contest.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf) (accessed 19.07.13)

HM Government. 'CONTEST: The United Kingdom's Strategy for Countering Terrorism - Annual Report'. Cm 8583. March 2013. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/170644/28307\\_Cm\\_8583\\_v0\\_20.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170644/28307_Cm_8583_v0_20.pdf) (accessed 16.11.13)

HM Government. 'Controlling our borders: Making migration work for Britain'. Five year strategy for asylum and immigration. Cm 6472. February 2005. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/251091/6472.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251091/6472.pdf) (last accessed 29.12.14)

HM Government. 'Countering International Terrorism: The United Kingdom's Strategy.' Cm6888. London: TSO, 2006. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/272320/6888.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/272320/6888.pdf) (last accessed 02.01.15)

HM Government. 'Defence Technology Strategy for the Demands of the 21st Century'. London: The Stationary Office, 2006. Via: [http://webarchive.nationalarchives.gov.uk/20121026065214/http://www.mod.uk/NR/rdo\\_nlyres/27787990-42BD-4883-95C0-B48BB72BC982/0/dts\\_complete.pdf](http://webarchive.nationalarchives.gov.uk/20121026065214/http://www.mod.uk/NR/rdo_nlyres/27787990-42BD-4883-95C0-B48BB72BC982/0/dts_complete.pdf) (accessed 24.06.11)

HM Government. 'Equipment, Support and Technology for UK Defence and Security: A Consultation Paper'. London: The Stationary Office, 2010. Via: <http://defenceconsultations.org.uk/Cm7989.pdf> (accessed 25.06.11)

HM Government. 'Ideas and Innovation: How industry and academia can play their part'. August 2009. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/97947/ideas-and-innovations.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97947/ideas-and-innovations.pdf) (last accessed 30.12.14)

HM Government. 'Pursue Prevent Protect Prepare: The United Kingdom's Strategy for Countering International Terrorism.' Cm7547. London: TSO, 2009. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228644/7547.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228644/7547.pdf) (last accessed 02.01.15)

HM Government. 'Securing Britain in an Age of Austerity: The Strategic Defence and Security Review' (London: The Stationary Office, 2010. Via: [http://webarchive.nationalarchives.gov.uk/20121015000000/http://www.direct.gov.uk/pr\\_od\\_consum\\_dg/groups/dg\\_digitalassets/@dg/@en/documents/digitalasset/dg\\_191634.pdf](http://webarchive.nationalarchives.gov.uk/20121015000000/http://www.direct.gov.uk/pr_od_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf) (accessed 16.10.12)

HM Treasury. 'Pre-Budget Report 2004 - Opportunity for all: The strength to take the long-term decisions for Britain'. Cm 6408. 2 December 2004. Via: [http://webarchive.nationalarchives.gov.uk/20100407164511/http://www.hm-treasury.gov.uk/d/pbr04\\_chap06\\_256.pdf](http://webarchive.nationalarchives.gov.uk/20100407164511/http://www.hm-treasury.gov.uk/d/pbr04_chap06_256.pdf) (accessed 05.02.14)

Home Office. 'Audit & Review of Olympic & Paralympic Safety & Security Planning: Summary'. November 2010. Via: <http://www.homeoffice.gov.uk/publications/counter-terrorism/olympics/audit-olympic-security-nov10> (accessed 07.05.12)

Home Office. 'Business as Usual: Maximising business resilience to terrorist bombings, A Handbook for Managers.' Home Office Communications Directorate. February 1999. Via: <http://www.nationalarchives.gov.uk/ERORecords/HO/421/2/P2/oicd/business.pdf> (accessed 01.08.13)

Home Office. 'How Resilient is your Business to Disaster'. Home Office Communications Directorate. 1998. Via: <http://www.nationalarchives.gov.uk/ERORecords/HO/421/2/P2/EPD/hrib.txt> (accessed 01.08.13)

Home Office. 'Fair, effective, transparent and trusted: Rebuilding confidence in our immigration system'. Ref: 275921. July 2006. Via: <http://webarchive.nationalarchives.gov.uk/20080806121433/http://www.ukba.homeoffice>.

[gov.uk/sitecontent/documents/aboutus/reports/indreview/indreview.pdf?view=Binary](http://www.gov.uk/sitecontent/documents/aboutus/reports/indreview/indreview.pdf?view=Binary)  
(accessed 22.01.14)

Home Office. 'Government response to the seventh report from the Home Affairs Select Committee'. Session 2012-13. HC531. Olympics Security. November 2012. Cm 8500. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/235984/8500.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/235984/8500.pdf) (accessed 12.08.14)

Home Office. 'Have you got what it takes? The Police ICT Company'. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/117420/police-ict-company.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/117420/police-ict-company.pdf) (accessed 24.04.14)

Home Office. 'London 2012 Olympic and Paralympic Safety and Security Strategy'. London: The Stationary Office, 2009. Via: <http://webarchive.nationalarchives.gov.uk/20100407094535/http://security.homeoffice.gov.uk/news-publications/publication-search/olympic-security/olympic-strategy.html> (accessed 08.01.12)

Home Office. 'Securing the UK Border: Our vision and strategy for the future'. Ref. 280648. March 2007, Via: [http://dematerialisedid.com/pdfs/Securing\\_the\\_UK\\_Border\\_final.pdf](http://dematerialisedid.com/pdfs/Securing_the_UK_Border_final.pdf) (accessed 04.12.14)

Home Office. Border & Immigration Agency. 'e-Borders – Full Business Case, V1.0'. 12 November 2007. Via: [http://data.parliament.uk/DepositedPapers/Files/DEP2013-1847/20071112\\_FBC\\_v1\\_0\\_doc1\\_agreed\\_redactions.docx](http://data.parliament.uk/DepositedPapers/Files/DEP2013-1847/20071112_FBC_v1_0_doc1_agreed_redactions.docx) (accessed 04.02.14)

Home Office. Border & Immigration Agency. 'e-Borders – Full Business Case – Appendices, V1.0'. 12 November 2007. Via: <http://www.parliament.uk/business/publications/business-papers/commons/deposited-papers/?page=8&y=2012&fd=2012-09-30&td=2012-12-01&house=1#toggle-1847> (accessed 04.02.14)

Home Office. UK Border Agency. 'UK Border Agency Business Plan: April 2011-March 2015'. 13 May 2011. Via: <http://webarchive.nationalarchives.gov.uk/20140110181512/http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/uk-border-agency-business-plan/business-plan/ukba-business-plan?view=Binary> (last accessed 29.12.14)

London Fire and Emergency Planning Authority. 'Budget 2008/09'. FEP1195. March 2008. Via: <http://www.london-fire.gov.uk/Documents/FEP1195.pdf> (accessed 04.08.13)

London Fire and Emergency Planning Authority. 'Budget 2009/10'. FEP 1321. March 2009. Via: <http://www.london-fire.gov.uk/Documents/FEP1321.pdf> (accessed 04.08.13)

Ministry of Defence. 'The Defence Equipment Plan 2012'. [www.gov.uk](http://www.gov.uk). 31 January 2013. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/70258/Defence\\_Equipment\\_Plan\\_2012\\_20130130.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/70258/Defence_Equipment_Plan_2012_20130130.pdf) (accessed 05.02.13)

Ministry of Defence. 'National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security'. Cm8278. February 2012. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/27390/cm8278.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27390/cm8278.pdf) (accessed 01.15.13)

Office of the Deputy Prime Minister. 'Our Fire and Rescue Service'. Cm 5808. London: HMSO, 2003.

UKTI. 'Cyber Security: The UK's approach to exports'. April 2013. URN 13/720. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/275566/UKTI\\_Cyber\\_Security\\_Brochure.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf) (accessed 30.04.14)

UKTI. 'Increasing our Security Exports: A new government approach'. February 2014. Via: <https://www.gov.uk/government/publications/increasing-our-security-exports-a-new-government-approach> (accessed 02.05.14)

UKTI. 'UK Trade & Investment Defence & Security Organisation: Helping UK companies to export'. April 2009. Via: [http://webarchive.nationalarchives.gov.uk/20100222170314/http://dso.uktradeinvest.gov.uk/docs/UKTI\\_DSO\\_Brochure\\_Apr\\_09.pdf](http://webarchive.nationalarchives.gov.uk/20100222170314/http://dso.uktradeinvest.gov.uk/docs/UKTI_DSO_Brochure_Apr_09.pdf) (accessed 02.05.14)

UKTI DSO. 'Contact Directory 2014'. July 2014. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/328090/UKTI\\_DSO\\_Contacts\\_Directory\\_July\\_2014.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/328090/UKTI_DSO_Contacts_Directory_July_2014.pdf) (accessed 30.12.14)

### Government speeches

Brokenshire, James. 'Securing Asia 2013: James Brokenshire's Special Address'. 25 June 2013. Via: <https://www.gov.uk/government/speeches/using-international-partnerships-to-tackle-the-threat-of-global-terrorism> (accessed 12.05.14)

Cameron, David. '2012 New Year's Message'. Via: <https://www.gov.uk/government/speeches/2012-new-year-message-from-david-cameron> (accessed 08.01.12)

Evans, Jonathan. 'The Olympics and Beyond'. Lord Mayor's Annual Defence and Security Lecture. 25 June 2012. Via: <https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html> (accessed 27.08.12)

Green, Damian. 'Keynote Speech: Damian Green MP'. Speech delivered to Royal United Services Institute, London. 14 March 2012. Via: [http://www.rusi.org/events/ref:E4EE5DAE74B90C/info:public/infoID:E4F60AD5049495/#.UvDfEfl\\_vD8](http://www.rusi.org/events/ref:E4EE5DAE74B90C/info:public/infoID:E4F60AD5049495/#.UvDfEfl_vD8) (accessed 14.02.14)

Hague, William. 'Britain's Foreign Policy in a Networked World'. Speech delivered at the Foreign and Commonwealth Office. 1 July 2010. Via: <http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=22462590> (accessed 24.06.11)



May, Theresa. 'Olympic Security Conference Speech'. Speech delivered to Royal United Services Institute 21 November 2011. Via: <https://www.gov.uk/government/speeches/home-secretarys-olympic-security-conference-speech> (accessed 15.01.12)

Neville-Jones, Pauline. 'Speech at Farnborough Airshow Security Day Conference'. 22 July 2010. Via: <http://www.homeoffice.gov.uk/media-centre/speeches/neville-jones-security-day> (accessed 24.06.11)

Omand, David. 'National Resilience Priorities for UK Government'. Speech given at RUSI at the launch of the Homeland Security and Resilience Department. 1 July 2004. Via: <http://www.rusi.org/analysis/commentary/ref:C40AB913E66BA2/> (accessed 19.07.13)

Raine, Robert. 'Working with the private sector to deliver a safe and secure Olympic Games'. 7 September 2010. Speech to Police Foundation annual conference (2009). Via: <https://www.youtube.com/watch?v=azR3h9ugcfQ&feature=channel&list=UL> (last accessed 29.12.14)

Reid, John. 'Speech on anti-terrorism measures'. 31 October 2006. Via: <http://www.itnsource.com/shotlist/ITN/2006/10/31/R31100601/?v=1> (accessed 08.04.14)

Reid, John. 'Speech to RUSI Launching RISC'. 29 March 2007. Via: [www.riscuk.org](http://www.riscuk.org) (accessed 20.12.11)

#### Government press releases and statements

DCLG. 'Fire Minister Bob Neill calls time on FiReControl'. Gov.uk. 20 December 2010. Via: <https://www.gov.uk/government/news/fire-minister-bob-neill-calls-time-on-firecontrol> (accessed 08.08.13)

DCMS. 'First 2012 Cabinet meets at Olympic Park'. 9 January 2012. Via: [http://www.culture.gov.uk/news/news\\_stories/8758.aspx](http://www.culture.gov.uk/news/news_stories/8758.aspx) (accessed 14.01.12)

DCMS. 'Jeremy Hunt statement on Olympic security'. 24 July 2012. Via: <http://goc2012.culture.gov.uk/2012/07/jeremy-hunt-statement-on-olympic-security/> (accessed 26.08.12)

Green, Damian. 'e-Borders Programme'. Written Ministerial Statement. 22 July 2010. Via: <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100722/wmstext/100722m0001.htm#10072238000035> (accessed 14.02.14)

Home Office. 'Allocation of grants to police authorities in England and Wales'. 13 December 2010. Via: <http://www.homeoffice.gov.uk/publications/about-us/parliamentary-business/written-ministerial-statement/allocations-police-england-wales?view=Binary> (accessed 23.04.12)

Home Office. 'Home Secretary statement on Olympic Security'. 12 July 2012. Via: <http://www.homeoffice.gov.uk/media-centre/news/theresa-may-olympic-security> (accessed 26.08.12)

Home Office. 'E-borders contract terminated'. Home Office Press Release. 22 July 2010. Via: <https://www.gov.uk/government/news/e-borders-contract-terminated> (accessed 11.02.14)

Home Office. 'Government ramps up passenger screening'. Home Office Press Release. 12 March 2010. Via: <http://tna.europarchive.org/20100419081706/press.homeoffice.gov.uk/press-releases/government-passenger-screening.html> (accessed 04.02.14)

Home Office. 'Home Secretary letter on the e-Borders programme arbitration'. 18 August 2014. Via: <https://www.gov.uk/government/news/home-secretary-letter-on-the-e-borders-programme-arbitration> (accessed 18.08.14)

Ministry of Defence. 'Bernard Gray appointed Chief of Defence Materiel'. 16 December 2010. Via: <http://www.mod.uk/DefenceInternet/DefenceNews/DefencePolicyAndBusiness/BernardGrayAppointedChiefOfDefenceMateriel.htm> (accessed 16.08.12)

Ministry of Defence. 'Military support to 2012 Olympic Games announced'. 15 December 2011. Via: <http://www.mod.uk/DefenceInternet/DefenceNews/MilitaryOperations/MilitarySupportTo2012OlympicGamesAnnounced.htm> (accessed 08.01.12)

Scholefield, Susan. Letter from the Head of the CCS. 19 June 2003. Via: <http://webarchive.nationalarchives.gov.uk/20050523205851/http://ukresilience.info/contingencies/dwd/scholefield.pdf> (accessed 30.07.13)

#### Government internet webpages

Cabinet Office. 'The central government's concept of operations'. Via: <https://www.gov.uk/government/publications/the-central-government-s-concept-of-operations> (accessed 30.07.13)

Cabinet Office. 'Improving the UK's ability to absorb, respond to, and recover from emergencies'. Gov.uk. Via: <https://www.gov.uk/government/policies/improving-the-uks-ability-to-absorb-respond-to-and-recover-from-emergencies> (accessed 19.07.13)

Cabinet Office. 'Preparation and planning for emergencies: the National Resilience Capabilities Programme'. Via: <https://www.gov.uk/preparation-and-planning-for-emergencies-the-capabilities-programme> (accessed 30.07.13)

Cabinet Office. 'Resilience in society: infrastructure, communities and businesses'. Via: <https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses> (accessed 30.07.13)

Cabinet Office. 'Sector resilience plans'. Via: <https://www.gov.uk/government/publications/sector-resilience-plans> (accessed 30.07.13)

CPNI. 'Information Exchanges'. CPNI Website. Via: <http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/> (accessed 01.11.13)

CPNI. 'The national infrastructure'. CPNI Website. Via: <http://www.cpni.gov.uk/about/cni/> (accessed 01.11.13)

Department for Transport. 'List of Approved Security Providers'. DfT Website. Via: <https://www.gov.uk/government/publications/list-of-approved-security-providers> (accessed 15.01.12)

Emergency Planning College. 'Gold Standard'. EPC Website. Via: <http://epcollege.com/epc/training/goldstandard/> (accessed 19.01.12)

Emergency Planning College. 'About Us'. EPC Website, Via: <http://www.epcollege.com/epc/about-us/> (accessed 30.07.13)

Home Office. 'Counter-terrorism strategy (CONTEST)', Home Office Website. July 2011. Via: <https://www.gov.uk/government/publications/counter-terrorism-strategy-contest> (accessed 14.11.14)

Home Office. 'Our Organisation'. UK Border Agency Website. Via: <http://www.bia.homeoffice.gov.uk/aboutus/organisation/> (accessed 24.01.14)

Home Office. 'Science and Technology'. Home Office Website. Via: <http://www.homeoffice.gov.uk/counterterrorism/science-and-technology/> (accessed 15.01.12)

Home Office. 'Transparency Spend over £25,000'. June 2010. Home Office Website. Via: <https://www.gov.uk/government/publications/transparency-spend-over-25-000> (accessed 15.01.12)

London Fire Brigade. 'Resilience'. Via: <http://www.london-fire.gov.uk/Resilience.asp> (accessed 04.08.13)

Metropolitan Police Service. 'Met Command and Control'. MPS Website. Via: <http://content.met.police.uk/Article/Met-Command-and-Control/1400005435512/1400005435512> (accessed 20.01.12)

Ministry of Defence. 'Standing Commitments'. Gov.uk. 12 December 2012. Via: <https://www.gov.uk/standing-commitments> (accessed 05.02.13)

NaCTSO. 'Publications'. NaCTSO Website. Via: <http://www.nactso.gov.uk/publications> (accessed 15.11.13)

Scottish Enterprise. 'Security and resilience industry in Scotland'. Via: <http://www.scottish-enterprise.com/your-sector/aerospace-defence-and-marine/adm-strategy/adm-facts/security-facts.aspx> (accessed 06.08.13)

Security Service. 'International Terrorism'. Security Service Website. Via: <https://www.mi5.gov.uk/output/international-terrorism.html> (accessed 24.02.12)

Security Service. 'What are threat levels?' Security Service Website. Via:  
<https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels/the-uks-threat-level-system/what-are-threat-levels.html> (accessed 03.09.12)

UKTI. 'About the UKTI Defence & Security Organisation'. 2 December 2009. Via:  
<http://webarchive.nationalarchives.gov.uk/20100222170314/http://dso.uktradeinvest.gov.uk/about.htm> (accessed 30.04.14)

### **Parliamentary Proceedings**

All Party Parliamentary Group on Specialist Security. 'VIP Security at the London 2012 Olympic & Paralympic Games'. First Report of Session 2011-12. 11 July 2012. Via:  
<http://appgsecurity.com/downloads/VIPSecurityAtLondon2012OlympicGames.pdf>  
(accessed 02.09.12)

Brooke-Holland, Louisa. 'In brief: Outsourcing defence procurement'. Standard Note: SN06633. 10 May 2013. Via: <http://www.parliament.uk/briefing-papers/SN06633.pdf>  
(accessed 24.04.14)

European Parliament, Committee on Transport and Tourism. 'Working Document on aviation security charges'. DT\793269EN.doc. 20 October 2009. Via:  
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-430.335%2B01%2BDOC%2BPDF%2BV0%2F%2FEN> (accessed 26.02.14)

Grimwood, Gabrielle. 'E-borders and Operation Semaphore'. Standard Note: SN/HA/3960. 7 November 2008. Via: <http://www.parliament.uk/briefing-papers/SN03980/eBorders-and-operation- semaphore> (accessed 14.02.14)

Hansard. Douglas Alexander, Parliamentary Question Reply. 21 March 2003: Column 958W. Via:  
[http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030321/text/30321w01.htm#30321w01.html\\_wqn7](http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030321/text/30321w01.htm#30321w01.html_wqn7) (accessed 02.08.13)

Hansard. Damian Green, Parliamentary Question Reply: 15 Sep 2010: Column 1073W. Via:  
<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100915/text/100915w0002.htm#10091521000116> (accessed 05.02.14)

Hansard. Damian Green, Parliamentary Question Reply: 15 Sep 2010: Column 1074W. Via:  
<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100915/text/100915w0002.htm#10091521000116> (accessed 05.02.14)

Hansard. Francis Maude, Parliamentary Question Reply. 10 Nov 2011: Column 452W. Via:  
<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm111110/text/111110w0003.htm#11111097001723> (accessed 01.08.13)

Hansard. 'Machinery of Government: Defence Trade Promotion'. Written Ministerial Statement. 25 July 2007. Via:

<http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070725/wmstext/70725m0005.htm#07072565000047> (accessed 30.04.14)

House of Commons, Committee of Public Accounts. 'The Border Force: securing the border'. Thirty-first Report of Session 2013-14. HC 663. 2 December 2013. Via: <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/663/663.pdf> (accessed 29.12.14)

House of Commons, Committee of Public Accounts. 'The failure of the FiReControl project'. Fiftieth Report of Session 2010-12. HC 1397. September 2011. Via: <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1397/1397.pdf> (last accessed 29.12.14)

House of Commons, Committee of Public Accounts. 'FiReControl: Update report', Sixteenth Report of Session 2013-14. HC 110. July 2013. Via: <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/110/110.pdf> (last accessed 29.12.14)

House of Commons, Committee of Public Accounts. 'Police Procurement'. Twenty-first Report of Session 2013-14. 17 July 2013. Via: <http://webcache.googleusercontent.com/search?q=cache:http://www.publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/115/115.pdf> (accessed 23.04.14)

House of Commons, Committee of Public Accounts. 'Preparations for the London 2012 Olympic Games and Paralympic Games'. Seventy-fourth Report of Session 2010-12. 29 February 2012. Via: <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1716/1716.pdf> (accessed 24.04.12)

House of Commons, Committee of Public Accounts. 'Uncorrected transcript of oral evidence taken before the Public Accounts Committee on Managing Preparations for the Olympics'. 14 December 2011. Via: <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/uc1716-i/uc171601.htm> (accessed 11.01.12)

House of Commons, Communities and Local Government Committee. 'Fire and Rescue Service'. Fourth Report of Session 2005-06. Volume I. HC 872-1. July 2006. Via: <http://www.publications.parliament.uk/pa/cm200506/cmselect/cmcomloc/872/872i.pdf> (last accessed 29.12.14)

House of Commons, Communities and Local Government Committee. 'Fire and Rescue Service'. Fourth Report of Session 2005-06. Volume II. HC 872-II. March 2006. Via: <http://www.publications.parliament.uk/pa/cm200506/cmselect/cmcomloc/872/872ii.pdf> (last accessed 29.12.14)

House of Commons, Communities and Local Government Committee. 'FiReControl'. Fifth Report of Session 2009-10. HC 352. April 2010. Via:

<http://www.publications.parliament.uk/pa/cm200910/cmselect/cmcomloc/352/352.pdf>

(last accessed 29.12.14)

House of Commons, Defence Select Committee. 'Defence Acquisition'. Seventh Report of Session 2012–13. 5 February 2013. Via:

<http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/9/9.pdf>

(accessed 08.02.13)

House of Commons, Home Affairs Select Committee. 'Border Controls: Report and Proceedings of the Committee'. First Report from the Home Affairs Committee. Session 2000-01. HC 163-I. Via:

<http://www.publications.parliament.uk/pa/cm200001/cmselect/cmhaff/163/16311.htm#a14> (accessed 10.02.14)

House of Commons, Home Affairs Select Committee. 'Border Controls: Minutes of Evidence and Appendices'. HC 163-II. Annex 7. Via:

<http://www.publications.parliament.uk/pa/cm200001/cmselect/cmhaff/163/163ap06.htm>

(accessed 05.02.14)

House of Commons, Home Affairs Select Committee. 'Border Controls'. Fourth Special Report. Government Reply to the First Report from the Home Affairs Committee. Session 2000-01. HC 375. Via:

<http://www.publications.parliament.uk/pa/cm200001/cmselect/cmhaff/375/37502.htm>

(accessed 10.02.14)

House of Commons, Home Affairs Select Committee. 'The E-Borders Programme'. Third Report of Session 2009-10. HC 170. 15 December 2009. Via:

<http://www.publications.parliament.uk/pa/cm200910/cmselect/cmhaff/170/170.pdf>

(accessed 10.04.14)

House of Commons, Home Affairs Committee. 'The New Landscape of Policing'. Fourteenth Report of Session 2010-12. 15 September 2011. Via:

<http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/939/939.pdf>

(accessed 24.04.13)

House of Commons, Home Affairs Select Committee. 'Olympics Security'. Seventh Report of Session 2012–13. 21 September 2012. Via:

<http://www.publications.parliament.uk/pa/cm201213/cmselect/cmhaff/531/531.pdf>

(accessed 21.09.12)

House of Commons, Home Affairs Select Committee. 'Project CONTEST: The Government's Counter-Terrorism Strategy'. Ninth Report of Session 2008-2009. June 2009. Via:

<http://www.publications.parliament.uk/pa/cm200809/cmselect/cmhaff/212/212.pdf>

(accessed 23.04.12)

House of Commons, Home Affairs Select Committee. 'Supplementary memorandum submitted by the Permanent Secretary, Home Office'. December 2010. Via:

<http://www.publications.parliament.uk/pa/cm201011/cmselect/cmhaff/626/626we06.htm> (accessed 15.01.12)

House of Commons, Home Affairs Select Committee. 'Uncorrected Transcript of Oral Evidence, Olympic Security Inquiry Session 2012-13'. 11 September 2012. Via: <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmhaff/uc531-iii/uc53101.htm> (accessed 24.09.12).

House of Commons, Home Affairs Select Committee. 'Uncorrected Transcript of Oral Evidence, Olympic Security Inquiry Session 2012-13'. 17 July 2012. Via: <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmhaff/uc531-i/uc53101.htm> (accessed 06.09.12)

House of Commons, Home Affairs Select Committee. 'The work of the Permanent Secretary'. Thirteenth Report of Session 2013-14. HC 233. Via: <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/233/233.pdf> (accessed 05.02.14)

House of Commons, Transport Committee. 'Transport Security: Travelling without Fear'. Oral and written evidence. HC 191. 12 December 2007. Via: <http://www.publications.parliament.uk/pa/cm200708/cmselect/cmtran/191/191.pdf> (accessed 26.02.14 )

Intelligence and Security Committee. 'Annual Report 2010-2011'. July 2011. cm8114. Via: <http://isc.independent.gov.uk/committee-reports/annual-reports> (accessed 15.11.14)

## **Government Oversight Reports**

### *NAO Reports*

National Audit Office. 'FiReControl Project'. Memorandum for the House of Commons Communities and Local Government Select Committee. February 2010. Via: [http://www.nao.org.uk/wp-content/uploads/2010/02/0910\\_CLG\\_FiReControl.pdf](http://www.nao.org.uk/wp-content/uploads/2010/02/0910_CLG_FiReControl.pdf) (last accessed 29.12.14)

National Audit Office. 'The failure of the FiReControl project'. Report by the Comptroller and Auditor General. HC 1272. Session 2010-2012. 1 July 2011. Via: <http://www.nao.org.uk/wp-content/uploads/2011/07/10121272.pdf> (last accessed 29.12.14)

National Audit Office. 'Preparations for the London 2012 Olympic and Paralympic Games - Risk assessment and management'. 2 February 2007. Via: [http://www.nao.org.uk/publications/0607/preparations\\_for\\_the\\_olympics.aspx](http://www.nao.org.uk/publications/0607/preparations_for_the_olympics.aspx) (accessed 24.04.12)

National Audit Office. 'New Dimension - Enhancing the Fire and Rescue Services' capacity to respond to terrorist and other large-scale incidents'. Report by the Comptroller and Auditor General, HC 1050, Session 2007-2008. 31 October 2008. Via: <https://www.nao.org.uk/wp-content/uploads/2008/10/07081050.pdf> (accessed 19.12.14)

National Audit Office. 'Returning failed asylum applicants'. Report by the Comptroller and Auditor General. HC 76. Session 2005-2006. 14 July 2005. Via: <http://www.nao.org.uk/wp-content/uploads/2005/07/050676.pdf> (accessed 04.02.14)

National Audit Office. 'The UK Border Agency and Border Force: Progress in cutting costs and improving performance'. Report by the Comptroller and Auditor General. HC 467. Session 2012-13. 17 July 2012. Via: <http://www.nao.org.uk/wp-content/uploads/2012/07/1213467es.pdf> (accessed 04.02.14)

### Other Reports

Advisory Committee on Business Appointments. 'Appointments taken up by former Crown servants'. Via: [http://acoba.independent.gov.uk/former\\_crown\\_servants/former\\_crown\\_servants\\_appointments\\_2012.aspx](http://acoba.independent.gov.uk/former_crown_servants/former_crown_servants_appointments_2012.aspx) (accessed 28.03.14)

Advisory Committee on Business Appointments, 'Eighth Report 2005-2006'. Via: [http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/acoba/assets/acobaeighthreport2005\\_06.pdf](http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/acoba/assets/acobaeighthreport2005_06.pdf) (accessed 28.03.14)

Advisory Committee on Business Appointments. 'Eleventh Report 2009-2010'. Via: <http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/20565/acobaeleventhreport2009-2010.pdf> (accessed 28.03.14)

Advisory Committee on Business Appointments. 'Twelfth Annual Report 2010-2011'. Via: <http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/acoba/assets/acobatwelfthreport2010-2011.pdf> (accessed 28.03.14)

Advisory Committee on Business Appointments. 'Thirteenth Annual Report 2011-2012'. Via: <http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/26724/acoba%20thirteenth%20annual%20report%202011-12.pdf> (accessed 28.03.14)

Advisory Committee on Business Appointments. 'Fourteenth Report 2012-2013'. Via: <http://webarchive.nationalarchives.gov.uk/20140404084345/http://acoba.independent.gov.uk/media/29744/acoba%2012-13%20annual%20report.pdf> (accessed 28.03.14)

Anderson, David. 'The Terrorism Acts in 2011: Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006'. June 2012: Via: <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2013/04/report-terrorism-acts-2011.pdf> (accessed 01.01.15)

Anderson, David. 'The Terrorism Acts in 2012: Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006'. July 2013. Via: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/243472/9780108512629.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/243472/9780108512629.pdf) (accessed 10.11.14)



Vine, John. “‘Exporting the border’”? An inspection of e-Borders: October 2012 – March 2013’. Ref. HO\_02088\_ICI. 9 October 2013. Via: <http://icinspector.independent.gov.uk/wp-content/uploads/2013/10/An-Inspection-of-eborders.pdf> (last accessed 29.12.14)

### **Industry Documentation / Material**

4Global. ‘Testimonials’. Via: <http://www.fourglobal.org/experience/testimonials.aspx> (accessed 31.08.14)

ADS Group. ‘Security Policy’. ADS Group Website. Via: <https://www.adsgroup.org.uk/pages/58346194.asp> (accessed 02.15.14)

ADS Group. ‘UK Security Survey 2011’. London: ADS Group, 2011. Via: <http://www.adsgroup.org.uk/articles/26154> (accessed 17.08.12)

ADS Group. ‘UKTI DSO: UK Defence and Security Exports 2011 – UK Maintains Position as Second Most Successful Defence Exporter’. ADS News (01.05.12). Via: <http://www.adsgroup.org.uk/articles/29509> (accessed 05.02.13)

Airwave. ‘London 2012’s Critical Communications Ready for Service’. 8 July 2011. Airwave Solutions Website. Via: <https://www.airwavesolutions.co.uk/media/news/article/london-2012s-critical-communications-ready-for-service/> (accessed 15.01.12)

Airwave. ‘The Airwave Service’, Airwave Solutions Website. Via: <https://www.airwavesolutions.co.uk/about/the-service/> (accessed 30.12.14)

Beesley, Amanda. ‘The BSIA Briefing: June 2012’. ifsecglobal.com. June 2012. Via: <http://www.ifsecglobal.com/the-bsia-briefing-june-2012/> (accessed 30.12.14)

Bridging the Gap. ‘Stakeholders’. BtG Website. Via: <http://www.bridging-the-gap.co.uk/Stakeholders.aspx> (accessed 19.01.12)

BSIA. ‘New co-ordination unit matches VIPs with reputable Close Protection suppliers’. BSIA Website. 3 July 2012. Via: [http://www.bsia.co.uk/M01W4033507/LY8WLW49550/new-Close-Protection\\_co-ordination-unit?backlinktype=newscentre&src=in\\_t](http://www.bsia.co.uk/M01W4033507/LY8WLW49550/new-Close-Protection_co-ordination-unit?backlinktype=newscentre&src=in_t) (accessed 30.12.14)

BSIA. ‘Cross-sector Safety and Security Communications’. BSIA Website. Via: <http://www.bsia.co.uk/CSSC> (accessed 06.09.12)

BSIA. ‘Publications’. Via: <http://www.bsia.co.uk/publications.php?r=NQ4W5W616041> (accessed 15.11.13)

Buro Happold. ‘SEA Article’. Buro Happold Website. Via: <http://www.happoldsafesecure.com/CompanyAwards.aspx> (accessed 15.01.12)

Crofts, Tim. ‘RISC Chairman’s Speech’. Launch of the UK’s Security Exports Strategy. 27 February 2014. Via: [https://www.adsgroup.org.uk/pages/42220705.asp#aGroup\\_1](https://www.adsgroup.org.uk/pages/42220705.asp#aGroup_1) (accessed 02.05.14)

Deloitte. 'The State of Play: our journey to London 2012 and beyond'. Issue 1, 2009. Via: <http://www.deloittelondon2012.co.uk/london-2012/the-state-of-play/issue-1-our-journey-to-london-2012-and-beyond> (accessed 12.01.12)

Delorge, Robert. Letter from Robert M Delorge to Rt Hon Keith Vaz MP. 3 August 2011. Via: <http://www.parliament.uk/documents/commons-committees/home-affairs/110815-hac-corr.pdf> (last accessed 29.12.14)

FE Investigate. 'Serco Group PLC Contract Award'. 12 Oct. 2005. Via: <http://www.investigate.co.uk/article.aspx?id=20051012092509PCC89> (accessed 30.12.14)

G4S. 'G4S plc Annual Report and Accounts 2012'. Via: [http://www.g4s.com/~media/Files/Annual%20Reports/g4s\\_annual\\_report\\_2012.ashx](http://www.g4s.com/~media/Files/Annual%20Reports/g4s_annual_report_2012.ashx) (accessed 11.08.14)

G4S. 'Half yearly results announcement for the six months ended 30 June 2012'. 28 August 2012. Via: <http://www.g4s.com/~media/Files/Investor%20Relations%20documents/Results%20Announcements/2012%20interims%20announcement%20combined%20Final.ashx> (accessed 29.08.12)

G4S. 'G4S H1 2012 results'. 28 August 2012. Via: <http://www.g4s.com/en/Investors/News%20and%20Presentations/Regulatory%20Announcements/2012/08/28/G4S%20H1%202012%20results/> (accessed 29.08.12)

G4S. 'Statement regarding the Olympic Games Security Contract'. 13 July 2012. Via: <http://www.g4s.com/en/Investors/News%20and%20Presentations/Regulatory%20Announcements/2012/07/13/Olympic%20Games%20Security%20Contract/> (accessed 27.08.12)

G4S. 'G4S – Delivering the Games', G4S Corporate Video. 21 October 2011. Via: <http://www.youtube.com/watch?NR=1&v=6sgDdPDLOTQ&feature=endscreen> (accessed 11.01.12)

Mott MacDonald. 'The Future of Fire and Rescue Service Control Rooms in England and Wales Update 2003 – Full Report'. Via: [http://www.esfrs.org/document/pdf/fa/membersArea/mott\\_mac\\_report.pdf](http://www.esfrs.org/document/pdf/fa/membersArea/mott_mac_report.pdf) (accessed 12.08.13)

NMI. 'NMI appoints Neul CEO Stan Boland as chairman'. NMI Website. Via: <http://archive.nmi.org.uk/news/press-releases/nmi-stan-boland> (accessed 30.12.14)

Northrop Grumman. 'Northrop Grumman Appoints Graham Wright and Kathy Salyan to Key Cyber Security and Intelligence-Related Roles in the UK'. Northrop Grumman News Release. 4 January 2011. Via: [http://www.irconnect.com/noc/press/pages/news\\_releases.html?d=210183](http://www.irconnect.com/noc/press/pages/news_releases.html?d=210183) (accessed 28.03.14)

Phillips, Mark. 'The Challenge of Police Procurement – What is ADS doing about it'. ADS Blog. 15 April 2014. Via: <http://blog.adsgroup.org.uk/challenge-police-procurement-ads/> (accessed 23.04.14)

Phillips, Mark. 'The UK's first security export strategy'. ADS Blog. 27 February 2014. Via: <http://blog.adsgroup.org.uk/uks-first-security-exports-strategy/> (accessed 02.05.14)

RISC. 'Coordination of national security and resilience'. Via: [www.riscuk.org](http://www.riscuk.org) (accessed 20.12.11)

SCS. 'SCS helps to deliver safe London 2012 Olympic and Paralympic Games'. 10 September 2012. Via: <http://scs.scs.biz/news/scs-helps-to-deliver-safe-london-2012-olympic-paralympic-games/> (accessed 17.09.12)

techUK. 'Increasing our Security Exports - New Strategy Launched Today!' Via: <http://www.techuk.org/insights/news/item/1080-increasing-our-security-exports-new-strategy-launched-today> (accessed 02.05.14)

Turner, Mike. Letter from Mike Turner (CEO of BAE Systems) to the Prime Minister. 'Support for Exports'. 26th July 2007. Via: [http://www.defenseindustrydaily.com/files/DESO\\_Letter\\_BAE\\_2007-07-26.pdf](http://www.defenseindustrydaily.com/files/DESO_Letter_BAE_2007-07-26.pdf) (accessed 30.04.14)

### **London 2012 documentation**

International Olympic Committee. 'Report of the IOC Evaluation Commission for the Games of the XXX Olympiad in 2012'. 22 March 2005. Via: [http://www.olympic.org/Documents/Host\\_city\\_elections/2012\\_OG-Report\\_of\\_the\\_Evaluation\\_Commission.pdf](http://www.olympic.org/Documents/Host_city_elections/2012_OG-Report_of_the_Evaluation_Commission.pdf) (accessed 06.09.12)

International Olympic Committee. 'The Worldwide Top Partners'. Via: <http://www.olympic.org/sponsors> (accessed 23.09.12)

London 2012. 'Biometric scanners enhance Olympic Park security as big build ramps up'. 16 October 2009. Via: <http://www.london2012.com/press/media-releases/2009/10/biometric-scanners-enhance-olympic-parksecurity-as-big-build-ramps-up.php> (accessed 11.01.12)

London 2012. 'List of commercial partners for the Games'. <http://www.london2012.com/about-us/the-peopledelivering-the-games/london-2012-olympic-games-partners.php> (accessed 19.01.12)

London 2012. 'London 2012 confirms vehicle screening plans for Westfield shopping centre'. 5 September 2011. Via: <http://www.london2012.com/news/2011/09/london-2012-confirms-vehicle-screeningplans-for-westfie.php> (accessed 15.01.12)

London 2012. 'London 2012 confirms Westfield as sponsor and hits £700m mark'. 7 September 2011. Via: <http://www.london2012.com/news/2011/09/london-2012-confirms-westfield-as-sponsor-andhits-700m-.php> (accessed 15.01.12)

London 2012, 'London 2012 secures G4S as Games Sponsor'. 21 March 2011. Via: <http://www.london2012.com/press/media-releases/2011/03/london-2012-secures-g4s-as-sponsor.php> (accessed 11.01.12)

London 2012. 'London 2012 signs Rapiscan as tier three sponsor'. 10 March 2011. Via: <http://www.london2012.com/press/media-releases/2011/03/london-2012-signs-rapiscan-as-tier-threesponsor.php> (accessed 11.01.12)

London 2012. 'Olympic Park security set to increase as construction intensifies'. 4 July 2008. Via: <http://www.london2012.com/press/media-releases/2008/07/olympic-park-security-set-to-increase-asconstruction-intensifies.php> (accessed 12.01.12)

London 2012. 'Preparing your business for the games'. Via: <http://www.london2012.com/getinvolved/business-network/preparing-your-business.php> (accessed 15.01.12)

London 2012. *Theme 12, London 2012 Candidature File*. London: London 2012, 2004.

Olympic Delivery Authority. 'London 2012 Suppliers Map'. Via: <http://www.london2012.com/get-involved/business-network/odasuppliers/map.php> (accessed 11.01.12)

### **Reports and Pamphlets**

Allouche, Jeremy, and Jeremy Lind. 'Public Attitudes to Global Uncertainties: A Research Synthesis exploring the trends and gaps in knowledge'. November 2010. Via: [http://www.esrc.ac.uk/\\_images/ESRC%20Global%20Uncertainties%20Research%20Synthesis%20FINAL\\_tcm8-14632.pdf](http://www.esrc.ac.uk/_images/ESRC%20Global%20Uncertainties%20Research%20Synthesis%20FINAL_tcm8-14632.pdf) (Accessed 16.08.12)

Brito, Jerry, and Tate Watkins. 'Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy', Mercatus Center Working Paper No.11-24. April 2011. Via: <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy> (accessed 24.06.11)

Campaign Against the Arms Trade. 'Arms trading at UKTI'. November 2008. Via: <http://www.caat.org.uk/resources/publications/government/ukti-briefing.pdf> (accessed 30.04.14)

Campaign Against the Arms Trade. 'Introduction to the Arms Trade'. April 2011. Via: <http://www.caat.org.uk/resources/publications/intro-briefing-2011.pdf> (accessed 16.07.14)

Chalmers, Malcolm. 'The Financial Context for the 2015 SDSR The End of UK Exceptionalism?'. RUSI Briefing Paper. September 2014. Via: [https://www.rusi.org/downloads/assets/201409\\_BP\\_Financial\\_Context\\_of\\_the\\_2015\\_SDSR.pdf](https://www.rusi.org/downloads/assets/201409_BP_Financial_Context_of_the_2015_SDSR.pdf) (accessed 15.11.14)

Chatham House, 'The Chatham House-YouGov Survey 2011, British Attitudes Towards the UK's International Priorities'. July 2011. Via:

[http://www.chathamhouse.org/sites/default/files/0711ch\\_yougov\\_analysis.pdf](http://www.chathamhouse.org/sites/default/files/0711ch_yougov_analysis.pdf) (accessed 24.02.12),

Edwards, Charlie. *National Security for the Twenty-First Century*. London: Demos, 2007. Via: <http://www.demos.co.uk/publications/nationalsecurityforthetwentyfirstcentury>

Edwards, Charlie. *Resilient Nation*. London: Demos, 2009. Via: [http://www.demos.co.uk/files/Resilient\\_Nation\\_-\\_web-1.pdf?1242207746](http://www.demos.co.uk/files/Resilient_Nation_-_web-1.pdf?1242207746)

Feuchtwanger, Antonia. *The Best Kit: Why Britain's Defence Doesn't Need an All-British Defence Industry*. London: Policy Exchange, 2004.

Gray, Bernard. 'Review of Acquisition for the Secretary of State for Defence - An independent report by Bernard Gray'. October 2009. Via: <http://www.bipsolutions.com/docstore/ReviewAcquisitionGrayreport.pdf> (accessed 05.02.13)

Gregory, Frank. 'UK Border Security: Issues, systems and recent reforms'. A submission to the ippr Commission on National Security for the 21st Century. 20 March 2009. Via: <http://www.ippr.org/publications/55/1680/uk-border-security-issues-systems-and-recent-reforms> (accessed 20.01.14)

Hayes, Ben. 'NeoConOpticon: The EU Security-Industrial Complex'. Statewatch/Transnational Institute Report. September 2009. Via: <http://neoonopticon.wordpress.com/read-the-report/> (accessed 24.06.11)

Heidenkamp, Henrik. 'Sustaining the UK's Defence Effort: Contractor Support to Operations Market Dynamics'. London: Royal United Services Institute, 2012. Via: [http://www.rusi.org/downloads/assets/WHR\\_2-12\\_CS0\\_Final\\_WEB.pdf](http://www.rusi.org/downloads/assets/WHR_2-12_CS0_Final_WEB.pdf) (accessed 15.08.12)

Heidenkamp, Henrik, John Louth and Trevor Taylor. 'The Defence Industrial Ecosystem: Delivering Security in an Uncertain World'. RUSI Whitehall Report 2-11. June 2011. Via: <http://www.rusi.org/publications/whitehallreports/ref:O4E03231821048/> (accessed 20.02.11)

Horseman Sewell, Ian. 'Augmenting resilience and response: in partnership with the private sector' in Jennifer Cole (Ed.) *Emergency Response and Civil Defence: Report of the workshop held at the Royal United Services Institute on 11 December 2007*. RUSI: London, 2008.

Institute for Public Policy Research. 'Shared Responsibilities: A national security strategy for the UK'. The final report of the IPPR Commission on National Security in the 21st Century. June 2009. Via: [http://www.ippr.org/images/media/files/publication/2012/01/shared-responsibilities\\_security-final\\_June2009\\_1704.pdf](http://www.ippr.org/images/media/files/publication/2012/01/shared-responsibilities_security-final_June2009_1704.pdf) (accessed 01.03.12),

Jones, Seth G. 'The Rise of Europe's Defense Industry'. U.S.-Europe Analysis Series No.18, The Brookings Institution (May 2005). Via: <http://www.brookings.edu/research/papers/2005/05/europe-jones> (accessed 04.02.13)

Latham, Neil. 'Defence Industry in a Global Context: Policy Implications for the United Kingdom', Royal United Service Institute, Whitehall Paper 57:1 (2003)

MacIntosh, Jamie P, John Reid and Len Tyler. 'Cyber Doctrine: Towards a coherent evolutionary framework for learning resilience'. London: Institute for Security and Resilience Studies, 2011. Via: <http://www.ucl.ac.uk/isrs/publications/CyberDoctrine> (accessed 01.07.11)

Murakami Wood, David, and Kirstie Ball. 'A Report on the Surveillance Society: Public Discussion Document'. Surveillance Studies Network, 2006. Via: [http://www.privacyconference2006.co.uk/files/discussion\\_eng.pdf](http://www.privacyconference2006.co.uk/files/discussion_eng.pdf) (accessed 16.08.12)

RUSI Acquisition Focus Group. 'The Defence Materiel Strategy and the GOCO Proposal for Abbey Wood'. Briefing Paper. July 2012. Via: [https://www.rusi.org/downloads/assets/GOCO\\_Briefing.pdf](https://www.rusi.org/downloads/assets/GOCO_Briefing.pdf) (accessed 24.04.14)

Taylor, Trevor, and John Louth. 'What the Government must do in Defence Procurement. The Inherently Governmental Function and the GOCO Proposal for Defence Equipment and Support'. Briefing Paper. September 2013. Via: <https://www.rusi.org/downloads/assets/GOCO.pdf> (accessed 24.04.14)

United Kingdom National Defence Association. 'Inconvenient Truths – Threats Justify Prioritising Defence'. UKNDA Report. September 2011. Via: [http://www.uknda.org/uploads/1/5/3/0/15302742/inconvenient\\_truths\\_tue\\_27\\_final\\_f1\\_3.pdf](http://www.uknda.org/uploads/1/5/3/0/15302742/inconvenient_truths_tue_27_final_f1_3.pdf) (accessed 15.11.14)

Valasek, Tomas. *Surviving Austerity: The case for a new approach to EU military collaboration*. London, Centre for European Reform, 2011. Via: [http://www.cer.org.uk/sites/default/files/publications/attachments/pdf/2011/rp\\_981-141.pdf](http://www.cer.org.uk/sites/default/files/publications/attachments/pdf/2011/rp_981-141.pdf) (accessed 29.06.11)

Walker, Dinah. 'Trends in U.S. Military Spending'. Council on Foreign Relations. 23 August 2012. Via: <http://www.cfr.org/geoeconomics/trends-us-military-spending/p28855> (accessed 04.02.13)

### **Newspaper Articles, Media reports and Documentaries**

BBC News. 'BAE Systems cuts 1,775 jobs at English and Scottish shipyards'. *BBC Website*. 6 November 2013. Via: <http://www.bbc.com/news/uk-scotland-glasgow-west-24831779> (accessed 17.07.14)

BBC News. 'Britain is "surveillance society"'. *BBC Website*. 2 November 2006. Via: [http://news.bbc.co.uk/2/hi/uk\\_news/6108496.stm](http://news.bbc.co.uk/2/hi/uk_news/6108496.stm) (accessed 17.10.12)

BBC News. 'FBU calls for regional fire centres to be scrapped'. *BBC Website*. 6 October 2010. Via: <http://www.bbc.co.uk/news/uk-11478008> (accessed 28.10.13)

BBC News. 'G4S Security boss: "We are sorry and bitterly disappointed"'. *BBC Website*. 14 June 2012. Via: <http://www.bbc.co.uk/news/uk-18840185> (accessed 06.09.12)

BBC News. 'Images of 7 July: Reluctant hero'. *BBC Website*. 2 July 2006. Via: <http://news.bbc.co.uk/2/hi/5105750.stm> (accessed 19.07.13)

BBC News. 'London 2012: Lord Coe applauds armed forces Olympic efforts'. *BBC Website*. 16 January 2013. Via: <http://www.bbc.co.uk/news/uk-19182310> (accessed 21.02.13)

BBC News. 'Soca chairman resigns over undeclared directorship'. *BBC Website*. 1 August 2013. Via: <http://www.bbc.com/news/uk-23537513> (accessed 28.03.14)

BBC News. 'Terror advice pamphlet unveiled', *BBC Website*. 26 July 2004. Via: [http://news.bbc.co.uk/2/hi/uk\\_news/politics/3923949.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/3923949.stm) (accessed 16.11.13)

BBC Radio 4. 'Today Programme'. *BBC Radio Broadcast*. 20 July 2012, Via: [http://news.bbc.co.uk/today/hi/today/newsid\\_9739000/9739444.stm](http://news.bbc.co.uk/today/hi/today/newsid_9739000/9739444.stm) (accessed 09.09.12)

Bounds, Andrew, and Helen Warrell. 'Senior City police detective decamps to private sector'. *Financial Times*. 21 February 2014.

Boxell, James. 'May sacks Raytheon from e-borders contract'. *Financial Times*. 22 July 2010.

'BSIA launches Close Protection Unit for London 2012'. *Ifsecglobal.com*. 3 July 2012. Via: <http://www.ifsecglobal.com/bsia-launches-close-protection-unit-for-london-2012/> (accessed 30.12.14)

Channel 4. 'MPs: G4S Olympics security is a "humiliating shambles"'. *Channel 4 Website*. 17 July 2012. Via: <http://www.channel4.com/news/mps-g4s-olympics-security-is-a-humiliating-shambles>, (accessed 29.08.12)

Corera, Gordon. 'Securing the Games'. *BBC Radio Documentary*. 22 July 2012. Via: <http://www.bbc.co.uk/programmes/b01ky5h1> (accessed 09.09.12)

Cox, Simon. 'The Accountant Kings'. *BBC Radio Documentary*. 9 March 2014. Via: <http://www.bbc.co.uk/programmes/b03wpjja> (accessed 30.03.14)

De la Poer, Robert. 'Securing the Olympic legacy'. *Intersec*. 17 November 2013. Via: <http://www.intersecmag.co.uk/olympics-nov13/> (accessed 01.05.14)

Dodd, Vikram. 'Fresh pressure on Met chief Blair as top Asian police officer sues force over alleged racial discrimination'. *The Guardian*. 19 August 2008. Via: <http://www.theguardian.com/politics/2008/aug/20/police.race> (accessed 11.08.14)



The Economist. 'Defence Costs'. *The Economist online*. 8 August 2011. Via: <http://www.economist.com/blogs/dailychart/2011/06/military-spending> (accessed 04.02.13)

Evans, Rob, and David Leigh. 'Treasury plans to shut arms sales department'. *The Guardian*. 9 July 2007. Via: <http://www.theguardian.com/uk/2007/jul/09/armstrade.economy> (accessed 30.04.14)

Gibson, Owen. 'London 2012 organisers: security estimate was a 'finger in the air exercise''. *The Guardian*. 14 December 2011. Via: <http://www.theguardian.com/sport/2011/dec/14/london-2012-security-estimate-cost> (accessed 11.01.12)

Gilligan, Andrew. 'MoD lobbying claims: The muck and the top brass'. *telegraph.co.uk*. 15 October 2012. Via: <http://www.telegraph.co.uk/news/uknews/defence/9608493/MoD-lobbying-claims-The-muck-and-the-top-brass.html> (accessed 26.02.14)

Gumm, Peter. 'New London CCTV Control Room designed to thwart terrorists'. *SMT Online*. 7 August 2007. Via: <http://www.ifsecglobal.com/new-london-cctv-control-room-designed-to-thwart-terrorists/> (accessed 20.01.12)

Harris, Paul. 'How private firms have cashed in on the climate of fear since 9/11'. *theguardian.com*. 5 September 2011. Via: <http://www.theguardian.com/world/2011/sep/05/private-firms-fear-9-11> accessed 12.11.14)

Hildebrand, Anthony. 'Olympic concerns'. *SMT Online*. 25 October 2007. Via: <http://www.ifsecglobal.com/olympic-concerns/> (accessed 03.09.12)

Hopkins, Nick. 'Army warns Olympic Games recovery will take two years'. *The Guardian*. 13 August 2012. Via: <http://www.guardian.co.uk/uk/2012/aug/13/army-olympic-games-recovery-two-years> (accessed 26.08.12)

Hopkins, Nick, and Owen Gibson, 'Olympics security bill: how it soared to more than £1bn'. *The Guardian*. 9 March 2012. Via: <http://www.guardian.co.uk/sport/2012/mar/09/olympics-security-bill-how-it-soared> (accessed 07.05.12)

Hopkins, Nick, and Richard Norton-Taylor. 'US officials worried about security at London 2012 Olympics'. *The Guardian*. 13 November 2011. Via: <http://www.guardian.co.uk/sport/2011/nov/13/us-worried-london-olympics-security-2012> (accessed 07.05.12)

'Invest in UK national security and resilience industry'. *CT Review* (Sept/Oct 2010)

Jack, Andrew. 'Britain set to test pioneering 'e-borders' monitoring system'. *Financial Times*. 4 August 2008.



King, Leo. 'FireControl failure blasted by Fire Brigades Union'. *Computerworlduk.com*. 1 July 2011. Via: <http://www.computerworlduk.com/news/public-sector/3289170/firecontrol-failure-blasted-by-fire-brigades-union/> (accessed 25.10.13)

Kobie, Nicole. 'New IT industry alliance to look at national security'. *ITPRO*. 2 April 2007. Via: <http://www.itpro.co.uk/109313/new-it-industry-alliance-to-look-at-national-security#ixzz2yIJQ8Xuj> (accessed 08.04.14)

Lewis, Jason. 'Stasi HQ UK... where details of all your journeys are secretly logged and kept for a decade'. *Mail on Sunday*. 21 March 2009. Via: <http://www.dailymail.co.uk/news/article-1163786/Stasi-HQ-UK---details-journeys-secretly-logged-kept-decade.html> (accessed 05.02.14)

Leyden, John. 'UK e-Borders scheme thrown into confusion by EU rules'. *The Register*. 18 December 2009. Via: [http://www.theregister.co.uk/2009/12/18/e\\_borders\\_confusion/](http://www.theregister.co.uk/2009/12/18/e_borders_confusion/) (accessed 26.02.14)

Lomas, Natasha. '£39m boost for London Olympics' emergency comms'. *ZDNet.com*. 3 November 2009. Via: <http://www.zdnet.com/article/39m-boost-for-london-olympics-emergency-comms/> (accessed 12.01.15)

'London 2012: IOC President 'reassured' by troops presence for Olympic security'. *The Telegraph*, 23 July 2012). Via: <http://www.telegraph.co.uk/sport/olympics/olympicsvideo/9421384/London-2012-IOC-President-reassured-by-troops-presence-for-Olympic-security.html> (accessed 06.09.12)

Luce, Edward. 'Data intelligence complex is the real story'. *Financial Times*. 7 June 2014. Via: <http://www.ft.com/cms/s/0/a1dd626c-cf80-11e2-be7b-00144feab7de.html?siteedition=intl> (accessed 12.11.14)

'More markets at the double'. *Professional Security Magazine*. Vol.24.4. April 2014. Via: <http://www.professionalsecurity.co.uk/online-magazine/20-03-14/april/#p=46> (accessed 01.05.14)

Pfeifer, Sylvia. 'Defence groups turn focus to security at home'. *Financial Times*. 4 August 2008. Via: <http://www.ft.com/intl/cms/s/0/cdd2deb6-61bb-11dd-af94-000077b07658.html#axzz3N8B2pAKS> (accessed 27.12.14)

Plimmer, Gill, and Jonathan Moules. 'G4S takes £88m hit for Olympics fiasco'. *Financial Times*. 12 February 2013. Via: <http://www.ft.com/cms/s/0/73df1bae-74e9-11e2-8bc7-00144feabdc0.html#axzz3A7clDdfN> (accessed 11.08.14)

Robertson, David, Roland Watson and Angus Macleod. 'Revealed: truth about the aircraft carrier deal'. *The Times*. 22 October 2010. Via: <http://www.pressawards.org.uk/userfiles/files/entries-01287-01284.pdf> (accessed 10.12.14)

- Rohde, David. 'The Security-Industrial Complex'. *The Atlantic*. 15 June 2013. Via: <http://www.theatlantic.com/politics/archive/2013/06/the-security-industrial-complex/276906/> (accessed 12.11.14)
- Sengupta, Ramananda. 'Interview: UK-India defence ties'. *sify.com*. 11 February 2009. Via: <http://www.sify.com/news/interview-uk-india-defence-ties-news-columns-jegsUJhhaib.html> (accessed 30.04.14)
- Shaw, Danny. 'E-borders system "failing on passenger checks"'. *BBC Website*. 9 October 2013. Via: <http://www.bbc.co.uk/news/uk-24453677> (accessed 11.02.14)
- Tobin, Edmund. 'CHIGWELL: CBE for security firm executive'. *East London and West Essex Guardian*. 26 October 2010. Via: [http://www.guardian-series.co.uk/news/8475939.CHIGWELL\\_CBE\\_for\\_security\\_firm\\_executive/](http://www.guardian-series.co.uk/news/8475939.CHIGWELL_CBE_for_security_firm_executive/) (accessed 31.08.14)
- Topping, Alexandra. 'G4S Olympic scandal: Ed Miliband calls for rethink of police outsourcing'. *The Guardian*. 19 July 2013. Via: <http://www.guardian.co.uk/politics/2012/jul/19/g4s-olympic-ed-miliband-police> (accessed 10.02.13)
- Travis, Alan, and Owen Gibson. 'G4S failed to understand size of Olympic security job, says Lord Coe'. *The Guardian*. 11 September 2012. Via: <http://www.guardian.co.uk/business/2012/sep/11/g4s-failed-olympic-security-lord-coe> (accessed 14.09.12)
- Turley, Jonathan. 'Big money behind the military-industrial complex'. *Al Jazeera*. 11 January 2014. Via: <http://www.aljazeera.com/indepth/opinion/2014/01/big-money-behind-war-military-industrial-complex-20141473026736533.html> (accessed 12.11.14)
- Tusa, Francis. 'Buying Defence'. BBC Radio Documentary. 27 December 2011. Via: <http://www.bbc.co.uk/programmes/b017mtfc> (accessed 16.08.12)
- Uchitelle, Louis, and John Markoff. 'Terrorbusters Inc.'. *New York Times*. 17 October 2004. Via: [http://www.nytimes.com/2004/10/17/business/yourmoney/17home.html?\\_r=0](http://www.nytimes.com/2004/10/17/business/yourmoney/17home.html?_r=0) (accessed 12.11.14)
- Wainwright, Daniel. 'John Prescott: Don't blame me for Wolverhampton fire control centre fiasco'. *The Express & Star*. 11 June 2013. Via: <http://www.expressandstar.com/news/politics/2013/06/11/john-prescott%E2%80%88dont-blame-me-for-wolverhampton-fire-control-centre-fiasco/> (accessed 28.11.13)
- Walker, Peter. 'Olympic military guards will not take orders from security staff'. *The Guardian*. 26 January 2012. Via: <http://www.theguardian.com/uk/2012/jan/26/olympics-military-guards-take-orders> (accessed 29.01.12)

Warrell, Helen, and Ed Crooks. 'UK ordered to pay Raytheon £224m over eBorders contract'. *Financial Times*. 18 August 2014. Via: <http://www.ft.com/intl/cms/s/0/68f98f04-23bf-11e4-8e29-00144feabdc0.html#axzz3Bmd5FHsZ> (accessed 31.08.14)

Watts, Nick. 'Latching onto the future'. Interview with Richard Paniguan. 29 March 2014. Via: <http://www.defenceviewpoints.co.uk/interviews/latching-onto-the-future> (accessed 18.01.15)

Wolf, Naomi. 'The spectacle of terror and its vested interests'. *The Guardian*. 9 May 2012. Via: <http://www.guardian.co.uk/commentisfree/cifamerica/2012/may/09/spectacle-terror-vested-interests> (accessed 15.08.12)

### **Opinion Pieces**

Barry, Tom. 'Synergy in Security: The Rise of the National Security Complex.' *Dollars & Sense: Real World Economics*. March/April 2010. Via: <http://www.dollarsandsense.org/archives/2010/0310barry.html> (Originally accessed on 19.05.11)

Coughlin, Con. 'An army without soldiers is doomed to failure'. *blogs.telegraph.co.uk*. 19 December 2013. Via: <http://blogs.telegraph.co.uk/news/concoughlin/100251343/an-army-without-soldiers-is-doomed-to-failure/> (accessed 14.06.14)

Cross, Michael. 'The illegal e-Borders disaster'. *theguardian.com*. 18 December 2009. Via: <http://www.theguardian.com/commentisfree/libertycentral/2009/dec/18/illegal-eborders-disaster-it-profession> (accessed 07.02.14)

Danil, Linda. 'The arms trade and the military-industrial complex: a UK perspective', *Critical Legal Thinking Blog*. 20 July 2012. Via: <http://criticallegalthinking.com/2012/07/30/the-arms-trade-and-the-military-industrial-complex/> (accessed 12.11.14)

Embassy, United States. 'Ambassador Susman calls 2012 greatest ever Games'. 14 August 2012. Via: <http://www.usembassy.org.uk/london2012/2012/08/14/congratulations-britain-says-ambassador-susman/> (accessed 17.08.12)

Gash, Tom. 'Blame Games'. Institute for Government Blog. 20 July 2012. Via: <http://www.instituteforgovernment.org.uk/blog/4658/blame-games/> (accessed 28.11.13)

Greenwald, Glenn. 'The decade's biggest scam'. *salon.com*. 29 August 2011. Via: [http://www.salon.com/2011/08/29/terrorism\\_39/](http://www.salon.com/2011/08/29/terrorism_39/) (accessed 12.11.14)

Hughes, Solomon. 'Shining A Light On Raytheon'. *The People's Daily Morning Star*. 22 November 2013. Via: <http://www.morningstaronline.co.uk/a-b0f3-Shining-a-light-on-Raytheon> (accessed 12.11.14)

Hughes, Solomon. 'Follow the money: the "war on terror" and the multinationals who are profiteering from it'. *Socialist Review*. March 2008. Via: <http://www.socialistreview.org.uk/article.php?articlenumber=10305> (accessed 24.02.12)

Jenkins, Simon. 'How Londoners can survive the Olympics'. *London Evening Standard*. 26 July 2011. Via: <http://www.standard.co.uk/news/how-londoners-can-survive-the-olympics-6426212.html> (accessed 20.01.12)

Jenkins, Simon. 'If the MoD can't name the enemy, it shouldn't buy the weapons'. *theguardian.com*. 16 January 2014. Via: <http://www.theguardian.com/commentisfree/2014/jan/16/mod-cant-name-enemy-shouldnt-buy-weapons-threat-cold-war-defence> (accessed 12.11.14)

Jenkins, Simon. 'Oh! What a Lovely War on Terror - it's the number the arms dealers love', *theguardian.com*. 14 September 2007. Via: <http://www.theguardian.com/commentisfree/2007/sep/14/comment.politics> (accessed 12.11.14)

Jenkins, Simon. 'The real threat to our way of life? Not terrorists or faraway dictators, but our own politicians and securocrats'. *theguardian.com*. 27 August 2013. Via: <http://www.theguardian.com/commentisfree/2013/aug/27/real-threat-terrorist-politicians-national-security> (accessed 14.06.14)

Kelly, Mel. 'Police, magistrates and prisons by G4S. Is this what the British people want?' *openDemocracy*. 6 March 2012. Via: <http://www.opendemocracy.net/ourkingdom/mel-kelly/police-magistrates-and-prisons-by-g4s-is-this-what-british-people-want> (accessed 19.04.12)

King, Eric. 'Selling arms and snooping technology is no way to help democracy, Cameron'. *guardian.com*. 11 April 2012. Via: <http://www.theguardian.com/commentisfree/2012/apr/11/selling-arms-cameron> (accessed 23.04.12).

Kone, Aminata. 'The Military-Industrial Complex in the United States: Evolution and Expansion from World War II to the War on Terror'. *Student Pulse*. Vol.5:8 (2013). Via: <http://www.studentpulse.com/articles/749/the-military-industrial-complex-in-the-united-states-evolution-and-expansion-from-world-war-ii-to-the-war-on-terror> (accessed 12.11.14)

Palmer, Alasdair. 'FiReControl Project: silly name, stupid idea – but you and I will pay for the fiasco'. *Daily Telegraph*. 24 September 2011. Via: <http://www.telegraph.co.uk/news/politics/8786524/FiReControl-Project-silly-name-stupid-idea-but-you-and-I-will-pay-for-the-fiasco.html> (accessed 08.08.13)

Palombi, Simon. 'Foreign Fighters and Threat Magnification', *Chatham House Expert Comment*, 12 August 2014. Via: <http://www.chathamhouse.org/expert/comment/15511> (accessed 10.11.14).

Phillips, Chris. 'Why we need Counter Terrorism'. *Professional Security Magazine*. 5 June 2013. Via: <http://www.professionalsecurity.co.uk/news/interviews/why-we-need-counter-terrorism/> (accessed 15.11.13)

Rosemont, Hugo. 'Reassessing the G4S Olympic security affair'. *Defencemanagement.com*. 3 October 2012. Via: [http://www.defencemanagement.com/feature\\_story.asp?id=20939](http://www.defencemanagement.com/feature_story.asp?id=20939) (accessed 05.10.12)

Rosemont, Hugo. 'What does security mean to you?'. *The Guardian*. 13 August 2009. Via: <http://www.guardian.co.uk/commentisfree/2009/aug/13/national-security-strategy-liberty> (accessed 17.06.11)

Rowe, Mark. 'Editor's Comment'. *Professional Security Magazine*. Vol.24:5. May 2014. Via: <http://www.professionalsecurity.co.uk/online-magazine/28-04-14/24-5/#p=6> (accessed 01.05.14)

Sambrook, Claire. 'Surveillance + detention = £Billions: How Labour's friends are 'securing your world''. *opendemocracy.net*. 13 April 2010. Via: <http://www.opendemocracy.net/ourkingdom/clare-sambrook/surveillance-detention-%C2%A3billions-how-labour%E2%80%99s-friends-are-%E2%80%98securing-your-w> (accessed 27.03.14)

Soria, Valentina. 'G4S and London 2012: Choosing your partners wisely?' *RUSI Analysis*. 26 July 2012. Via: <http://www.rusi.org/analysis/commentary/ref:C50115986AD337/> (accessed 26.08.12)

Toynbee, Polly. 'Accountancy's Big Four are laughing all the way to the tax office'. *theguardian.com*. 1 February 2013. Via: <http://www.theguardian.com/commentisfree/2013/feb/01/accountancy-big-four-laugh-tax-office> (accessed 30.03.14)

Wedel, Janine R., and Linda Keenan. 'Shadow Elite: Eisenhower's Dark Vision Realized – The Military-Industrial Complex at 50'. *The Huffington Post*. 13 January 2011. Via: [http://www.huffingtonpost.com/janine-rwedel/emshadow-eliteem-eisenhow\\_b\\_808410.html](http://www.huffingtonpost.com/janine-rwedel/emshadow-eliteem-eisenhow_b_808410.html) (accessed 02.06.11)

### **Miscellaneous websites**

Biography for Charlie Edwards. *CSaP Website*. Via: <http://www.csap.cam.ac.uk/network/charlie-edwards/> (accessed 27.03.14)

Biography for Charlie Edwards. *Demos Website*. Via: <http://www.demos.co.uk/people/charlieedwards> (accessed 27.03.14)

Biography for Richard Fletcher. *Anthem Corporate Finance Website*. Via: <http://www.anthemcf.com/team-senioradvisor-RichardFletcher.html> (accessed 26.03.14)

Biography for John Howe. *Debretts.com*. Via: <http://www.debretts.com/people-of-today/profile/819/John-Francis-HOWE> (accessed 19.01.15)

Biography for Sir Richard Mottram. *CSaP Website*. Via: <http://www.csap.cam.ac.uk/network/richard-mottram/> (accessed 18.01.15)

Biography for Adam-Ogilvie-Smith. *Robert Gordon University Website*. Via:  
<http://www.rgu.ac.uk/dmstaff/adam-ogilvie-smith> (accessed 27.01.14)

Biography for Sir David Omand. 'Management Team'. *Babcock Plc Website*. Via:  
<http://www.babcockinternational.com/mobile/about-us/management-team/> (accessed 28.03.14)

Biography for Mark Phillips. 'Register of Interests of Lords Members' Staff'. Via:  
[www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests/register-of-interests-of-lords-members-staff/?letter=N](http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests/register-of-interests-of-lords-members-staff/?letter=N) (accessed 26.02.14)

Biography for John Yard. *CIO Development Website*. Via:  
<http://www.ciodevelopment.com/about-us/john-yard/> (accessed 26.03.14)

British American Security Information Council. 'Four major UK security announcements on eve of parliamentary recess'. July 30 2007. Via:  
<http://www.basicint.org/press/releases/2010/four-major-uk-security-announcements-eve-parliamentary-recess> (accessed 30.04.14)

BSIA. 'Part 1 of 3 Admiral the Lord West of Spithead speaking at The BSIA Annual Lunch 2009'. BSIA YouTube Channel. Uploaded on Aug 11, 2009. Via:  
<http://www.youtube.com/watch?v=43RBKV6w2IQ> (accessed 15.11.13).

BSIA. 'Part 2 of 3 - Admiral the Lord West of Spithead speaking at The BSIA Annual Lunch 2009'. BSIA YouTube Channel. Uploaded on Aug 11, 2009. Via:  
<http://www.youtube.com/watch?v=Qd9gmhSdA6w> (accessed 15.11.13)

BSIA. 'Part 3 of 3 - Admiral the Lord West of Spithead speaking at The BSIA Annual Lunch 2009'. BSIA YouTube Channel. Uploaded on Aug 11, 2009. Via:  
<http://www.youtube.com/watch?v=eHSPGuvlCBQ> (accessed 24.04.14)

'Budget 2014: the government's spending and income visualised'. *theguardian.com*. Via:  
<http://www.theguardian.com/news/datablog/2014/mar/21/budget-2014-tax-spending-visualised> (accessed 19.12.14)

Campaign Against the Arms Trade. 'About CAAT'. CAAT Website. Via:  
<http://www.caat.org.uk/about/> (accessed 26.03.14)

Campaign Against the Arms Trade. 'Delegations'. CAAT Website. Via:  
<http://www.caat.org.uk/issues/arms-fairs/security-and-policing/delegations/> (accessed 01.05.14)

Campaign Against the Arms Trade. 'High-level advisory bodies'. CAAT Website. Via:  
<http://www.caat.org.uk/issues/influence/advisory-bodies.php> (accessed 03.04.14)

Campaign Against the Arms Trade. 'Political Influence'. CAAT Website. Via:  
<http://www.caat.org.uk/issues/influence/> (accessed 26.03.14)

Campaign Against the Arms Trade. 'Revolving Door Log'. CAAT Website. Via: <http://www.caat.org.uk/issues/influence/revolving-door.php> (accessed 26.03.14)

Campaign Against the Arms Trade. 'UKTI: Armed & Dangerous'. CAAT Website. Via: <http://www.caat.org.uk/issues/ukti/> (accessed 01.04.14)

Cann, Vicky. 'Magnus Ovilius and sabbatical'. Letter to Human Resources and Security, European Commission. 20 December 2013. Via: [http://www.asktheeu.org/en/request/magnus\\_ovilius\\_and\\_sabbatical](http://www.asktheeu.org/en/request/magnus_ovilius_and_sabbatical) (accessed 28.03.14)

Cityforum. 'The security and Safety of the 2012 Olympics'. *Cityforum Website* (event listing). Via: [http://www.cityforum.co.uk/index.php?option=com\\_eventlist&func=details&did=4&book=no](http://www.cityforum.co.uk/index.php?option=com_eventlist&func=details&did=4&book=no) (accessed 19.01.12)

Considerate Constructors Scheme. Details of Gold award for CLM. Via : <http://www.ccscheme.org.uk/index.php/site-registration/national-site-awards/search-for-award-winners> (accessed 29.12.14)

Corporate Europe Observatory. 'RevolvingDoorWatch Cases – Magnus Ovilius'. *Corporate Europe Observatory Website*. Via: <http://corporateeurope.org/revolvingdoorwatch/case/Magnus-Ovilius> (accessed 28.03.14)

CSSC. 'About CSSC'. Via: <http://www.vocal.co.uk/cssc/about-cssc/> (accessed 30.12.14)

Defence IQ. 'UK Border Agency Director Says E-borders Is Ready For London 2012 Olympics'. *Defence IQ Podcast*. Via: <http://www.defenceiq.com/army-and-land-forces/podcasts/uk-border-agency-director-says-e-borders-is-ready/> (accessed 15.01.12)

Global Day of Action on Military Spending UK. 'Home'. Via: <http://demilitarize.org.uk/> (accessed 01.04.14)

Historic Currency Converter. *X-Rates Website*. Via: <http://www.x-rates.com/> (accessed 27.08.12)

'Historic Spending By Area'. *Guardian Datablog*. Via: <http://www.guardian.co.uk/news/datablog/2010/oct/18/historic-government-spending-area#data> (accessed 04.02.13)

LCIA. 'Frequently Asked Questions'. *LCIA Website*. Via: [http://www.lcia.org/Frequently\\_Asked\\_Questions.aspx#Length](http://www.lcia.org/Frequently_Asked_Questions.aspx#Length) (accessed 28.01.14)

RUSI. 'Olympic and Paralympic Security Conference 2012'. *RUSI Website* (event listing). Via: <http://www.rusi.org/go.php?structureID=S4332E5804C30C&ref=E4EA806969DDDB> (accessed 15.01.12)

'Security Sector Advisory Group (SSAG)'. Opentoexport.com. 4th April 2012. Via: <http://opentoexport.com/article/security-sector-advisory-group-ssag/> (accessed 01.05.14)

Souka, Irene. 'Your application for access to documents - Ref GestDem No 2014/31'. Letter to Vicky Cann from European Commission, Directorate-General Human Resources and Security. 27 March 2014. Via:

<http://www.asktheeu.org/en/request/1111/response/4515/attach/3/Signed%20letter%20by%20Ms%20Souka.pdf> (accessed 28.03.14)

Stockholm International Peace Research Institute. 'The SIPRI Military Expenditure Database'. Military Expenditure of USA. Via: <http://milexdata.sipri.org/result.php4> (accessed 04.02.13)

Stockholm International Peace Research Institute. 'The SIPRI Military Expenditure Database'. Military Expenditure of UK. Via: <http://milexdata.sipri.org/result.php4> (accessed 04.02.13)



## LATER WORKS

### Books

- Abrahamsen, Rita, and Michael C. Williams. *Security Beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press, 2011.
- Adams, Gordon. *The Politics of Defense Contracting: The Iron Triangle*. New York: Transaction Publishers, 1981.
- Armstrong, Stephen. *War plc: The Rise of the New Corporate Mercenary*. London: Faber and Faber Ltd, 2009.
- Avant, Deborah. *The Market for Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press, 2005.
- Baumgartner, John Stanley. *The Lonely Warriors: Case for the Military-Industrial Complex*. Los Angeles: Nash Publishing, 1970.
- Bennett, Colin J., and Kevin D. Haggerty. *Security Games: Surveillance and Control at Mega-Events*. Oxford: Routledge, 2011.
- Bobbitt, Philip. *The Shield of Achilles: War, Peace and the Course of History*. London: The Penguin Press, 2002.
- Bobbitt, Philip. *Terror and Consent: The Wars for the Twenty-First Century*. London: Allen Lane, 2008.
- Busch, Nathan E., and Austen D Givens. *The Business of Counterterrorism: Public-Private Partnerships in Homeland Security*. New York: Peter Lang Publishing, Inc., 2014.
- Buzan, Barry, Ole Waever and Jaap de Wilde. *Security: A New Framework for Analysis*. London: Lynne Rienner, 1998.
- Chalmers, Malcolm. *Paying for Defence: Military Spending and British Decline*. London: Pluto Press, 1985.
- Chicago University Press. *The Chicago Manual of Style: 15<sup>th</sup> Edition*. Chicago: Chicago University Press, 2003.
- Cooper, Robert. *The Breaking of Nations: Order and Chaos in the Twenty-first Century*. London: Atlantic Books, 2004.
- Dexter, Lewis Anthony. *elite and specialized interviewing*. Colchester: ECPR Press, 2006.
- Edgerton, David. *Britain's War Machine: Weapons, Resources and Experts in the Second World War*. London: Penguin Books, 2012.
- Farrell, Theo. *Weapons Without A Cause: The Politics of Weapons Acquisition in the United States*. London: MacMillan Press, 1997.

- Feinstein, Andrew. *The Shadow World: Inside The Global Arms Trade*. London: Penguin Books, 2011.
- Freedman Laurence. *The Revolution in Strategic Affairs*. Oxford: International Institute for Strategic Studies, 1998.
- Freedman, Lawrence. *The Politics of British Defence, 1979-98*. Basingstoke: MacMillan Press, 1999.
- Fussey, Pete, Jon Coaffee, Gary Armstrong and Dick Hobbs. *Securing and Sustaining the Olympic City: Reconfiguring London for 2012 and Beyond*. Farnham: Ashgate Publishing, 2011.
- Gansler, Jacques. *Democracy's Arsenal: Creating a Twenty-First-Century Defense Industry*. London: MIT Press, 2011.
- Gottlieb, Sanford. *Defense Addiction: Can America Kick the Habit?* Oxford: Westview Press, 1997.
- Hayman, Andy, and Margaret Gilmore. *The Terrorist Hunters*. London: Bantam Press, 2009.
- Held, David, and Anthony McGrew, (Eds.) *The Global Transformations Reader, Second Edition*. Cambridge: Polity Press, 2003.
- Hennessy, Peter. *The Secret State: Preparing For The Worst 1945-2010*. London: Penguin Books, 2010.
- Hewitt, Steve. *The British War on Terror: Terrorism and Counter-terrorism on the Home Front Since 9/11*. London: Continuum, 2008.
- Hoffman, Bruce. *Inside Terrorism: Revised and Expanded Edition*. New York: Columbia University Press, 2006.
- Horgan, John. *The Psychology of Terrorism*. Oxford: Routledge, 2005.
- Hughes, Solomon. *War on Terror, Inc. Corporate Profiteering from the Politics of Fear*. London: Verso, 2007.
- Johnston, Les, and Clifford Shearing. *Governing Security: Explorations in policing and justice*. Oxford: Routledge, 2003.
- Kampfner, John. *Blair's Wars*. London: Simon & Schuster Ltd, 2004.
- Kampfner, John. *Freedom For Sale*. New York: Basic Books, 2010.
- Kennedy, John F. *Why England Slept*. New York: Wilfred Funk Inc., 1940.
- Kilcullen, David. *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. London: Hurst & Co, 2009.

- Kincaid, Bill. *Changing the Dinosaur's Spots: The Battle to Reform Defence Acquisition*. London: RUSI, 2008.
- King, Anthony, and Ivor Crewe. *The Blunders of our Governments*. London: Oneworld Publications, 2013.
- Kinsey, Christopher. *Private Contractors and the Reconstruction of Iraq*. Oxford: Routledge, 2009.
- Krahmann, Elke. *States, Citizens and the Privatization of Security*. Cambridge: Cambridge University Press, 2010.
- Krasner, Stephen D. *Sovereignty: Organised Hypocrisy*. Chichester: Princeton University Press, 1999.
- Krause, Keith, and Michael C. Williams (Eds.), *Critical Security Studies: Concepts and Cases*. London: UCL Press, 1997.
- Ledbetter, James. *Unwarranted Influence: Dwight D. Eisenhower and the Military-Industrial Complex*. Yale: Yale University Press, 2011.
- Mabee, Bryan. *The Globalisation of Security: State Power, Security Provision and Legitimacy*. Basingstoke: Palgrave, 2009.
- Manningham-Buller, Eliza. *Securing Freedom*. London: Profile Books Limited, 2012.
- Mueller, John. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*. New York: Simon and Schuster, Inc., 2006.
- Mueller, John, and Mark G. Stuart. *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*. Oxford: Oxford University Press, 2011.
- O'Hanlon, Michael. *Technological Change and the Future of Warfare*. Washington: Brookings Institution, 2000.
- Omand, David. *Securing the State*. London: C. Hurst & Co., 2010.
- Page, Lewis. *Lions, Donkeys and Dinosaurs: Waste and Blundering in the Military*. London: Random House, 2006.
- Parrott, David. *The Business of War: Military Enterprise and Military Revolution in Early Modern Europe*. Cambridge: Cambridge University Press, 2012.
- Priest, Dana, and William Arkin. *Top Secret America: The Rise of the New American Security State*. New York: Little, Brown and Company, 2011.
- Pursell, Jr., Carroll W. (Ed.) *The Military-Industrial Complex*. New York: Harper and Row, 1972.
- Richards, Anthony, Pete Fussey and Andrew Silke (Eds.) *Terrorism and the Olympics: Major event security and lessons for the future*. London: Routledge, 2011.

- Richards, Julian. *A Guide to National Security: Threats, Responses, and Strategies*. Oxford: Oxford University Press, 2012.
- Risen, James. *Pay any Price: Greed, Power, and Endless War*. New York: Harcourt Publishing, 2014.
- Sarkesian, Sam C. (Ed.) *The Military-Industrial Complex: A Reassessment*. London, Sage Publications, 1972.
- Sassen, Saskia. *Losing Control? Sovereignty in an Age of Globalization*. New York: Cambridge University Press, 1996.
- Schmid , Alex P., and Albert J. Jongman. *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*. New Jersey: Transaction Publishers, 1998.
- Shaw, Jonathan. *Britain in a Perilous World: The Strategic Defence and Security Review We Need*. London: Haus Publishing, 2014.
- Sheehan, Michael. *International Security: An Analytical Survey*. London: Lynne Rienner, 2005.
- Shorrock, Tim. *Spies for Hire: The Secret World of Intelligence Outsourcing*. London: Simon & Schuster, 2008.
- Singer, Peter. *Corporate Warriors: The Rise of the Privatized Military Industry*. New York: Cornell University Press, 2003.
- Smith, Dan, and Ron Smith. *The Economics of Militarism*. London: Pluto Press, 1983.
- Smith, Ron. *Military Economics: The Interaction of Money and Power*. Basingstoke: Palgrave Macmillan, 2009.
- Spruyt, Hendrik. *The Sovereign State and its Competitors*. Princeton: Princeton University Press, 1996.
- Strange, Susan. *The Retreat of the State: The Diffusion of Power in the World Economy*. New York: Cambridge University Press, 1996.
- Stanger, Allison. *One Nation Under Contract: The Outsourcing of American Power and the Future of Foreign Policy*. London: Yale University Press, 2009.
- Van Steden, Ronald. *Privatizing Policing: Describing and explaining the growth of private security*. Hoofddorp: BJU Publishers, 2007.
- Verkuil, Paul R. *Outsourcing Sovereignty: Why Privatization of Government Functions Threatens Democracy and What We Can Do About It*. New York: Cambridge University Press, 2007.
- White, Adam. *The Politics of Private Security*. London: Palgrave Macmillan, 2010.

Wilkinson, Paul (Ed.) *Homeland Security in the UK: Future preparedness for terrorist attack since 9/11*. London: Routledge, 2007.

Wilkinson, Paul. *Terrorism Versus Democracy: The Liberal State Response*. London: Frank Cass, 2001.

Wilkinson, Paul. *Terrorism Versus Democracy; The Liberal State Response*. London: Frank Cass, 2005.

Wilkinson, Paul. *Terrorism Versus Democracy: The Liberal State Response, Second Edition*. Oxford: Routledge, 2006.

Wood, Jennifer, and Benoit Dupont. *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press, 2006.

Wright Mills, C. *The Power Elite*. New York: Oxford University Press, 1956.

Zarate, Juan C. *Treasury's War: The Unleashing of a New Era of Financial Warfare*. New York: Public Affairs Books, 2013.

Zedner, Lucia. *Security*. Oxford: Routledge, 2009.

### **Book chapters**

Aspaturian, Vernon V. 'The Soviet Military-Industrial Complex: Does It Exist?' in Rosen (Ed.) *Testing the Theory of the Military-Industrial Complex*. Lexington: DC Heath and Company, 1973

Bernhard, Daniel, and Aaron K. Martin. 'Rethinking security at the Olympics' in Bennett and Haggerty (Eds.) *Security Games: Surveillance and Control at Mega-Events*. Oxford: Routledge, 2011.

Booth, Ken. 'Critical Explorations' in Ken Booth (Ed.) *Critical Security Studies and World Politics*. London: Lynne Rienner Publishers, 2005.

Eisenhower, Dwight D. 'The military-industrial complex'. Radio and television broadcast from Washington, DC, USA (17 January 1961), in *Chambers Book of Speeches*. Edinburgh: Harrap Publishers, 2006.

Evans, David. 'The role of the private security industry' in Richards et. al. (Eds.) *Terrorism and the Olympics: Major event security and lessons for the future*. London: Routledge, 2011.

Feakin, Tobias. 'UK Perspectives on Security in an age of 'Shock and Aftershock'' in Klaus Thoma (Ed.) *European Perspectives on Security Research*. Berlin: Springer-Verlag, 2011.

Freedman, Lawrence. 'Britain and the Revolution in Military Affairs' in Andrew Dorman, Mike Smith and Matthew Uttley (Eds.) *The Changing Face of Military Power: Joint Warfare in and Expeditionary Era*. Basingstoke: Palgrave, 2002.

- Dupont, Benoit. 'Power struggles in the field of security: implications for democratic transformation' in Jennifer Wood and Benoit Dupont. *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press, 2006.
- Franklin, Julian. 'Introduction' in Jean Bodin, *On Sovereignty: Four chapters from The Six Books of the Commonwealth*. Cambridge: Cambridge University Press, 1992.
- Gearson, John. 'The Nature of Modern Terrorism' in Lawrence Freedman (Ed.) *Superterrorism: Policy Response*. (Oxford: Blackwell Publishing Ltd, 2002).
- Gregory, Frank. 'The European Union and the promotion of major event security within the EU area' in Richards et. al. *Terrorism and the Olympics: Major event security and lessons for the future*. London: Routledge, 2011.
- Gregory, Frank. 'National governance structures to manage the response to terrorist threats and attacks: A cross-national comparative analysis with special reference to the UK 'lead department' response structure and UK counter-terrorism strategy' in Wilkinson (Ed.) *Homeland Security in the UK: Future preparedness for terrorist attack since 9/11*. London: Routledge, 2007.
- Gregory, Frank. 'Private sector roles in counter-terrorism' in Wilkinson (Ed.) *Homeland Security in the UK: Future preparedness for terrorist attack since 9/11*. London: Routledge, 2007.
- Gregory, Frank. 'UK draft Civil Contingencies Bill 2003 and the subsequent Act: Building block for homeland security?' in Wilkinson (Ed.) *Homeland Security in the UK: Future preparedness for terrorist attack since 9/11*. London: Routledge, 2007.
- Hayward, Keith. 'Defence Industrial Strategy Under the Coalition' in Michael Codner and Michael Clarke (Eds.), *A Question of Security: The British Defence Review in An Age of Austerity*. London: IB Taurus and RUSI, 2011.
- Howard, Michael. 'Philip Bobbitt's Terror and Consent: A Brief Critique' in David Fisher and Rian Wicker (Eds.) *Just War on Terror?: A Christian and Muslim Response*. Farnham: Ashgate Publishing, 2010.
- Jennings, Will. 'Governing the Games in an age of uncertainty: The Olympics and organisational responses to risk in Richards et. al. (Eds.) *Terrorism and the Olympics: Major event security and lessons for the future*. London: Routledge, 2011.
- Johnston, Les. 'Transnational Security Governance' in Jennifer Wood and Benoit Dupont (Eds.) *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press, 2006.
- Keohane, Robert O. 'Sovereignty in International Society' in David Held and Anthony McGrew (Eds.) *The Global Transformations Reader, Second Edition*. Cambridge: Polity Press, 2003.

- Krause, Keith, and Michael C. Williams. 'From Strategy to Security: Foundations of Critical Security Studies' in Keith Krause and Michael C. Williams (Eds.) *Critical Security Studies: Concepts and Cases*. London: UCL Press, 1997.
- Levine, Edward P. 'Methodological Problems in Research on the Military-Industrial Complex' in Steven Rosen (Ed.) *Testing the Theory of the Military-Industrial Complex*. Lexington: DC Heath and Company, 1973.
- Makarenko, Tamara. 'Immigration and asylum issues' in Wilkinson (Ed.) *Homeland Security in the UK: Future preparedness for terrorist attack since 9/11*. London: Routledge, 2007.
- Mann, Bruce. 'The UK civil contingencies framework – building common endeavour' in Paul Cornish (Ed.) *Britain and Security*. London: Smith Institute, 2007. Via: <http://www.smith-institute.org.uk/file/BritainandSecurity.pdf> (accessed 29.07.13)
- Mann, Michael. 'Has Globalization Ended the Rise and Rise of the Nation State?' in David Held and Anthony McGrew (Eds.) *The Global Transformations Reader, Second Edition*. Cambridge: Polity Press, 2003.
- Miles, Roger. 'Empowering Emergency Responders' in Simon Bennett (Ed.) *Innovative Thinking in Risk, Crisis, and Disaster Management*. Farnham: Gower Publishing Ltd, 2012.
- Molnar, Adam, and Laureen Snider. 'Mega-events and mega-profits: Unravelling the Vancouver 2010 security-development nexus' in Bennett and Haggerty, *Security Games: Surveillance and Control at Mega-Events*. Oxford: Routledge, 2011.
- Moskos, Jr., Charles C. 'The Military-Industrial Complex: Theoretical Antecedents and Conceptual Contradictions' in Sam C. Sarkesian (Ed.) *The Military-Industrial Complex: A Reassessment*. London, Sage Publications, 1972.
- Mottram, Richard. 'Protecting the Citizen in the Twenty-First Century: Issues and Challenges' in Peter Hennessy (Ed.) *The New Protective State: Government, Intelligence and Terrorism*. London: Continuum Books, 2007.
- Mueller, John. 'The Terrorism Industry: The Profits of Doom', in George Kassimeris (Ed.), *Playing Politics with Terrorism: A User's Guide*. New York: Columbia University Press, 2008.
- Neville-Jones, Pauline, and Neil Fisher. 'Homeland Security and the Role of Business' in Esther Brimmer (Ed.) *Transforming Homeland Security: U.S. and European Approaches*. Washington, DC: Center for Transatlantic Relations, 2006.
- Osborne, Peter. 'The Use and Abuse of Terror: The Construction of a False Narrative on the Domestic Terror Threat' in George Kassimeris (Ed.) *Playing Politics with Terrorism: A User's Guide*. Chichester: Columbia University Press, 2008.
- Percy, Sarah. 'Morality and regulation' in Simon Chesterman and Chia Lehnhardt (Eds.) *From Mercenaries to Market: The Rise and Regulation of Private Military Companies*. Oxford: Oxford University Press, 2007.

- Philpott, Dan. 'Sovereignty' in Edward N. Zalta (Ed.) *The Stanford Encyclopedia of Philosophy*. Summer 2010 Edition. Via: <http://plato.stanford.edu/archives/sum2010/entries/sovereignty/> (accessed 23.06.11)
- Pilisuk, Marc, and Thomas Hayden. 'Is there a military-industrial complex?' in Carroll W. Pursell, Jr. (Ed) *The Military-Industrial Complex*. New York: Harper and Row, 1972.
- Richards, Anthony. 'The emergency response: Progress and problems' in Wilkinson (Ed.) *Homeland Security in the UK: Future preparedness for terrorist attack since 9/11*. London: Routledge, 2007.
- Roland, Alex. 'The Military-Industrial Complex: Lobby and Trope' in Andrew J. Bacevich (Ed.) *The Long War: A New History of National Security Policy since World War II*. New York: Columbia University Press, 2007.
- Rosen, Steven. 'Testing the Theory of the Military-Industrial Complex', in Rosen (Ed.) *Testing the Theory of the Military-Industrial Complex*. Lexington: DC Heath and Company, 1973.
- Ruxton, Alastair. 'Structure of the Olympic Movement, the Paralympic Movement and London 2012' in Adam Lewis and Jonathan Taylor (Eds.) *Sports Law and Practice - 2nd Edition*. Haywards Heath: Tottell, 2008.
- Samatas, Mina. 'Surveilling the 2004 Athens Olympics in the aftermath of 9/11' in Bennett and Haggerty *Security Games: Surveillance and Control at Mega-Events*. Oxford: Routledge, 2011.
- Shearing, Clifford. 'Reflections on the refusal to acknowledge private governments' in Jennifer Wood and Benoit Dupont. *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press, 2006.
- Slater, Jerome, and Terry Nardin. 'The Concept of a Military-Industrial Complex' in Rosen (Ed.) *Testing the Theory of the Military-Industrial Complex*. Lexington: DC Heath and Company, 1973.
- Slaughter, Anne-Marie. 'Governing Through Government Networks' in David Held and Anthony McGrew (Eds.) *The Global Transformations Reader, Second Edition*. Cambridge: Polity Press, 2003.
- Stewart, Andrew. 'The UK Private Sector and the Threat from Terrorism' in Bowen, Wyn Q, and Andrew Stewart (Eds.) *Terrorism in the UK: Broadening the UK Government's Counter-Terrorist Response - CONTEST, The Airey Neave Papers, Occasional 50*. UK: Strategic and Combat Studies Institute, 2005.
- Strange, Susan. 'The Declining Authority of States' in David Held and Anthony McGrew (Eds.) *The Global Transformations Reader, Second Edition*. Cambridge: Polity Press, 2003.



Stuart, Andrew. 'The UK Private Sector and the Threat from Terrorism' in Wyn Q Bowen and Andrew Stuart (Eds.) *Terrorism in the UK: Broadening the UK Government's Counter-Terrorist Response – CONTEST*. UK: Strategic and Combat Studies Institute, 2005.

Uttley, Matthew. 'Defence Procurement and Industrial Policies' in Stuart Croft, Andrew Dorman, Wyn Rees and Matthew Uttley. *Britain and Defence 1945-2000: A Policy Re-evaluation*. Harlow: Pearson Education Limited, 2001.

Uttley, Matthew. 'Equipping Britain's Armed Forces: Continuity and Change in Defence Procurement and Industrial Policy' in Andrew Dorman, Mike Smith and Matthew Uttley (Eds.) *The Changing Face of Military Power: Joint Warfare in and Expeditionary Era*. Basingstoke: Palgrave, 2002.

Weston, Keith. 'The challenge of inter-agency coordination' in Richards et. al., *Terrorism and the Olympics: Major event security and lessons for the future*. London: Routledge, 2011.

Wilkinson, Paul. 'The threat from the Al-Qaeda network' in Wilkinson (Ed.) *Homeland Security in the UK: Future preparedness for terrorist attack since 9/11*. Oxford: Routledge, 2007.

Wolf, Jr, Charles. 'Military-Industrial Simplicities, Complexities and Realities' in Sam C. Sarkesian (Ed.) *The Military-Industrial Complex: A Reassessment*. London: Sage Publications, 1972.

### **Journal Articles**

Aitken, Jonathan. 'Defence Procurement: Past, Present and Future'. *RUSI Journal*. Vol. 139:1 (1994): pp.39-42

Amoore, Louise. 'Algorithmic War: Everyday Geographies of the War on Terror'. *Antipode*. Vol:41:1 (2009): pp.49-69

Anders, Birthe. 'Private Military and Security Companies and Humanitarian Organisations: Partners in Aid?' *World Defence Systems* (2010:2): pp.130-131

Baldwin, David A. 'The Concept of Security'. *Review of International Studies*. Vol.23 (1997): pp.5-26

Boyle, Phillip, and Kevin D. Haggerty. 'Spectacular Security: Mega-Events and the Security Complex'. *International Political Sociology*. Vol.3:3 (2009): pp.257-274

Bures, Oldrich. 'Private Actors in the Fight Against Terrorist Financing: Efficiency Versus Effectiveness'. *Studies in Conflict and Terrorism*. Vol.35:10 (2012): pp.712-732

Busch, Nathan, and Austen Givens. 'Public-Private Partnerships in Homeland Security: Opportunities and Challenges'. *Homeland Security Affairs*. Vol.8 (October 2012). Via: <http://www.hsaj.org/?article=8.1.18> (accessed 26.12.14): pp.1-14

- Byrne, Edmund F. 'The U.S. Military-Industrial Complex is Circumstantially Unethical'. *Journal of Business Ethics*. Vol.95 (2010): pp.153-165
- Caverley, Jonathan, and Ethan B. Kapstein. 'Arms Away: How Washington Squandered Its Monopoly on Weapons Sales'. *Foreign Affairs* (September-October 2012). Via: <http://www.foreignaffairs.com/articles/138035/jonathan-caverley-and-ethan-b-kapstein/arms-away> (accessed 20.02.13)
- Chalmers, Malcolm, Neil V Davies, Keith Hartley and Chris Wilkinson. 'The Economic Costs and Benefits of UK Exports'. *Fiscal Studies*. Vol. 23:3 (2002): pp.343-367
- Coaffee, Jon. 'From Counterterrorism to Resilience'. *The European Legacy*. Vol.11:4 (2006): pp.389-403
- Coaffee, Jon, Pete Fussey and Cerwyn Moore. 'Laminated Security for London 2012: Enhancing Security Infrastructures to Defend Mega Sporting Events'. *Urban Studies*. Vol.48:15 (2011): pp.3311-3327
- Cornish, Paul. 'Technology, Strategy and Counterterrorism'. *International Affairs*. Vol. 86:4 (2010): pp.875-888
- Davies, Philip H.J. 'Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services'. *Politics*. Vol.21:1 (2001): pp.73-80
- Desch, Michael C. 'The State and the Monopolization of International Violence'. *Mershon International Studies Review*. Vol.39:1 (1995): pp.149-151
- Dibb, Sally, Kirstie Ball, Ana Canhoto, Elizabeth M. Daniel, Maureen Meadows, and Keith Spillar. 'Taking responsibility for border security: Commercial interests in the face of e-borders'. *Tourism Management*. Vol.24 (2014): pp.50-61
- Dover, Robert. 'Britain, Europe and Defense in the Post-Industrial Age'. *Defence & Security Analysis*. Vol.27:1 (2011): p.19-30
- Dover, Robert. 'For Queen and Company: The Role of Intelligence in the UK's Arms Trade'. *Political Studies*. Vol.55 (2007): pp.683-708.
- Drayson, Lord. 'The Defence Industrial Strategy: Our Relationship with Industry'. *RUSI Defence Systems*. Vol. 9:1 (2006). Via: [http://www.rusi.org/downloads/assets/020-025\\_The\\_Debate1.pdf](http://www.rusi.org/downloads/assets/020-025_The_Debate1.pdf) (accessed 01.06.11): pp.20-22
- Dunlap Jr., Charles J. 'The Military-Industrial Complex'. *Daedalus*. Vol.140:3 (2011): pp.135-143
- Dunne, J Paul. 'The Changing Military Industrial Complex in the UK'. *Defence Economics*. Vol.4 (1993): pp.91-111
- Edgerton, David. 'The British military-industrial complex in history: the importance of political economy'. *The Economics of Peace and Security Journal*. Vol. 3:1 (2008): pp.6-10

- Edmunds, Timothy. 'The defence dilemma in Britain'. *International Affairs*. Vol.86:2 (2010): pp.389-393
- Engerer, Hella. 'Security as a public, private or club good: some fundamental considerations'. *Defence and Peace Economics*. Vol.22:2 (2001): pp.135-145
- Erbel, Mark. 'Contractors in the "War on Terror": Enabling Global Military Deployment'. *e-International Relations* (18.08.11). Via: <http://www.e-ir.info/2011/08/18/contractors-in-the-%e2%80%9cwar-on-terror%e2%80%9d-enabling-global-military-deployment/> (accessed 15.08.12)
- Fallows, James. 'The Dustbin of History: The Military-Industrial Complex'. *Foreign Policy*. No.131 (November/December 2002): pp.46-48
- Fussey, Pete. 'Command, control and contestation: negotiating security at the London 2012 Olympics'. *The Geographical Journal* (2013). Via: <http://onlinelibrary.wiley.com/doi/10.1111/geoj.12058/abstract> (last accessed 30.12.14)
- Gearson, John, and James Gow. 'Security, Not Defence, Strategic, Not Habit: Restructuring the Political Arrangements for Policy Making on Britain's Role in the World'. *Political Quarterly*. Vol. 81:3 (2010): pp.406-419
- Gilmore, Margaret. 'Countdown to the Olympics'. *RUSI Journal*. Vol.156:2 (2011): pp.28-34
- Giulianotti, Richard, and Francisco Klauser. 'Security Governance and Sport Mega-events: Toward an Interdisciplinary Research Agenda'. *Journal of Sport and Social Issues*. Vol.34:1 (2010): pp.49-61
- Godfrey, Richard, Jo Brewis, Jo Grady and Chris Grocott. 'The private military industry and neoliberal imperialism: Mapping the terrain'. *Organization*. Vol.21:1 (2014): pp.106-125
- Hartley, Keith. 'Collaboration and European Defence Industrial Policy'. *Defence and Peace Economics*. Vol.19:4 (2008): pp.303-315
- Hartley, Keith. 'Defence Procurement in the UK'. *Defence and Peace Economics*. Vol.9:1 (1998): pp.39-61
- Hartley, Keith. 'The Economics of the UK Defence Industrial Strategy'. *Security Challenges*. Vol.3:2 (2007) Via: <http://www.securitychallenges.org.au/ArticlePDFs/vol3no2Hartley.pdf> (accessed 04.02.13): pp.19-30
- Hartung, William D. 'Eisenhower's Warning: The Military-Industrial Complex Forty Years Later'. *World Policy Journal*. Spring 2001: pp.39-44
- Hayward, Keith. "'I have seen the future and it works": The US Defence Industry Transformation - Lessons for the UK Defence Industrial Base'. *Defence and Peace Economics*. Vol. 16:2 (2005): pp.127-141
- Hayward, Keith. 'The Globalisation of Defence Industries'. *Survival*. Vol.43:2 (2001): pp.115-132

- Herrington, Lewis, and Richard Aldrich. 'The Future of Cyber-Resilience in an Age of Global Complexity'. *Politics*. Vol.33:4 (2013): pp.299-310
- Hills, Alice E. 'Co-ordination and Disaster Response in the United Kingdom'. *Disaster Prevention and Management*. Vol.3:1 (1994): pp.66-71
- Hinds, Alphas. 'Fortress Olympics: Counting the cost of major event security'. *Jane's Intelligence Review*. Vol.19:5 (2007): pp.20-26
- Houlihan, Barrie, and Richard Giulianotti. 'Politics and the London 2012 Olympics: the (in)security Games', *International Affairs*. Vol.88:4 (2012): pp.701-717
- Jeffrey, Bill. 'Implementing the Defence Industrial Strategy'. *RUSI Defence Systems*. Vol. 9:1 (2006). Via: [http://www.rusi.org/downloads/assets/020-025\\_The\\_Debate1.pdf](http://www.rusi.org/downloads/assets/020-025_The_Debate1.pdf) (accessed 01.06.11): pp.22-23
- Kirkpatrick, David. 'The UK's Defence Industrial Strategy'. *Defence Studies*. Vol.8:3 (2008): pp.286-310
- Kirkpatrick, David. 'Trends in the costs of weapon systems and the consequences'. *Defence and Peace Economics*. Vol.15:3 (2004): pp.259-273
- Krahmann, Elke. 'Conceptualizing Security Governance'. *Cooperation and Conflict: Journal of the Nordic International Studies Association*. Vol. 38:1 (2003): pp.5-26
- Krahmann, Elke. 'Security Governance and Networks: New Theoretical Perspectives in Transatlantic Security'. *Cambridge Review of International Affairs*. Vol.18:1 (2005): pp.15-30
- Krause, Keith, and Michael Williams. 'Broadening the Agenda of Security Studies: Politics and Methods'. *Mershon International Studies Review*. Vol. 40:2 (1996): pp.229-254
- Lai, David. 'The great power dilemma: The trade-off between defense and growth in Great Britain, 1830-1980'. *Defence and Peace Economics*. Vol. 12:2 (2001): pp.145-156
- Lake, David A. 'The New Sovereignty in International Relations'. *International Studies Review*. Vol.5 (2003): pp.303-323
- Leander, Anna. 'The Market for Force and Public Security: The Destabilizing Consequences of Private Military Companies'. *Journal of Peace Research*, Vol.42:5 (2005): pp.605-622
- Livingstone, Ken, and Jerry Hart. 'The Wrong Arm of the Law?: Public images of Private Security'. *Policing and Society*. Vol. 13:2 (2003): pp.159-170
- Loader, Ian. 'Thinking Normatively About Private Security'. *Journal of Law and Society*. Vol.24:3 (1997): pp.377-394
- Markusen, Ann. 'The Rise of World Weapons'. *Foreign Policy*. No.114 (Spring 1999): pp.40-51

- Martin, Stephen. 'The subsidy savings from reducing UK arms exports'. *Journal of Economic Studies*. Vol.26:1 (1999): pp.15-37
- Mueller, John, and Mark G Stewart. 'The Terrorism Delusion'. *International Security*. Vol.37:1 (2012): pp.81-110.
- Neocleous, Mark. 'Security, Commodity, Fetishism', *Critique: Journal of Socialist Theory*. Vol.35:3 (2007): pp.339-355
- Neuman, Stephanie G. 'Power, Influence, and Hierarchy: Defense Industries in a Unipolar World'. *Defence and Peace Economics*. Vol.21:1 (2010): pp.105-134
- O'Brien, Geoff, and Paul Read. 'Future UK emergency management: new wine, old skin?' *Disaster Prevention and Management*. Vol.14:3 (2005): pp.353-361
- Omand, David. 'Emergency Planning, Security and Business Continuity'. *RUSI Journal*. Vol.149:4 (2004): pp.26-33
- Omand, David. 'The Terrorist Threat to the UK in the Post-9/11 Decade'. *Journal of Terrorism Research*. Vol.3:1 (2012). Via: <http://ojs.st-andrews.ac.uk/index.php/jtr/article/view/412/371> (accessed 22.07.13)
- Omand, David. 'What is the Future for the Critical National Infrastructure?'. *RUSI Monitor*. Vol. 7:4 (2008): pp.8-15
- O'Reilly, Conor. 'The transnational security consultancy industry: A case of state-corporate symbiosis'. *Theoretical Criminology*. Vol. 14:2 (2010): pp.183-210
- Owens, Patricia. 'Distinctions, distinctions: 'public' and 'private' force?' *International Affairs*. Vol. 84:5 (2008): pp.977-990
- Phillips, Mark. 'Policy-Making in Defence and Security: Lessons from the Strategic Defence and Security Review'. *RUSI Journal*. Vol.157:1 (2012): pp.28-35
- Pilisuk, Marc, and Thomas Hayden. 'Is there a military-industrial complex which prevents peace?' *Journal of Social Issues*. Vol.21:3 (1965): pp.67-117
- Rathmell, Andrew. 'Privatising Intelligence'. *Cambridge Review of International Affairs*. Vol.11:2 (1998): pp.199-211
- Richards, Anthony. 'Conceptualizing Terrorism'. *Studies in Conflict and Terrorism*. Vol.37:3 (2014): pp.213-236
- Richards, David. 'Elite Interviewing: Approaches and Pitfalls'. *Politics*. Vol.16:3 (1996): pp.199-204;
- Ritchie, Nick. 'Rethinking security: a critical analysis of the Strategic Defence and Security Review'. *International Affairs*. Vol.87:2 (2011): pp.355-376

- Rosemont, Hugo. 'Getting Down to Business: Industry's Role in National Security'. *RUSI Journal*. Vol.155:1 (2010): pp.80-85
- Rosemont, Hugo. 'Industry's role in counter terrorism'. *Defence Contracts Bulletin*. Vol.9:22 (2011): pp.14-15
- Rosemont, Hugo. 'Private Sector Engagement in the UK's Counter-Terrorism Strategy: A New Agenda', *Behavioral Sciences of Terrorism and Political Aggression*. Vol.6 (2014): pp.147-161
- Schneider, Ernest. 'Causal Factors in Variations in US Postwar Defense Spending'. *Defense Analysis*. Vol.4:1 (1988): pp.53-79
- Scott, James P. 'Does UK defence spending crowd-out UK private sector investment?'. *Defence and Peace Economics*. Vol. 12:4 (2001): pp.325-336
- Sempere, Carlos. 'The European Security Industry. A Research Agenda'. *Defence and Peace Economics*. Vol.22:2 (April 2011): pp.245-264
- Smith, James. 'Civil Contingency Planning in Government'. *Parliamentary Affairs*. Vol.56:3 (2003): pp.410-422
- Soria, Valentina. 'Beyond London 2012: The Quest for a Security Legacy'. *RUSI Journal*. Vol.156:2 (April/May 2011): pp.36-43
- Soria, Valentina. 'Promoting the Concept of 'UK plc': A Public-Private Sector Olympic Challenge'. *RUSI Journal*. Vol.157:2 (April/May 2012): pp.32-38
- Taylor, Trevor. 'Defence industries in international relations'. *Review of International Studies*. Vol.16:1 (1990): pp.59-73.
- Taylor, Trevor. 'Reforming UK Defence Industrial Policy'. *RUSI Defence Systems*. Vol.14:1 (2011): pp.35-37
- Taylor, Trevor. 'Smart Procurement and the Partnership with Industry'. *RUSI Journal*. Vol.143:2 (1998): pp.41-46
- Ullman, Richard H., 'Redefining Security'. *International Security*. Vol.8:1 (1983): pp.129-153
- Van Steden, Ronald, and Sarre, Rick. 'The Growth of Private Security: Trends in the European Union'. *Security Journal*. Vol.20 (2007): p.222-235
- Veness, David. 'The safety of the realm in retrospect and prospect'. *RUSI Journal*. Vol.148:4 (2003): pp.14-17
- Weiss, Robert P. 'From Cowboy Detectives to Soldiers of Fortune: Private Security Contracting and Its Contradictions on the New Frontiers of Capitalist Expansion'. *Social Justice*. Vol.34:3/4 (2007): pp.1-19

White, Adam. 'The new political economy of private security'. *Theoretical Criminology*. Vol.16:1 (2011): pp.85-101

Williams, Chris A. 'Constables for hire: the history of private 'public' policing in the UK'. *Policing and Society*. Vol.18:2 (2008): pp.190-205

Williams, Michael C. 'The Public, the Private and the Evolution of Security Studies'. *Security Dialogue*. Vol. 41:6 (2010): pp.623-630

Wolfers, Arnold. "'National Security" as an Ambiguous Symbol'. *Political Science Quarterly*. Vol. 67:4 (1952): pp.481-502

### **Working Papers**

Chesterman, Simon. "'We Can't Spy... If We Can't buy!": The Privatization of Intelligence and the Limits of Outsourcing "Inherently Government Functions"'. European University Institute (EUI) Working Paper. AEL 2009/2. Via:

[http://cadmus.eui.eu/bitstream/handle/1814/11403/AEL\\_2009\\_02.pdf?sequence=1](http://cadmus.eui.eu/bitstream/handle/1814/11403/AEL_2009_02.pdf?sequence=1)

(accessed 28.05.11)

Dunne, J Paul, and Elisabeth Sköns. 'The Changing Military Industrial Complex'. Economics Discussion Paper Series. School of Economics, University of the West Of England. March 2011. Via: <http://carecon.org.uk/DPs/1104.pdf> (accessed 01.06.11)

Dunne, J Paul and Elisabeth Sköns. 'The Military Industrial Complex' Economics Discussion Paper Series. School of Economics, University of the West of England. May 2009. Via: <http://carecon.org.uk/DPs/0907.pdf> (accessed 01.06.11)

Ninua, Tinatin. 'Regulating the Revolving Door', Transparency International Working Paper #06/2010. 1 June 2010. Via:

[http://www.transparency.org/whatwedo/pub/working\\_paper\\_06\\_2010\\_regulating\\_the\\_revolving\\_door](http://www.transparency.org/whatwedo/pub/working_paper_06_2010_regulating_the_revolving_door) (accessed 26.03.14)

### **Public Addresses / Conference Papers**

Remarks of an anonymous speaker at the 'Military Aid to the Private Authorities?' seminar hosted by the Private Military and Security Research Group (PMSRG) at King's College, London. 3 May 2012.

Baker-Beall, Christopher, and Nicholas Robinson. Abstract of 'The Emergence of the Security-Industrial Complex' at 'Neoliberalism and/as Terror: Critical Studies on Terrorism Annual Conference 2014'. Full Program. Via: [http://www.leejarvis.com/wp-content/uploads/2011/11/Neoliberalism-and\\_as-terror-2014.pdf](http://www.leejarvis.com/wp-content/uploads/2011/11/Neoliberalism-and_as-terror-2014.pdf) (accessed 10.11.14)

Hughes, Robert T. 'Could Agile Development have prevented the FiReControl project failure'. UK Academy for Information Systems Conference Proceedings 2012. Via: <http://www.ukais.org.uk/Documents/Downloads/Conference20124c054606-9517-41d3-96d4-b0dd1913f68.pdf> (accessed 12.08.13)

Rosemont, Hugo. 'Operating a Tighter Ship in 2009'. Speech to TRANSEC Annual Security Conference. Via: <http://www.assa-int.org/Uploads/dbsAttachedFiles/Day1-Operatingatightershipin2009-HugoRosemont.pdf> (accessed 26.02.14)

Rosemont, Hugo. 'Outsourcing or interdependency? Why we need to widen our approach to the study of the private sector's involvement in UK national security'. Presentation to inaugural conference of King's College, London. Private Military and Security Research Group. 18 November 2011.

Silke, Andrew. 'The Golden Age? Assessing the State of Terrorism Studies'. Keynote Speech at 7th Annual Conference of Society of Terrorism Research, London. 27 June 2013.

### **Theses and dissertations**

Abou-Bakr, Ami Jihan. 'Managing disaster: public-private partnerships as a tool for disaster mitigation, preparedness, response and resiliency in the United States'. PhD dissertation. King's College, London, 2011.

Murphy, Cian Christopher. 'The European Union rule of law in the "war on terrorism"'. PhD dissertation. King's College, London, 2010.